NSW Health

Protecting People and Property

NSW Health Policy and Standards for Security Risk Management in NSW Health Agencies

NSW Ministry of Health
1 Reserve Road
ST LEONARDS NSW 2065
Tel. (02) 9391 9000
Fax. (02) 9391 9101
TTY. (02) 9391 9900
www.health.nsw.gov.au

Produced by: NSW Ministry of Health

The NSW Ministry for Health acknowledges the traditional custodians of the lands across NSW. We acknowledge that we live and work on Aboriginal lands. We pay our respects to Elders past and present and to all Aboriginal people.

Further copies of this document can be downloaded from the NSW Health webpage www.health.nsw.gov.au

February 2022

Contents

Introduction

Purpose and Scope of Document

The purpose of the NSW Health *document 'Protecting People and Property: NSW Health Policy and Standards for Security Risk Management in NSW Health Agencies'* (The Security Manual) is to:

- Outline NSW Health policy on key aspects of personal and property security and
- Provide standards to assist NSW Health Agencies to maintain an effective security risk management program, that is based on:
  - structured ongoing risk management
  - consultation
  - appropriate documentation and record keeping
  - regular monitoring and evaluation.

In Australia everyone shares a fundamental right to basic health care. However, workers also have a right to safety in the workplace and to be treated with respect. These rights must be balanced to ensure the safety of everyone is the priority.

How the Manual is Arranged

This Manual is made up of a series of chapters, divided into four sections:

Section 1	Security Risk Management Framework
Section 2	Core Security Risk Controls
Section 3	Security Risk Controls in Priority Areas
Section 4	Security Risk Controls in Unplanned Events

Those responsible for security risk management will need to have a comprehensive awareness of the issues covered in this document.

Regular checking of the electronic copy of this Manual on the NSW Health intranet is required, to ensure the most current policy and standards are being referenced.

Each chapter deals with a key aspect of personal or property security and has the following sections:

Policy statement

This section outlines NSW Health policy on the relevant issue. NSW Health Agencies **must comply** with the policy outlined in each chapter. Policy is always presented at the start of each chapter.

Standards

The standards contained in each chapter **must** be implemented, unless a risk assessment determines that an alternative/additional control is required. A risk assessment may also identify local controls necessary to address the identified risk. Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

Definitions

Security

For the purposes of this Manual, security is the protection of a person from violence, threats and/or intentional harm; the protection of sensitive and confidential information from unauthorised disclosure, misuse and intentional destruction; and the protection of property and assets from intentional damage and from theft.

For policies about protection from cyber attack please contact eHealth or local information technology (IT) departments.

Security Risk

A factor or event, or combination of factors or events, which may impact on the security and welfare of patients, workers and others, and property (including information) for which the facility has a duty of care (AS4485.1:2021).

Violence**

Workplace violence and aggression covers a broad range of actions and behaviours that create a risk to health and safety, for example:

- physical assault such as biting, scratching, hitting, kicking, pushing, grabbing, or throwing objects
- intentionally coughing or spitting on someone
- sexual assault or any other form of indecent physical contact
- harassment or aggressive behaviour that creates a fear of violence, such as stalking, sexual harassment, verbal threats and abuse, or yelling and swearing
- hazing or initiation practices for new or young workers
- gendered violence, which is any behaviour directed at any person or that affects a person because of their sex, gender or sexual orientation, or because they do not adhere to socially prescribed gender roles, that creates a risk to health and safety, and
- violence from a family or domestic relationship when this occurs at the workplace, including if the person's workplace is their home.

NSW Health policy requirements regarding workplace conduct, including bullying and harassment are not covered within this document. They may be found at this link.

NSW Health Agency

Throughout this document the term NSW Health Agency is used to mean all public health organisations and all other bodies and organisations under the control and direction of the Minister for Health or the Secretary of NSW Health including:

- a Local Health District
- a statutory health corporation
- an affiliated health organisation in respect of its recognised establishments and recognised services and
- Health Albury Wodonga in respect of staff who are employed in the NSW Health Service. Albury Hospital is required to apply NSW Health policy relating to staff.

This Manual does not apply to the Ambulance Service of NSW or to the Ministry of Health which have separate standards. Where the Ambulance Service of NSW or the Ministry of Health are carrying out activities in conjunction with other NSW Health Agencies they would be required to comply with the standards of that agency.

Worker

The term 'worker' is used to mean anyone who carries out work for a NSW Health Agency including:

- employees
- contractors, including visiting practitioners
- sub–contractors
- employees of contractors and subcontractors
- an employee of a labour hire company e.g. agency staff/contingent workers
- volunteers
- an apprentice or trainee
- work experience students.

Anyone who carries out work for a NSW Health Agency is given the legal status of 'worker' under section 7 of the *NSW Work Health and Saferty (WHS) Act 2011*.

Other or shared duty holder

An 'other duty holder', referred to in section 16 of the *NSW WHS Act*, means another person (or organisation) who concurrently has a duty for the same health and safety matter as the NSW Health Agency eg other NSW Health Agencies (such as NSW Ambulance, Health Share, Health Infrastructure or HealthPathology), labour hire companies, building /service contractors, retail stores and lessors. Each duty holder must comply with that duty to the standard required by the *NSW WHS Act*, even if another duty holder has the same duty.

(**Preventing workplace violence and aggression, National guidance material, SafeWork Australia, January 2012)

1. Security Risk Management

Policy

NSW Health Agencies are required to ensure that:

- **there is a governance structure in place that establishes and maintains effective leadership, oversight and reporting of security risk management in all facilities**
- **Chief Executives and the Board (including the Audit and Risk Committees) are provided with relevant information on security related risks and incidents and how they are being addressed**
- **a formal mechanism to facilitate collaboration and information sharing between clinical, WHS and security personnel must be established and implemented (eg a security committee). This mechanism must identify emerging security related risk, optimise the effectiveness of risk control strategies and increase and integrate security awareness within the NSW Health Agency**
- **all reasonably foreseeable security related hazards are identified and assessed**
- **risks associated with these hazards are eliminated where reasonably practicable**
- **where the risk cannot be eliminated, appropriate control strategies are implemented so that risks are reduced to the lowest practicable level**
- **consultation with workers and/or nominated health and safety representatives (HSRs) and any other WHS consultative mechanisms occurs during all stages of risk management**
- **each stage of the risk management process, including the consultation that occurred, is documented**
- **risk control strategies are monitored and regularly evaluated for effectiveness, including the assessment of factors that contributed to incidents**
- **consultation, co-operation and co-ordination with other duty holders occurs where there is a shared duty**
- **incidents and near misses are reported and investigated, and outcomes communicated to workers in the area where incidents have occurred**
- **allocation of appropriate harm scores are monitored**
- **ims+ records are monitored and closed only once appropriate action is taken and communicated to relevant workers.**

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

1.1 Establish and deliver a sound security governance within the NSW Health Agency

Effective security governance involves a number of interconnected elements:

- strong leadership in security risk management
- clear and defined accountability and responsibility for security risk management (and security operations)
- allocation of authority to make decisions about security (risk and operations) in the appropriate way and at the appropriate level within the facility and NSW Health Agency
- processes to identify, assess and eliminate or control security risks
- processes to engage with and consult workers, WHS representatives and other external bodies (eg Security Licencing and Enforcement Directorate (SLED), SafeWork NSW, unions etc) on security risk
- processes for decision makers, and those with allocated accountability, to be informed about security risk, control measures in place and security performance
- processes for checking compliance with NSW legislative obligations (eg WHS and Security Industry) and NSW Health security standards (this Manual and related policies).

NSW Health Agencies are to ensure that all elements of a security governance structure are in place and are continuously monitored for effectiveness.

1.2 Understand and utilise the security risk management process

Security risk management involves assessing all aspects of the clinical and non–clinical environment, including internal and external risks eg local crime profile.

NSW Health Agencies must identify hazards arising from their work/workplaces, assess the risks arising from the hazards and develop strategies to eliminate, or where they cannot be eliminated, minimise these risks. This process is referred to as risk management. The NSW Health Policy Directive *Work Health and Safety: Better Practice Procedures* outlines the risk management process and in what circumstances it must occur. NSW Health Agencies may have developed templates and tools to be used, consistent with the requirements set out in these relevant NSW Health policies.

Assessment of risk must occur:

- before changing premises, work practices, procedures (including clinical procedures) or the work environment eg introducing new models of care, redesigning a staff station, or ensuring the absence of concealment/entrapment points when designing premises
- before purchasing equipment eg providing duress alarms or using new substances
- before planning to improve productivity or reduce costs
- when new information about workplace violence/security risks becomes available
- when reviewing and responding to past violent/security incidents (even if they have caused no injury)
- when responding to concerns raised by workers, health and safety representatives or others at the workplace about risks arising from potential violence
- as required by the WHS regulations for specific hazards.

Risk management must also be part of the process for designing and planning products or services, processes or places used for work. It is more effective to eliminate hazards at the design stage, eg ensuring that new buildings do not have concealment/entrapment points, implementing standard procedures for after–hours access control in emergency departments, or implementing assessment procedures prior to workers visiting a patient in the community.

The security risk management process must be undertaken by those who have expertise in the areas being assessed, in consultation with workers and other stakeholders (see Section 1.3 below). A multidisciplinary team approach that incorporates the expertise of clinical, non–clinical, WHS and security staff is essential when undertaking risk management to ensure the full scope of risk can be identified and assessed.

1.2.1 Undertake consultation as an essential part of risk management

WHS legislation requires NSW Health Agencies to consult with workers and/or their representatives. If there is a HSR they must be involved in the consultation.

Consultation is a pivotal activity at all stages of the risk management process. Workers are most likely to know the risks associated with their work and may be in a good position to comment on the practicality of suggested controls or suggest other effective controls.

Consultation must be undertaken with those performing the activity and, where appropriate, other persons with relevant knowledge, such as security and risk managers. During the security risk management process consultation should also occur with other appropriate stakeholders, such as Police.

Consultation must occur:

- when identifying hazards and assessing risks
- when making decisions about ways to eliminate or minimise those risks
- when making decisions about the adequacy of facilities
- when proposing changes that may affect the health or safety of workers
- when making decisions about the procedures for consultation, WHS issue resolution
- health monitoring or provision of information and training.

Additionally, where there is a shared duty as outlined in section 16 of the WHS Act, NSW Health Agencies are required to consult, co-operate and co-ordinate activities with all other persons who have a work health or safety duty in relation to the same matter so far as is reasonably practicable.

Consultation requires that:

- relevant information is shared
- workers are given a reasonable opportunity to express their views and contribute to decision making processes
- views of workers are taken into account
- those consulted are advised of the outcome in a timely manner.

1.2.2 Establish the context

The first step in security risk management involves the process of establishing the context. This is done by identifying:

- what type of workplace it is? Is it a private residence for a community nurse, a multipurpose facility in rural NSW, a kitchen, office, mental health ward or a metropolitan emergency department?

- who are the stakeholders (internal and external) and who will be affected? Consider workers and other businesses or organisations that may be impacted by hazards in the workplace eg: paramedics, visitors, retail workers on the premises, external businesses, University clinical schools that use NSW Health Agency premises
- what tasks are being undertaken in that workplace? For example, the clinical treatment of patients with high medical dependency or home visits to monitor post discharge progress?
- what are the work processes? Consider the activities making up the work process, including workers, their knowledge and experience, and the equipment and systems of work being used.

1.2.3 Identify security hazards

In order to eliminate or control factors that can affect the security of people, property and the environment, a structured approach for identifying security hazards and their contributing factors must be established and undertaken.

Security hazard identification is the process of identifying all contributing factors including situations, procedures, events or factors in the workplace (including the design of premises) and which arise during the course of work (eg during the delivery of clinical care, during work related travel or during the procurement of equipment) that could potentially cause injury or illness to workers, patients or others, the unauthorised disclosure of information, or loss of or damage to property.

To ensure that all aspects of the work system and environment are considered, security hazard identification must include:

- observing the nature of the work being undertaken
- reviewing incident, first aid and workers compensation statistics, incident reports, hazard reports and any other available data including trend data
- reviewing results of recent security incident investigations
- reviewing results of recent duress response operational reviews
- reviewing results of formal workplace inspections and security/violence/aggression audits
- consulting with workers in the workplace to determine what they consider are the hazards
- consulting with other stakeholders as appropriate, including external agencies eg unions, police and other duty holders
- review of the location including formal workplace inspections and security audits, co–located business and services (as relevant)
- developing scenarios about what could happen during or because of a security incident
- analysing incidents and near misses
- considering all possible contributing risk factors, eg staffing and skills, clinical procedures, work environment/building design, equipment, training, patient demographics and other related factors
- considering who might be harmed and how, including:
  - potential hazards that may arise from or affect patients, clients or others, including:
    - alcohol and drug affected individuals
    - medical / mental health conditions
    - known as against unknown clients
    - socio–economic/crime factors in the local area
    - the type of service being delivered (eg ward /unit or in the community).
  - potential targets of violence, eg workers, patients/clients, others such as visitors
  - systems in place to manage violence and aggression risks from patients/clients/others:
    - assessment protocols
    - treatment protocols
    - systems for review of the above
    - access to response services in the event of an emergency, for example availability of Code Black response.
  - once it is clear who has the potential to cause or be harmed by aggression/violence, consider:
    - particular requirements of the workers eg knowledge and skills, young or new workers, older workers, workers with a disability, workers working in the community, pregnant workers, workers with English as a second language
    - potential for psychological harm arising from aggression, from those involved in an incident, those witnessing an incident or vicarious trauma
    - particular requirements of different patient groups –diagnosis and treatment to reduce risk of aggressive/violent behaviours
    - people who may not be in the workplace all the time eg cleaners, visitors, contractors, maintenance workers.

1.2.4 Types of hazards potentially experienced in the health environment

NSW Health Agencies are complex work environments which accommodate and deliver a wide range of internal and external services to a wide variety of individuals. The large number of people who frequent health facilities reflect the communities they serve including some people who exhibit challenging and aggressive behaviours, including arising from their clinical condition.

Services delivered outside of a hospital setting such as Community Health Centres must manage the specific risks present by working remotely from such hubs and in settings that are not under the control of the service, ie in clients' homes.

Throughout the risk management process attention must be paid, in particular, to the following hazards:

- individuals who present with severe behavioural disturbances/known history of physical and or verbal aggression
- individuals with complex clinical conditions that may cause unpredictable behaviour
- the potential for violence to occur outside of the workplace but arising from the workplace.
- unauthorised access to staff only or clinical areas within a workplace (including unauthorised access to keys, ID cards)
- unauthorised access to critical infrastructure (telecommunications, mains and backup power, water, chillers, gas etc)
- unauthorised access to high risk plant, equipment or substances (biomedical, nuclear medicine, cytotoxic etc), including waste materials
- proximity to support and assistance services (Security, Emergency Services)
- entrapment of workers and/or other persons
- concealment of individuals/ concealment of weapons (opportunistic and prohibited)
- undertaking enforcement actions such as the enforcement of parking restrictions and no–smoking areas
- working at night or outside of normal business hours (including access to parking)
- isolated and/or remote working
- theft of equipment, information, medications, workers/ patient belongings etc
- use of/ access to equipment which may be used as a weapon
- patients in the custody of another Agency
- large campuses with dark surroundings/ inadequate lighting
- trespass
- bomb threats/terrorist threats/armed hold–up
- exposure to infectious diseases
- relationship issues eg domestic violence
- worker factors eg fatigue, rushing / work pressure, relevant skills and qualities for engagement with highly distressed individuals.

1.2.5 Assess security risk

Security risk assessment is the process of determining how likely it is that someone could be harmed or that property could be damaged/stolen and how serious the consequences might be.

Factors to consider in assessing security risks are:

- extent of exposure to the hazard (frequency and duration)
- severity of potential injury/illness or loss associated with the risk arising from each hazard
- likelihood of injury/illness/loss/damage occurring
- number of people/amount or type of property at risk
- the effectiveness of the existing control strategies (if they are in place).

The process of assessment will involve:

- consultations with workers, their HSRs, relevant unions and any subject matter experts or other stakeholders
- examining the experience of the workplace or other similar workplaces including a review of incident data and near misses and other information such as SafeWork Improvement Notices and actions implemented from within the health agency and across the state. Several state–wide forums exist for the exchange of information and innovation
- reviewing relevant legislation, codes of practice from NSW or other Australian jurisdictions, Australian Standards, industry guidance material and NSW Health policies and guidelines
- reviewing clinical, WHS and security information relating to incidents.

Part of the assessment process is the prioritisation of risks for action. Security hazards assessed as having a high risk factor must be eliminated/controlled immediately. Likewise, low priority hazards that can be easily addressed must also be done without delay. Actions must be planned and prioritised to improve workplace security. See the *NSW Health Enterprise–wide Risk Management Policy and Framework* for details.

Risk Managers and Security Managers must be consulted to identify the tools currently used within the NSW Health Agency for identifying and assessing risk.

1.2.6 Control security risks

Security risk control is the process of implementing appropriate measures to eliminate or, where they cannot be eliminated, minimise risks to personal and property security.

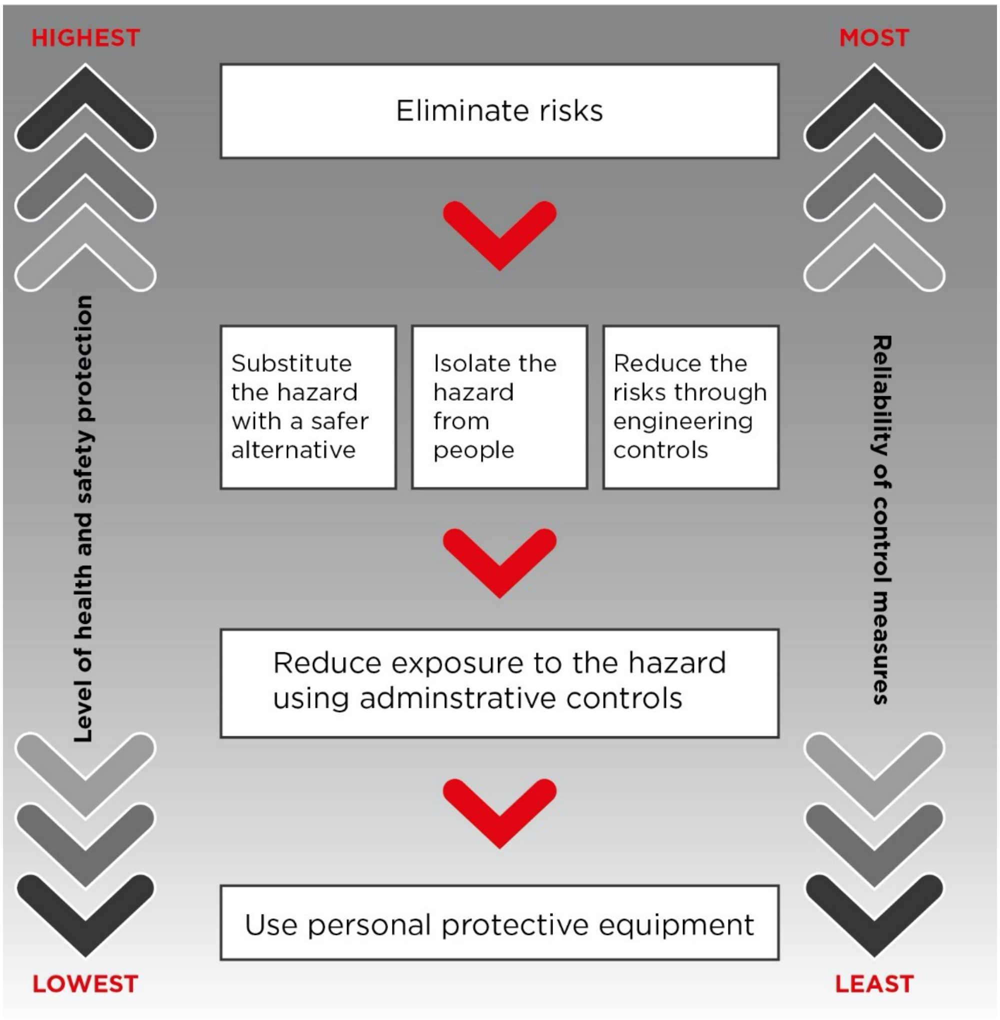
Eliminating the hazard is the most effective way of controlling risk (eg securing a storage area to ensure opportunistic thieves cannot enter, which in turn eliminates the risk of a worker member being assaulted if they find somebody in the act of stealing property). Where the elimination of a risk cannot be achieved immediately interim controls must be put in place to reduce that risk as far as practicable.

> *By way of example, there are current entrapment risks in an old treatment room. There are capital works planned in 12 months' time to address the design of the room. In the interim, the room will be fitted with fixed duress alarms, workers will carry mobile duress alarms, patients assessed as being a high risk of violence will not be treated in that room, workers will be trained in de–escalation skills and how to summon assistance, and local procedures will state that workers must enter the room after the patient and ensure the set–up of the room does not allow the patient to routinely get between the workers and the door.*

Where the hazard cannot be eliminated, then the following must be considered (in order of most to least effective):

1. Change or reduce the exposure to the hazard by one or a combination of the following
   a. Substituting the hazard with a safer alternative. For example:
      - transferring a client to a unit that is better able to manage disturbed behaviour
      - attending to a client in a community health centre rather than in the client's home.
   b. Isolating the hazard from people. For example:
      - having secure staff areas that patients cannot easily enter
      - providing time out rooms for patients experiencing behavioural problems
      - designing counter heights / widths so that workers cannot be easily assaulted over the counter
      - physical barriers between workers and others, such as desks or screens.
   c. Reduce the risk through engineering controls. For example:
      - access control systems like swipe access or automatic door locking / unlocking systems to limit areas to staff only
      - increased lighting on paths.
2. Minimise any remaining risk using administrative controls. For example:
   - supervision, information
   - ensuring workers have the skills outlined in NSW Health policy *Violence Prevention and Management Training Framework for the NSW Public Health System*
   - Code Black response procedures
   - pre home visit risk identification checklists
   - effective clinical protocols for the diagnosis and treatment of patients with potentially violent expression of symptoms
   - escort workers to vehicles at the end of evening shift
   - structured environmental scanning, where in a potentially violent situation eg paramedic assaults, and supported withdrawal from scene.
3. If risks remain, minimise the impact on people by using personal protective equipment. For example:
   a. wearing a personal duress alarm
   b. access to portable radio / mobile / satellite phones when working in the community.

Where a single measure is not enough to effectively minimise risk, a combination of the above measures must be used.


HIGHEST
MOST
Eliminate risks
Substitute the hazard with a safer alternative
Isolate the hazard from people
Reduce the risks through engineering controls
Reduce exposure to the hazard using adminstrative controls
Use personal protective equipment
Level of health and safety protection
Reliability of control measures
LOWEST
LEAST

1.2.7 Identify priority workplaces

Within NSW Health Agency workplaces there will be a number of priority areas where the likelihood of security related incidents occurring may be increased. These areas must be identified and priority given to ensuring effective risks controls are in place and being monitored.

These areas may include emergency departments, maternity units, mental health services, oral health clinics, intensive care units, high dependency units, community health services, drug and alcohol services, aged care wards, pharmacies and car parks.

However medical and surgical wards can experience increasing security related incidents and where this is the case they must be identified as a priority workplace.

1.2.8 Monitor and review your security risk and security risk controls:

To ensure that the outcomes from the security risk management process continue to effectively address security hazards, monitoring and evaluation of risk control strategies must be undertaken.

Security risk monitoring and review involves:

- consulting with workers located in that workplace to assist in determining whether controls are working or if they are introducing new hazards or risks
- regularly examining the workplace, equipment and systems of work for new risk factors and taking appropriate and effective action where they are identified
- reviewing existing risk assessments and any measures adopted to control the risk
- monitoring implementation and taking action to ensure compliance eg wearing of duress alarms
- carrying out inspections and audits to assess compliance with legislation, Codes of Practice Australian Standards and NSW Health policy
- examining workers compensation records and incident reports (eg from the incident management system (ims+) and other security reporting systems) to assess the effectiveness of actions taken
- reviewing local procedures and protocols for continuing relevance and effectiveness
- ensuring safety equipment continues to effectively meet the needs/purposes for which it was initially provided
- reviewing responses to violent incidents, including the duress response.

NSW Health Agencies must review an existing risk assessment and any measures adopted to control the risk, and provide feedback to workers on changes, whenever:

- there is evidence that the risk assessment requires review, eg an incident occurs
- injury or illness results from exposure to a hazard to which the risk assessment relates
- a change is proposed in the place of work, systems of work, equipment or in work practices or procedures to which the risk assessment relates
- new information about the risk becomes available
- there are concerns raised by workers or other stakeholders at the workplace.

Risk assessments and control strategies must be reviewed on an agreed basis depending on the level of risk to ensure they remain relevant and effective. For example, a higher risk matter requires a review at 3-monthly intervals if an earlier review has not been triggered by the above reasons.

Recommendations for change must be implemented and monitored.

1.3 Ensure hazards and incidents are reported, managed and investigated

Effective hazard and incident reporting, management and investigation provide information to assist with monitoring, reviewing and evaluating security programs by highlighting new risks and identifying the effectiveness of current control strategies.

The information reported must be assessed and strategies to address the risk implemented in a timely way. This action must be completed in consultation with affected workers and their HSRs and communicated to relevant workers.

1.3.1 Hazard reporting

As an essential part of risk management, all workers must be encouraged to report problems/hazards as soon as they notice them using the appropriate local process eg notify your supervisor and enter into ims+

Appropriate action to address hazards must be taken immediately.

1.3.2 Incident reporting

All security related incidents and near misses must be reported and recorded using the appropriate local format (eg ims+).

Depending on the nature of the incident, it may need to be reported to the NSW Health Agency Chief Executive, the Ministry of Health (refer to NSW Health Policy Directive Incident Management) or external agencies such as the NSW Police or SafeWork NSW (refer to the NSW Health Policy Directive *Work Health and Safety: Better Practice Procedures).*

1.3.3 Incident management

All security related incidents need to be efficiently and effectively managed (Refer to Chapter 29 Code Black arrangements and Chapter 30 Effective Incident Management in this Manual).

1.3.4 Incident investigation

The most effective way to minimise the recurrence of a security incident is to determine why it happened (ie identify the contributing risk factors) and take steps to minimise its recurrence (ie eliminate the risk or develop and implement control strategies).

Incident investigations need to:

- be undertaken by managers in consultation with those involved and relevant experts including clinicians, WHS and security personnel as appropriate
- specifically, where the incident involves a patient and /or their family, be conducted by a multidisciplinary team that includes clinical, WHS and security personnel
- be carried out promptly
- be conducted in a supportive and non–judgemental way
- focus on identifying the underlying root cause/s and contributing factors
- not apportion blame
- focus on system breakdowns and identifying control measures to prevent recurrence
- canvas all sources of relevant information (eg witnesses, incident reports, relevant work policies and procedures, the working environment, equipment used, level of supervision at the time, relevant training provided and expert advice)
- include an operational review if relevant
- investigations should consider an incident from all perspectives and may draw upon the expertise of reviewers with a lived experience of the conditions or incidents being reviewed
- result in clear recommendations to senior management to address the causes and where possible to prevent a recurrence – recommendations can be clinical and non–clinical in nature
- result in feedback to affected workers.

It is crucial to the success of the investigation process that it results in clearly defined recommendations to prevent a recurrence, identifies resource implications (if any), identifies who is responsible for the implementation of the recommendations and outlines appropriate time frames.

Further information can be found in Chapter 30 Effective Incident Management in this Manual.

1.4 Ensure effective and timely injury management and worker support occurs

The loss or disruption that can result when an incident occurs in the workplace is multiplied when that incident leads to an injury to a worker or a patient/visitor. A comprehensive, effective security program must therefore minimise the risk of and severity of injuries by effective incident response and address what needs to happen if an injury occurs.

NSW Health Agencies can reduce the effect of a workplace injury or illness for the injured worker and the workplace with the implementation of early intervention and early return to work strategies.

See Chapter 30 Effective Incident Management for additional standards to support workers post incident.

NSW Health Policy Directive *NSW Health Policy and Procedures for Injury Management and Return to Work* provides policy and guidelines for the management of workplace injuries.

NSW Health Agency compliance with the standards set out in this chapter relating to the risk management systems and frameworks in place are audited as part of the *NSW Health Work Health Safety Audit.*

Application of these systems and frameworks to the security risk context is audited under the *NSW Health Security Improvement Assessment Tool Audit*.

2. Responsibilities

The *NSW Ministry of Health,* as the system manager, is responsible for setting the statewide policy framework and standards for security risk management and monitoring policy/standard implementation and effectiveness. The framework for risk management can be found in the *NSW Health Enterprise-wide Risk Management Policy and Framework*.

Underpinning what we do are the values we apply to our work as described in the *NSW Health Workplace Culture Framework* which embodies our CORE values (Collaboration, Openness, Respect and Empowerment) and helps us strive to make continuous improvement in workplace culture.

Local Health District Boards and individual Board members must exercise due diligence to ensure the NSW Health Agency meets its obligations under NSW Work, Health and Safety (WHS) and NSW Security Industry Legislation, including by taking reasonable steps to ensure:

- they maintain up to date knowledge of occupational violence and aggression and security related risks as they pertain to the NSW Health Agency
- the NSW Health Agency has and uses appropriate resources and processes to eliminate or minimise security related risks
- the NSW Health Agency has systems in place to identify, assess and eliminate or control security related risks
- they receive relevant information on security related risks and how they are being addressed, including advice on compliance with the standards outlined in this Manual
- they review information provided to them on security related risk matters and take appropriate action to resolve issues or concerns.

Clearly defined and allocated responsibilities are an essential element of an effective security governance framework and must reflect the following:

Chief Executives must ensure:

- the resourcing, development, implementation and maintenance of effective security risk management within their NSW Health Agency. This must be based on a structured, ongoing risk management process, consultation, appropriate documentation and record keeping and regular monitoring and evaluation. The risk management process must be undertaken by those with the necessary subject matter expertise.
- effective security governance is in place, is utilised and is effective
- all managers and workers are aware of their security risk management related responsibilities ie security is everyone's responsibility
- that information on security risk management, and actions to address identified areas of risk are reported to the Board, including the Risk and Audit Committee
- that NSW Health security risk management standards, as set out this Manual, are met
- workers are consulted in the development and implementation of security procedures and when determining and purchasing equipment
- Ministry reporting requirements are met, particularly in relation to reporting and management of incidents
- legislative requirements, including when employing or engaging security staff, compliance with the *Security Industry Act 1997 and Regulation 2016* in nominating a suitably qualified and experienced person as a 'nominated person' for the purpose of holding the Master License and its associated responsibilities
- workers are provided with the necessary skills to prevent and manage security/aggression/violence related issues.

The following security risk management responsibilities apply within NSW Health Agencies. They must be formally delegated to each of the relevant NSW Health Agency executives and relevant workers, be captured in role descriptions and measured as part of performance reviews and in performance management plans:

Master Licence holders are responsible for:

- provision of or hiring licensed security staff to carry out security activities in your health agency
- ensuring the conditions of the master licence are upheld. These conditions are outlined at this link
- the licence holder must be involved in the day to day conduct of the organisation's security activities. The master licence holder may do this by regular communication with security managers and other relevant staff if no security manager is in place.

Facility Managers are responsible for:

- identifying individuals responsible for security administration within their facility
- ensuring the ongoing implementation of an effective security program, which is based on a structured, risk management process, consultation, appropriate documentation and record keeping and regular monitoring and evaluation, including local compliance with the standards set out in this Manual
- ensure all crimes and suspicious activity are reported to police. All physical assaults and serious threats of assault must be reported to the Police and an event number obtained
- ensuring integration of clinical and security teams and multidisciplinary responses to incidents and risk assessment
- ensuring the Chief Executive, Risk Managers, Security Master Licence holders, and where necessary external authorities such as Police and SafeWork NSW, are advised of security related incidents, as required under local procedures and the NSW Health directive *Work Health and Safety: Better Practice Procedures*.

Service Directors/Department Managers/Facility Security Administrators/Team Leaders/Supervisors are responsible for:

- monitoring and ensuring compliance with NSW Health security policies and local procedures including integrating security risk management into clinical practice, where appropriate
- consulting with workers and their health and safety representatives (HSRs), WHS and security staff, relevant unions and other duty holders on security matters
- keeping workers informed of personal and property security policy and procedures, and management's action in response to hazard and incident reports
- identifying and assessing areas where personal and property security can be improved in consultation with workers
- responding to incident and hazard reports including investigation of incidents and maintenance/ replacement of security equipment
- implementing risk control strategies in accordance with risk assessments and alerting senior management where the necessary controls are outside of their authority to implement
- identifying training needs for workers, consult on training and ensuring training is provided and attendance documented
- reporting security related incidents as required under local procedures.

Contract managers are responsible for:

- ensuring mechanisms are in place for managing shared WHS responsibilities (including consultation and processes for escalation of issues), and particularly for:
  - property leasing and maintenance
  - procurement processes (including procurement of security services
  - other contracts that include relevant security management controls consistent with this Manual
  - ensuring that external service providers hold the appropriate security licence eg a NSW 2B/2C security licence when selling or installing CCTV or other security equipment or a NSW 2A security licence if providing recommendations on security risks and controls.

Security staff including senior security staff and Health and Security Assistants, in addition to general worker responsibilities, are responsible for:

- maintaining a current 1A security licence and first aid certificate
- completing all the required legislative actions associated with their 1A security licence, including:
  - signing on/off on the security register at the commencement and end of their shift (see master licence requirements at this link)
  - recording all incidents of restraint in the NSW Health Agency incident register (ims+).
- ongoing professional development including maintaining current knowledge of relevant legislation appropriate to the security industry, and maintaining current knowledge of health care security requirements, e.g. patient restraint policy and techniques.

For further information on the role of security staff refer to Chapter 14 of this Manual.

All workers (clinical and corporate) are responsible for:

- complying with policies and procedures for personal and property security
- using the security equipment provided, appropriately and correctly eg duress alarms
- reporting all incidents and potential security risks to management in accordance with procedures. Including reporting in the incident management system (IMS+)
- participating in consultation and training on personal and property security matters
- not knowingly placing themselves or others at risk.

Health infrastructure oversees the planning, design, procurement and construction of health capital works in NSW and are responsible for leading:

- the delivery for capital investments valued $10 million and above
- the planning, procurement, delivery and evaluation for health facility investments valued at $10 million or greater
- stages 1–4 of the facility design/building process as the delivery arm for NSW Health, working in partnership with a range of stakeholders, including NSW Health Agencies as the client.

3. Security Risk Management in the Planning Process

Policy

NSW Health Agencies are required to ensure that the implications for security risks, controls and security operations are considered and documented in all organisational planning and decision making.

All plans and proposals including but not limited to construction/refurbishment of premises, changes to equipment, and changes to service plans and systems of work (such as models of care) must identify security risks and controls.

Planning documentation must record the consultation undertaken with workers, shared duty holders and experts in identifying and assessing risks, and in determining risk control options.

Standards

Planning takes place at all levels of a NSW Health Agency across all disciplines and workplaces (eg District, Facility and Unit levels). When planning and making the resulting decisions that affect workers, visitors, patients and others, and/or the place of work eg accommodation, work practices, purchasing equipment, security risk and operational issues must be considered.

Other plans that must include consideration of security risks, controls and where necessary, security operations include:

- business continuity planning
- disaster/emergency planning (including business continuity planning)
- procurement processes, including processes for procuring services, premises, equipment, furniture, fixtures and fittings see Chapter 4 Health facility Design and Chapter 15 Designing out Security Risk in the clinical environment for more detail)
- WHS/security improvement and management planning
- workforce, training and finance planning.

Consultation during planning provides improved and sustainable outcomes

Security staff, health and safety staff and affected workers (and where relevant their health and safety representatives (HSRs) or representative bodies such as unions) must be consulted when undertaking relevant planning activities. Consider including consumers/patients and carers when consulting about service planning or facility design planning. This includes all phases of facility design.

Other Resources:

This Chapter must be read in conjunction with NSW Health Policy Directive *Enterprise Wide Risk Management Policy and Framework* and *Work Health and Safety: Better Practice Procedures*.

4. Health Facility Design

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all reasonably foreseeable security risks are identified, assessed and eliminated where reasonably practicable, or where they can not be eliminated, effectively minimised as part of facility planning, design and refurbishment.

The standards outlined in the Australasian Health Facility Guidelines (AusHFG), Crime Prevention Through Environmental Design Principles (CPTED) and this Manual must be referenced and compliance achieved during all stages of the facility planning, design or refurbishment/construction process. This includes security considerations related to any temporary accommodation (ie decanting of workplaces during construction) or other temporary arrangements, eg access to wards, offices, parking and contractor access.

Work health and safety (WHS), risk management, security staff, and worker representatives, including health and safety representatives (HSRs), must be consulted during the planning and design of new facilities or the refurbishment of existing facilities.

Where changes are being made to the local working environment NSW Health Agencies are required to ensure, in consultation with workers and those involved in the planning and building, that all reasonably foreseeable security risks are identified, assessed, eliminated where reasonably practicable or effectively minimised.

Prior to finalising plans for new or redeveloped hospital and health facilities, Health Agency Chief Executives must ensure that the design of the facility has undergone a security review and meets the AusHFG and NSW Health security standards, set out in this Manual.

Where an AusHFG or NSW Health security standard has not been applied, the Chief Executive must confirm that a documented risk assessment, meeting the requirements of Work Health and Safety legislation, has been completed.

When purchasing fittings and equipment, security risks relating to the relevant workplaces must be evaluated as part of a WHS risk assessment process.

Standards

4.1 The AusHFG have been adopted by NSW Health and apply to all aspects of facility design

The AusHFG were developed to:

- establish minimum acceptable standards for the design of health care facilities
- achieve affordable solutions for the planning and design of health care facilities
- maintain public confidence in the standard of health care facilities
- provide general guidance to designers seeking information on the special needs of typical health care facilities
- promote the design of health care facilities with regard for the safety, privacy and dignity of patients, workers and visitors
- eliminate design features that result in unacceptable practices or risks
- update guidelines to meet current clinical practices and standards
- minimise recurrent costs and encourage operational efficiencies.

AusHFGs are not intended to restrict innovation that might improve performance, outcomes or safety/security. There are processes in place within NSW Health to manage instances where a facility determines the need to adopt a design standard that differs from the AusHFG standard. Evidence required as part of seeking a variation includes a WHS/Security assessment of the impact of the variation.

The NSW Health policy dealing with facility design and construction is in the *NSW Health facility planning process.*

4.2 Application of the standards in this Security Manual impacting on facility design are mandatory

The Standards set out in this Manual are in place to address security related risk that has been identified across NSW Health. The most common security related risks that can be addressed through design are:

- violence
- entrapment
- concealment
- isolation of workspaces
- unauthorised access or egress
- theft and property damage
- unrestricted movement through workplace
- opportunity to use equipment as weapons.

Standards designed to address these risks (and a range of other risks) are set out in the Chapters in this Manual and therefore must be incorporated in all facility design.

Consideration of the design of space to promote recovery and minimise trauma to patients/clients should be considered as this may reduce the risk of aggression.

Clinical areas should be designed to support the therapeutic intent and be culturally safe spaces but in addition to that they **must** be safe for workers.

4.3 Consultation on local work environment design improves outcomes

Managers have a role in enhancing the security of people and property when determining the layout of the furniture and equipment in their immediate workplace or unit eg the layout of desks, filing cabinets etc.

Prior to engaging in any significant reorganisation of the physical working environment managers must consult with their workers, and where relevant their representatives such as HSRs or representative bodies) to ensure that all security related risks are identified, assessed, eliminated or effectively controlled. Subject matter experts such as security managers and WHS staff must also be consulted.

Site specific security infrastructure that is installed using a standard specification, as identified by a risk assessment, are to be considered where they are consistent with policy and must be incorporated where practicable.

4.4 The principles of CPTED are to be applied to all facility design

CPTED is a multidisciplinary situational crime prevention strategy that focuses on the design, planning and structure and use of a built environment.

The CPTED approach relies on the ability of the environment to influence offender decisions that precede criminal offences and is largely limited to building perimeters and grounds. It has limited application to risk of violence from within health services particularly where the risk has a clinical origin. CPTED is therefore only one aspect of designing for security risk reduction.

All new or refurbished facilities must reflect the CPTED principles, during the design and building phases. The principles must be applied to the design and layout of indoor as well as outdoor environments.

CPTED principles fall into four broad categories: territorial reinforcement, surveillance, space management and access control. They apply in particular to the way that buildings and their surroundings are designed but also have an application in determining the most appropriate layout of individual work areas.

4.4.1 Territorial reinforcement

This draws on the territoriality principle and assumes that people can be encouraged to express feelings of ownership over work areas.

It includes maintaining the space so that it has a clean and well cared for appearance, using actual and symbolic territorial markers such as signage and site maps and the placement of activities to avoid conflict.

Examples of this principle in design include:

- allocating clear ‘staff only’ areas making it more likely that workers will pay more attention to the area and note an intruder
- clearly separated restricted areas (eg by signposting or locking) to reduce the likelihood of others entering the area and does not give intruders an excuse to be there (eg that they were not aware it was a restricted area)
- using materials/colours/textures to differentiate areas
- avoid creating too many ways to enter a space to reduce confusion.

This principle also applies to the facility precinct being clearly delineated from the rest of the community by fences, garden borders, signs etc.

4.4.2 Surveillance

Natural surveillance is the principle where people feel safe in public areas where they can see and be seen, and interact with others, particularly people connected with that space.

This principle refers to the way in which working areas of buildings have been designed (including building layout, orientation and location; the strategic use of design; landscaping and lighting) so that priority areas are overseen and watched by other workers going about their normal business.

Examples of this principle in design include:

- pathways to car parks and other outbuildings on a hospital campus are designed to provide a full view of the users and are overlooked by offices or wards
- co-locating high activity 24/7 spaces with lower activity spaces to allow for surveillance over the quieter spaces and avoid isolation
- eliminating blind spots in buildings and grounds'.

Technical/mechanical surveillance uses measures such as camera surveillance, which is more fully covered in Chapter 13 Workplace Camera Surveillance of this Manual.

Formal (or organised) surveillance is achieved through using security or other onsite supervision at high risk locations. This is covered more in Chapter 14 Role of security staff.

4.4.3 Space / activity management

This draws on the correlation between the feeling of safety experienced by people in a space and the level of maintenance and upkeep of that area. Well maintained spaces encourage frequent use allowing for natural surveillance and send a message that the facility workers and patients care about this space. Well designed spaces also improve the human experience. A run down structure with graffiti or a space that is dark and infrequently used will appear neglected and attract criminal activity and offenders.

Examples of this principle in design include:

- design spaces with materials, fixtures and fittings that are strong, hard to break and difficult to be tampered with/removed
- use surfaces that are resistant to graffiti
- co-locate low activity areas with high activity 24/7 areas (avoid creating isolation).

4.4.4 Access control

This draws on the use of physical and symbolic barriers to attract, channel or restrict pedestrian access and vehicle movement. It works on the premise that making it clear, by creating either physical or symbolic barriers, where people can and can't go makes it more difficult for offenders to reach potential victims and targets.

Examples of this principle in design include:

- controlled access between public and staff or clinical areas
- minimised points of entry to a space
- installation of barriers between pedestrian and vehicular spaces. Consider planters, hedges, public art and sculptures as potential barriers in place of bollards and fences, wherever possible, to soften the geometry and create a more visually appealing health facility and environment.

5. Leasing of Property to or from External Parties

Policy

NSW Health Agencies are required to ensure, in consultation with workers, and other duty holders, that all reasonably foreseeable security risks associated with:

- **leasing property for use by NSW Health Agencies or**
- **leasing premises to external organisations**

are identified, assessed, eliminated where reasonably practicable or, where they can not be eliminated effectively minimised, that the process is appropriately documented and arrangements for security included in leases.

Properties leased for use by NSW Health Agencies must meet the requirements set out in this Manual.

Standards

5.1 Prior to leasing properties for NSW Health workers a security risk assessment must be completed

In some instances, NSW Health Agencies, as part of providing services to the community, lease premises eg located within shopping centres, office blocks, community halls, schools or other premises remote from their community health team base.

In all the above mentioned scenarios any security related risks must be identified, assessed and controlled to ensure the security of workers, patients and clients of the services and the public is maintained. There is a shared obligation to manage the risks related to safety and security when organisations are leasing property (refer to Section 3 below). The risk assessment must be completed in consultation with workers who will be working in the leased properties.

As such, NSW Health Agencies must undertake an assessment of security risks prior to entering into any leasing arrangements. Lease arrangements must specify responsibilities for aspects of security such as the installation and maintenance of a range of security features (eg security grills, locks, alarms, lighting).

Where NSW Health Agencies lease premises from external organisations the following standards must be implemented, unless a risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk).

5.1.1 Factors to be considered as part of the security risk assessment when leasing from an external organisation:

NSW Health Agencies must assess, as a minimum, the following factors:

Suitability of the property

- geographical location in terms of safety and security issues eg is it isolated, driving distances, remoteness, proximity to licenced premises or other businesses/ services that may pose a security hazard, and access to emergency or security services
- crime risk/business security assessment of the locality. Police can provide statistics and advice, the NSW Bureau of Crime Statistics and Research (BOCSAR) is another source of information
- type of service to be provided from the premises including the number of workers to be working from the premises, likely clientele, hours of operation and associated security requirements
- security assessment of the property eg suitability of locks, alarms, interior and exterior lighting, security doors and screens, ability to separate and control access between public and clinical or staff only areas, absence of design that allows for entrapment or concealment, the ability to use telecommunications equipment (including equipment designed to alert a Code Black/duress situation)
- availability of safe parking for workers and patients, including during and after hours as relevant. Consideration must include the proximity to the premises and hours of operation in relation to parking location, eg will workers be arriving/departing or packing/unpacking vehicles in the dark
- public transport arrangements
- location relative to major roads and transport routes, eg an isolated location may be more attractive to criminals

- security of approaches, eg well lit, line of sight particularly access to parking and building egress, no potential hiding places
- will field communication technology work eg reception for mobile phones, remote and hard–wired duress alarms, tablet devices and laptops etc
- security services able to be accessed. If there are no current security arrangements that can be accessed, providing a service from that location must be reconsidered
  - proximity of local police services and/or a duress response team and their hours of operation relative to service operation
  - security already provided (eg shopping centre security staff) and the availability of these arrangements as part of the lease and that the security is of the whole building and not just the tenancies.
- any restrictions by the lessor/property owner on changes that can be made eg would the property owner allow the installation of security grilles, camera surveillance, duress alarms or approved locks
- who is responsible for prompt property maintenance and the hours it is available eg 24hrs glass repair
- what are the current access controls for the property eg: basic lock–up.

Business continuity planning

Business continuity plans must account for any potential loss of critical security measures. This would include planning for loss of communication, loss of electricity that may affect electronic access control or duress measures, processes for emergency repairs, loss of security services.

5.2 Prior to leasing NSW Health Agency property to an external organisation, a security risk assessment must be completed

External organisations may wish to enter into leasing agreements with NSW Health Agencies eg pharmacies, newsagents, gift shops, food outlets, banking services in hospital or car parks or hiring out lecture theatres, conference rooms etc.

In all the above mentioned scenarios any security related risks must be identified, assessed and controlled to ensure the security of workers, patients and clients of the services and the public is maintained. There is a joint obligation to manage the risks to safety and security when organisations are leasing property. The risk assessment must be completed in consultation with workers who will be affected by the change.

As such, an assessment of security risks must occur prior to entering into any lease arrangements. Lease arrangements must specify responsibilities for aspects of security such as the installation and maintenance of a range of security features (eg security grilles, locks, alarms, lighting) and who provides a security response when that is necessary.

5.2.1 Factors to be considered as part of the security risk assessment when leasing to an external organisation:

NSW Health Agencies must assess, as a minimum, the following factors:

Nature of the Business

- the type of business wanting to lease the premises and the likely security issues which may arise from the type of service provided eg pharmacies/drug theft, banking/armed robbery or ram raid (refer to Attachment A), food outlets/large volumes of people
- the proposed hours of operation.

Placement of the Business

- the most appropriate placement of the business within the facility eg if a financial business it may need to have an external door for cash delivery and pickup, or if property placement has external access so public do not have to access through health facility
- CPTED principles – refer to Chapter 4 Health facility Design standards
- if the tenant is a pharmacy, then there needs to be agreed arrangements for secure storage of drugs that comply with legislation and NSW Health policy and guidelines. That is, a drug safe attached to a load bearing wall and meeting the requirements of the *Pharmaceuticals Act*.

5.3 Location of ATMs to prevent theft

Where Automatic Teller Machines (ATMs) are being installed in NSW Health Agencies consideration must be given to the risks associated with armed hold up, break in, attempted ram raid and explosion style thefts.

An effective control strategy is to eliminate access to the ATM by vehicles, therefore priority must be given to placing the ATM in an area that is not visible from outside the facility. A risk assessment relating to the placement of the ATM must be conducted to ensure appropriate risk control strategies are put in place. To assist NSW Health Agencies a simple Risk Assessment guidance tool is provided at this link.

In relation to controlling the risk of explosives being used to access ATM content, consideration must be given to ensuring ATMs are located in an area that does not have any concealment points.

Security Arrangements

- determine the role of NSW Health security staff and what they will and will not respond to. Provide this information to relevant workers (including security staff)
- the security arrangements that must be provided by the lessee business eg if banking they employ their own security officer. The lease needs to clearly define what security arrangements will or will not be provided by NSW Health Agency security staff
- the procedures that need to be implemented by the business eg firearms security, cash in transit and armed escorts.

5.4 Health Agencies must consult, co-operate and co-ordinate activities with other duty holders

Additionally, where there is a shared duty as outlined in section 16 of the *NSW WHS Act*, NSW Health Agencies are required to consult, co-operate and co-ordinate activities with all other persons who have a work health or safety duty in relation to the same matter, so far as is reasonably practicable.

This includes undertaking a security risk assessment and implementing the required controls to manage the identified security risk. NSW Health Agencies must ensure that other workers on NSW Health property and NSW Health workers working in externally leased properties are provided with a work environment that is compliant with the standards set out in this Manual.

Leasing agreements must include the provision for the lease to be ceased if safety and security issues remain unmanaged.

NSW Health Agencies must ensure that arrangements on how the mandatory NSW Health *security improvement audits* are agreed with other duty holders where there is leased property.

6. Security Arrangements for Patients in Custody

Policy statement

NSW Health Agencies are required to ensure, in consultation with workers, Corrective Services NSW, Youth Justice NSW, Department of Home Affairs (Australian Border Force) and NSW Police Force (external Agency) and other duty holders that:

- **all reasonably foreseeable security risks associated with patients in custody are identified, assessed, and, where reasonably practicable, controlled**
- **effective procedures for safely managing patients in custody, including eliminating or minimising any associated security risks, which are consistent with the operational controls of the relevant external Agency, are developed and implemented**
- **the procedures are appropriately documented and communicated to relevant workers**
- **planning for patients in custody must include both clinical and security stakeholders.**

Where a Memorandum of Understanding (MOU) has been established with another external Agency they will set out all Agency roles. Local procedures must be developed that are consistent with the provisions set out in the MOU.

Note: In line with the recommendation set out in the Final Report from the review *Improvements to Security in Hospitals*, the Ministry of Health will seek to progress an MOU with the Department of Home Affairs. In the interim health facilities receiving patients from detention facilities must work with local Department of Home Affairs workers to develop procedures to ensure the safety of NSW Health workers and be consistent with the role of NSW Health workers.

Standards

For the purposes of this Chapter reference to ‘external Agency’ means reference to either NSW Police Force, Corrective Services NSW or Youth Justice NSW.

The following standards must be implemented unless a risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk. These standards are:

- develop facility protocols for managing patients who are in the custody of another external Agency while in the facility, including when there is a need to transfer a patient in custody if they cannot be safely managed at that facility
- protocols must provide a clear role delineation between the role of workers of the NSW Health Agency and the external Agency, and must reflect any current MOUs
- workers from these external Agencies must be made aware of any relevant health facility protocols to be followed when inmate/detainee patients (custodial patients) are in the facility. This may be achieved by providing escorting officers with written information upon their arrival at the facility
- NSW Health Agency workers must advise escorting officers from external Agencies upon arrival of local evacuation plans and places where a custodial patient can be taken in the event of a fire, blackout or other emergency
- procedures are in place to ensure appropriate NSW Health Agency workers (eg the facility manager, security manager and security staff) are made aware of the patient admission and any potential risks associated with their admission. Advice on risks will be provided by escorting officers
- all enquiries from the public and the media are channelled through to the relevant external Agency.

6.1 Corrective Services NSW custodial patients

An MOU has been established with Corrective Services NSW (CSNSW) in relation to the care of custodial patients in Health Agencies. The MOU can be found at this link.

The following principles underpin the MOU and must be reflected in local procedures:

- the safety of workers must remain a priority at all times
- custodial patients must be treated with respect and dignity
- there is a commitment to working together to ensure custodial patients have timely access to appropriate care and treatment in a safe environment
- there is a commitment to respond to incidents and provide services in a manner that is consistent with the custodial patient's clinical and safety needs and the circumstances at the time
- maintenance of confidentiality with regard to personal and clinical information relating to custodial patients
- age, gender, religion, culture, language and other significant factors must be recognised and accommodated whenever possible in the circumstances
- custodial patients are to be given the same treatment and consideration as extended to any other patient when they are admitted to a health care facility for care and treatment
- CSNSW and NSW Health workers must always exercise care and diligence to the best practice standards
- security and supervision of custodial patients who are admitted to a health care facility for care and treatment remain the responsibility of CSNSW Officers undertaken in line with CSNSW protocols
- NSW Health retains responsibility for decisions relating to the running of the health care facility where a custodial patient is in attendance
- compliance with any reasonable directions given by each Party from time to time; and
- a commitment to a robust governance structure to support the operational effectiveness of the MOU and support early and timely consultation with workers and issue resolution.

6.2 Youth Justice custodial patients

There is not currently an MOU that covers Youth Justice NSW (YJNSW) detainees. The following provisions and those set out for escorting YJNSW officers in their *Movement Out – hospitalisation (emergency & overnight stay)* procedure and the *Escorted Absences* procedure must be reflected in NSW Health Agency procedures as follows:

- the safety of workers must remain a priority at all times and information that may relate to potential risk to the safety of workers from either Agency must be shared
- all detainee patients from YJNSW are to be escorted by YJNSW Officers. The Centre Manager of a Youth Justice centre can determine the number of YJNSW officers required
- the custodial patient must, wherever possible, remain in the vehicle until called, if there is a wait on arrival to an appointment
- no custodial patient is to be left under the supervision of any person other than officer/s of YJNSW (the number of officers to be consistent with the custodial patient's criminal history and risk level)
- a custodial patient is not to make telephone calls without direct approval of the patient's Youth Justice Centre
- custodial patients admitted to a health facility for medical treatment are to be given the necessary considerations as extended to any other patient. Personal matters pertaining to the detainee patient are to be treated with strict confidentiality by NSW Health Agency workers
- security needs are to be appropriately instituted to ensure custodial patients' medical needs and the safety of workers, other patients and visitors are not compromised
- relieving YJNSW Officers are to identify themselves to the nurse in charge. Their identity is to be confirmed with the outgoing YJNSW Officer. Health facility workers responsible for the custodial patient's care must identify themselves to the attending YJNSW Youth Officer/s
- the name and contact telephone number of the YJNSW Officer's duty manager/centre manager is to be given to the health facility administration in case of an emergency or any infringement of facility protocol
- health facility workers are to be informed when the number of YJNSW Officers is reduced or increased
- YJNSW Officers are to ensure that the custodial patient does not engage in offensive or violent behaviour while at the facility
- YJNSW Officers are not to rely on health facility workers including nursing staff or security staff to supervise the custodial patient regardless of reason or length of time
- clinical staff are to be advised before handcuffs are removed if the custodial patient has a history of violence or escape. The handcuffing of a custodial patient is a decision best made by the centre manager of the Youth Justice centre in which the custodial patient is normally held
- custodial patient medical care is to be left to the health facility's clinical staff

- custodial patients must be supervised or escorted at all times by a YJNSW Officer unless the patient is:
  - receiving medical imaging
  - giving birth in the delivery suite
  - undergoing an operation in the operating suite
  - being barrier nursed, or reverse barrier nursed.

  Note: In the abovementioned circumstances YJNSW Officers will remain immediately outside of the examination/operating room but in a line of sight. If an examination room or radiology unit has more than one exit, YJNSW Officers will not leave an exit unsupervised unless the custodial patient's condition would prevent escape
- female YJNSW Officers are to supervise female custodial patients who are outpatient or in–patient for any obstetric and/or gynaecological matter. Male YJNSW Officers can only attend if female YJNSW Officers are unavailable
- YJNSW Officers are to eat their meals in the custodial patient's room, one at a time when there are two officers on duty. If YJNSW Officers are not required to be with the custodial patient, and are on a break, they must have access to the same amenities as NSW Health Agency workers
- access to custodial patients is to be controlled at all times – allowing as few entry and exit points as practicable
- approval from th e Centre Manager of the Youth Justice centre needs to be given before a custodial patient can receive visitors. YJNSW Officers will screen visitors and enforce any restrictions
- visits from legal, welfare and religious persons are to be allowed after verifying their identity with the YJNSW Officers
- custodial patients are to have access to television hire, at their own cost, with the approval of the Centre Manager of the Youth Justice centre
- gifts intended for the custodial patient will not be accepted
- the nurse in charge is to be advised immediately of problems with visitors. Security staff will then be contacted straight away. YJNSW Officers have the right to refuse or terminate visits
- complaints by health facility workers concerning a breach of protocol can be made to the nurse in charge or responsible manager. Custodial patients can also complain to the Patient Advocate (if the facility has one) on issues related to their care and treatment by health facility workers.

6.3 Patients in the Custody of Police

An MOU has been established with the NSW Police Force. The MOU sets out the principles which guide how agencies will work together when delivering services.

This MOU covers situations where a person is in distress in the community and requires transportation to a Declared Mental Health Facility under the provisions of the *NSW Mental Health Act*, where patients are in the custody of police and require medical assistance and where health facilities require the assistance of NSW Police Force to manage a public safety issue within a health facility.

The MOU can be found at this link.

Ensuring the safety of workers in all agencies remains a priority in the MOU, as well as the following principles and these must be reflected in local procedures:

- there is a commitment to ensure that people are treated with dignity and respect and that services are provided in a confidential environment
- there is a commitment to respond to incidents and to provide services in a manner that is least restrictive, consistent with the person's clinical and safety needs and the circumstances at the time
- there is a commitment to work together to ensure that people with mental illness have timely access to appropriate care and treatment in a safe environment
- every effort will be made to involve people with a mental illness or mental disorder and their carers where relevant, in the development of treatment plans and recovery plans and to consider their views and expressed wishes in that development. This includes obtaining the person's informed consent when collaboratively developing treatment and recovery plans, monitoring their capacity to consent and supporting those who lack capacity to understand their plans
- there is a commitment to respond to people in a mental health emergency with the same urgency as a physical health emergency
- age, gender, religious, cultural, language and other significant factors must be recognised and accommodated if possible in the circumstances
- for people with a mental illness, care and treatment must aim to support the person, wherever possible, to live, work and participate in the community
- all interventions will be in keeping with the provisions of the *NSW Mental Health Act*
- there is a commitment to a governance structure to support the operational effectiveness of the MOU and early and timely issue resolution. An appropriate structure for this is the local MOU committee.

6.4 Forensic patients arriving from a NSW Health mental health facility (including the Justice Health Forensic and Mental Health Network)

Forensic patients are people found to be proven to have committed an act but are not criminally responsible due to mental health impairment or cognitive impairment; correctional patients, sentenced and remanded inmates who become mentally ill while in custody and require treatment in a mental health facility; or civil patients: persons who require care in a high security environment.

In some circumstances forensic patients are admitted to or require medical attention in an external healthcare facility. They are not held in Correctional Centres so are not within the custody of Corrective Services NSW, NSW Police Force or Youth Justice NSW.

The following is to be reflected in local procedures:

- the security and supervision of the forensic patient is the responsibility of escorting mental healthcare workers and medical care is the responsibility of healthcare facility
- a risk assessment of the patient will be undertaken by the workers at the mental health facility prior to transporting the patient to a healthcare facility. The risk assessment will involve consideration of the likelihood of the patient becoming violent or attempting to abscond while at the health care facility and what measures will be in place to manage this
- escorting workers must continually be with the patient and continually risk assess the patient and the environment during an external escort
- information on the risk assessment and any particular security requirements will be provided to the healthcare facility by the escorting workers from the mental health facility they are coming from
- workers at health care facilities must ensure the environment is safe and any items that are deemed unsafe are removed from access for the forensic patients, where that is possible
- forensic patients may be escorted in an arm hold or mechanical restraint device by the escorting workers. The type of restraint will be determined by the escorting workers after a risk assessment
- patient's current mental state and risk factors determine the level and amount of workers required for escorting the forensic patient
- where healthcare facility workers believe this hold or mechanical restraint device compromises clinical care for the forensic patient and does not introduce safety or security risks for NSW Health Agency workers, the escorting workers may remove this hold or device after also ensuring this does not pose an unacceptable safety or security risk
- in the event that the risk is no longer able to be managed, the escorting workers may request assistance from the health facility workers (eg security staff, code black team) or the NSW Police Force
- where workers differ in opinion as to the level of risk or requirements for mitigating any identified safety or security issues, all efforts must be made to promptly resolve the situation to avoid unnecessary delays to the provision of appropriate patient care and treatment or compromise worker safety
- where it is determined that there is a risk that the patient may engage in violence or attempt to abscond, mental health workers from the health care facility, or other appropriate persons, must accompany the person during their treatment. Treatment may be terminated if the patient poses an unmanageable risk and the patient will be returned back to the originating mental health facility.

7. Education and Training as a Strategy to address Security Risk

Policy

NSW Health Agencies are required to ensure that:

- **all workers are provided with appropriate education and training to address identified security related risk in their workplaces, including violence prevention and management training**
- **education and training are appropriate to the role of the worker, targeted to the level and type of security risk that may be encountered in the course of their work, and, in relation to violence related risk, is consistent with NSW Health Policy *Prevention and Management of Violence Training Framework***
- **education and training for workers working in areas where there are significant or high security related risks must be provided prior to commencement or as soon as possible after commencement of duties**
- **all workers who are allocated to Code Black Teams must complete all the required violence prevention and management training, as set out in NSW Health Policy *Prevention and Management of Violence Training Framework* prior to, or as soon as possible after joining the Code Black team**
- **details of security risk related education and training conducted within the NSW Health Agency are documented and maintained**
- **training is provided on an ongoing basis, and in relation to violence prevention and management training, drills are to be undertaken in order to maintain worker confidence and skills. Therefore, consultation with workers must occur to determine the frequency of drills. Records must be kept.**

NOTE: Education and training is to be undertaken in work time. Refer to the NSW Health *Leave Matters Manual* for policy on study/training leave.

Standards

The provision of appropriate, well designed education and training in association with effective instruction and supervision and other risk management strategies can assist with effectively controlling security risks.

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

7.1 There must be a training needs analysis undertaken to identify the required security risk related education and training for all workers

Integral to an effective security risk management program is the adoption of processes that identify and assess the education and training needs of workers to develop their capacity to address security risk.

A training needs analysis must occur at least every two years or when work circumstances change, to ensure education and training strategies address the actual security related learning/skill needs of the individual and meet the goals of the organisation. Such an assessment may occur at the District level but must be complimented with local workplace assessments that identify local security training needs.

This must include, but not be limited to, identification of which workers need to complete Health Education and Training Institute (HETI) determined statewide mandatory training that requires local targeting. This is based on the workers role, hazards/risks/equipment etc.

When identifying and assessing security related training needs ensure the following elements are considered:

- duties being undertaken and CORE values
- security risks associated with those duties
- work location and environment including client characteristics, where relevant
- security of premises and availability of security equipment
- access to and availability of other workers and response personnel (eg duress teams, security staff and police)
- experience in the position
- previous training and transferability to local procedures/practices
- existing security measures
- nature, frequency, severity and duration of exposure to security risks
- linkages with related local policies and procedures (eg duress response, reporting requirements)
- providing workers with the necessary skills to prevent and manage security/violence related issues and understand how experiences of trauma may impact people's behaviour and responses.

7.2 Education and Training strategies must be appropriate to achieve the required learning outcomes

A training needs analysis will assist with determining the most effective method of delivery considering the needs of the target audience and the subject matter eg restraint techniques must include a practical element. NSW Health policy may also provide standards for the delivery of education and training programs.

These education and training activities must be undertaken during work hours, as far as practicable, and must be at the NSW Health Agency expense.

Security related education and training activities must be delivered by people with the appropriate workplace training qualifications and/or subject matter expertise and experience.

Records of who attended training, the nature of the training (topics covered) and when they attended training, must be kept. Health agencies must be able to identify any gaps in attendance at training.

In determining appropriate education and training content in relation to violence prevention and management, the required competencies outlined in *Prevention and Management of Violence Training Framework* must be met. Training for security issues may also be indicated in each chapter of this manual.

7.3 Ensure education and training is provided at the required critical times

Relevant security risk related education and training must be provided:

- at induction or where possible prior to commencing duties
- on arrival at or transfer to a new / refurbished work area (eg ward induction)
- during the course of employment/engagement (ongoing drills or refresher training)
- when there are changes to work practices or procedures
- where there are new risks identified
- when new or changed activities are introduced to the work area
- when incident investigations identify new hazards and/or new controls are introduced.

7.4 Ensure the appropriate training is provided to those workers in specialised roles or with specific organisational responsibilities

In additional to the education and training strategies in place for all workers in order to address security related risk, the NSW Health Agency must identify and implement any specialised and ongoing education and training strategies or methods to increase awareness of relevant clinical conditions to ensure the following roles are able to be undertaken effectively:

- supervisors and managers
- security staff/Health and Security Assistants (including where they are required to support clinicians engaged in clinical specialling)
- fire wardens.

7.5 Evaluation of security related education and training strategies must be undertaken to assess the effectiveness in reducing security related risk

Evaluation of the effectiveness of education and training activities, both as a control measure and in meeting organisational goals, must be undertaken. NSW Health Agencies must evaluate specific activities and the effectiveness of the education and training program against pre–determined performance indicators.

The performance indicators developed by NSW Health Agencies may cover areas such as:

- increasing worker awareness of security related policies and practices
- changes to number of incidents occurring and the outcomes of those incidents
- changes to the number of hazards being identified
- reduction of the number of investigations / audit reports / SafeWork notices where lack of training was an identified issue.

NSW Health Agency performance indicators must be clear and measurable.

The effectiveness of training and education must be reviewed at least every three years **and** when:

- the outcomes of an incident/investigation indicate that review may be required
- requested by the Health and Safety Committee, Health and Safety Representative (HSR) or other relevant person/body
- there are changes to premises, equipment, systems of work, laws, or policies that impact on the training required.

Where issues are identified related to state–wide training feedback must be provided to the training developer (eg HETI). Any locally developed training materials must be consistent with this policy and must be reviewed regularly and kept up to date.

8. Ongoing review and continuous improvement of security risk management

Policy

As part of a process of ongoing review, NSW Health Agencies are required to undertake an audit of security risk management and ensure that the audit outcomes are addressed in the ongoing risk assessment actions. Audits provide an opportunity to drive continuous improvement and must be undertaken with the purpose of genuinely identifying areas where compliance can be improved.

As a minimum, NSW Health Agencies are required to:

- undertake audits of facilities within a two-year audit cycle using the *Security Improvement Audit Tool* (SIAT) to assess compliance with the requirements of this Manual, and the status of actions arising from any previous audits
- ensure necessary resources are available to ensure security audits. Audits are to be carried out by a team that includes as a minimum a person with a security licence and extensive health care security experience and a WHS practitioner
  Note: Audit teams can be supplemented with individuals with the technical expertise (acquired through training/qualification/experience relevant to the sections being audited) for those sections, as required. This may include clinical (including safety culture coordinators) or corporate workers
- ensure security audits are undertaken by a team who are independent of the facility being audited
- ensure that the results and recommendations of the audits are provided to the Chief Executive and the Board (including a Committee of the Board eg Risk and Audit Committee) as the organisation's officers and primary duty holders under WHS legislation
- ensure that the results and recommendations of security audits are provided to the NSW Health Agency risk manager and the facility/service manager
- organise security audit arrangements with other NSW Health Agencies where the activities to be audited are the responsibility of another Agency, eg HealthShare may be responsible for the linen, catering and/or security at the facility being audited
- ensure reporting to the Ministry of significant outcomes from audits, as defined and set out the NSW Health Policy Directive *Security Improvement Audits*
- ensure that a security improvement plan is developed from the security audit findings and the actions/ recommendations implemented. The improvement plan must include actions, timeframes for implementation and responsibilities, and be signed off by the facility/ service manager
- the audit results and recommendations, as well as security improvement plans are to be provided to the local Health and Safety Committee (HSC) / Health and Safety Representative (HSR) and discussed with workers in the relevant workplace.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

8.1 Governance and Reporting

The progress of security audits, including significant areas of non-compliance and improvement are to be provided through the *Work Health and Safety Executive Report* to the Ministry of Health. This information must also be provided to CEs and Boards.

For reporting requirements to the Ministry please refer to the NSW Health Policy Directive *Security Improvement Audits* for further details.

8.2 Measuring and evaluating performance as part of continuous improvement

- NSW Health Agencies must measure existing security risk management performance, evaluate progress and feed the outcomes of this process back into ongoing security risk management.
- NSW Health Agencies must ensure that a documented plan for ongoing measurement, evaluation and monitoring of security is in place.
- Whenever there is a security incident, relevant findings arising from any investigation or review must be fed back into the security risk management process and be incorporated into the security improvement plan to prevent a recurrence and ensure continuous improvement.
- Regular, relevant information on security related matters, including the outcomes of security surveys, must be provided to the NSW Health Agency risk manager, Chief Executive and the Governing Boards.

Developing performance indicators

The most obvious way of determining whether violence prevention and management strategies are working effectively is looking for any trends in the frequency and severity of incidents of violence.

It should be noted that encouraging workers to report incidents can lead to an increase in the number of reported incidents, as distinct from the number of actual incidents.

A number of sources of information can be used to develop performance indicators and these may include:

- hazard and incident reports
- Code Black response records
- Health and Safety Committee meeting minutes
- results of security audits, surveys and inspections
- near miss events and review of Root Cause Analysis reports
- first aid records
- the standards set out in this Manual and associated NSW Health policies, and *Australian Standard 4485.2: Security for Health Care Facilities.*

Security related performance indicators may include:

- data (eg physical assaults data, workers compensation data)
- patients not treated / discharged from hospital due to aggressive incidents
- percentage of workers trained in security awareness
- percentage of workers trained in security awareness within 4 weeks of commencing work
- percentage of workers trained in department specific duress response procedures
- percentage of workers who have attended violence prevention and management training (the level and timing of training will be defined by the persons role requirements, see Chapter 7 Education and Training as a Strategy to address security risk)
- daily personal duress alarm checks – percentage occurring across site
- frequency of duress response drills completed by department
- number of audits conducted and where
- timeliness of audits
- number of improvements instigated as a result of the audits
- percentage of incidents that resulted in changes or additions to clinical protocols, worker training / orientation, the environment, incident response protocols or other existing risk control measures
- on–time completion/implementation of the security improvement plan
- compliance with security policies, eg percentage of workers wearing duress alarms in locations where they are required to be worn
- timeliness of repairs/maintenance / replacement of security equipment (eg alarms, locks, cameras)
- worker interviews and / or surveys on their perceptions regarding personal safety
- degree of implementation of key aspects of the Ministry's security related policies and Chapter 26 Violence of this Manual eg percentage of patients receiving information on their behavioural responsibilities, changes to frequency of violent incident reports, percentage of assaults reported to police.

This information can be used to look at the effectiveness of security risk control measures at the ward, division, facility and/or NSW Health Agency level.

Another important aspect of the evaluation process is identifying those initiatives with the greatest potential for impact on frequency and severity, and evaluating/ monitoring their implementation.

When using existing information sources to develop performance indicators, consideration must be given to the reliability and accuracy of the information being used, whether base line data is available and any other factors that may impact on the information to be collected (eg confidentiality).

When identifying performance indicators to be used as part of an evaluation process, a balance of qualitative, quantitative, positive and negative performance indicators gives the clearest picture on the effectiveness of local violence prevention and management strategies.

Further guidance on measuring and reporting on work health safety is provided by SafeWork Australia.

9. Access and Egress Control

Policy

NSW Health Agencies must ensure, in consultation with workers and other duty holders, that all reasonably foreseeable security risks associated with access to and egress from clinical and non-clinical buildings and facilities are identified, assessed, eliminated where reasonably practicable or, where they cannot be eliminated, effectively minimised.

NSW Health Agencies must ensure that this process is appropriately documented and effective access and egress control procedures and perimeter control, including the implementation of remote locking on main access doors to emergency departments, and access/ identification systems, are developed and implemented.

In older buildings where compliance of the building may reflect standards that were in place when it was built a risk assessment must be completed to assess whether the building features remain fit for purpose or what other measures are to be in place to manage any risks/hazards.

Processes for 'lockdown' in facilities are to be in place. Additional guidance on developing facility lockdown procedures, in response to threats and hazards, can be found at this link.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

9.1 Access and egress arrangements must focus on the safe movement of individuals

In general, effective access and egress controls are in place to provide a secure work environment. They involve:

- appropriate identification and securing of building perimeters, including doors and windows
- appropriately managing access to and egress from the land, controlled by the NSW Health Agency, on which the facility is situated (eg fences, roads, emergency services, traffic and pedestrian access, egress and flow)
- control of access and egress to ensure perimeter integrity eg door alarms
- providing safe access and egress, especially after hours and during emergencies to allow workers to respond and access safe retreats within a timely and safe manner
- controlling access to vulnerable areas and securing vulnerable patients
- clear wayfinding
- instituting access/ identification systems that allow individuals to be identified and allocates access limited by the requirements of the position or task being undertaken
- applying the principles of Crime Prevention Through Environmental Design (CPTED) as outlined in Chapter 4 Health facility design, to assist in managing risks associated with access control.

In assessing the most appropriate access and egress controls, NSW Health Agencies must consider, as a minimum, the following issues:

- the presence of critical infrastructure onsite
- the nature of items stored on the premises eg sensitive or highly confidential information or system critical information, drugs, cash, electronic equipment etc
- the work carried out / services provided by the premises eg methadone dispensing, cash handling, drug and alcohol, emergency and mental health services etc
- the need to provide a secure work environment where there are access controls in place to staff-only and treatment areas
- the need to provide for rapid escape routes and access to safe havens for workers eg in the event of a violent incident
- the need to prevent unauthorised access or, in the case of vulnerable patients (eg children, the wandering elderly, patients scheduled under the Mental Health Act), allow them to be secured and prevent unauthorised egress
- potential for use of emergency exits (eg fire escapes) by thieves to remove assets
- potential for break in via doors and/or windows to remove assets
- potential for break in to and theft of vehicles (where relevant).

9.1.1 Doors must allow safe access control

- Perimeter/external access doors must be locked and access restricted to the minimum necessary points in the building (especially at night). If assessed as necessary, separate appropriate perimeter doors may be allocated as 'staff only' access/egress points.
- Perimeter/ external access doors must meet the following building design standards and any additional standards set out in this Manual or the Australasian Health Facility Guidelines:
  - be fitted with a quality single cylinder lockset that complies with fire regulations
  - have a metal frame or have a strip of metal securely mounted to the frame from the top to the bottom of the lock–side, with allowance for the lock tongue to be inserted
  - have protected hinge pins in order to resist removal. This can be done by either replacing the existing hinges with fixed pin, security butt hinges or having dog bolts installed to prevent pins being removed
  - have entry warnings, appropriate to the work environment such as alarms or warning buzzers fitted to doors that need to remain unlocked or open or to indicate that someone has entered the area
  - have alarms fitted to doors that are normally externally locked to signal when the doors are chocked open or fail to close properly
  - be fitted with door closers, unless a risk assessment deems this is not appropriate.
- Where practicable and allowable by technology electronic door alarms are to be connected to pagers (eg security staff pagers) to alert of possible breach of perimeter security.
- Fire isolated exit doors must meet the requirements of the Building Code of Australia and NSW Health policy for *Fire Safety in Health Care Facilities* – including:
  - emergency exits are clearly marked and illuminated signage regularly checked/working, fire exits not obstructed or impeded
  - the egress opening action of a lock must be a single–handed downward lever action. A pushing action is also allowed. Internal knobs or turn snibs are not permitted. This provision anticipates the need for a critical infrastructure access /egress control assessment emergency opening mechanism to be operable by people with hand or arm related disabilities, burns to their hands, with perspiring or wet hands, or the aged or infirm
  - the opening mechanism must be capable of being operated by a nudging action whilst dragging an injured or unconscious person to safety
  - key locking is not permissible on the egress side (inside) of the door. In some areas (eg where patients may abscond) exemption may be provided and a process must be in place for unlocking, and managing the patients
  - only one lock per door is permissible
  - locks must be fitted at a height of between 900mm and 1100mm from the floor level.
- After hours external public and staff entry points must be fitted with video/camera intercom systems to allow screening of members of the public presenting at the door, to allow workers to request assistance on arrival/leaving, and to record any incidents that may occur at entry points. The features of the system must include:
  - camera and intercom points located outside the entrance
  - one or more monitoring and intercom points located in the building to enable workers to see and speak to persons at the entrance
  - entry doors fitted with locks that can be opened electronically from the monitoring point within the building. Workers must be cautious in allowing entry into the building particularly after hours. The need to escort the person seeking entry to their destination and the notification to colleagues in adjoining areas that a person has been allowed entry needs to be considered.
- A risk assessment must be undertaken to determine surveillance camera requirements for all egress points (if different from the external public and staff entry points above) in a facility (see Chapter 13 Workplace Camera Surveillance.
- Glazing in doors and panels beside doors must be resistant to breakage and not shatter on impact, ie the glazing must resist being breached.
- Emergency Department public entry doors must have the capacity to be locked from a remote location that is within the line of sight of the door (this includes camera vision line of sight).
- Other public entry doors, such as the main entry door to a hospital (if different to the Emergency Department entry), must be fitted with remote locking where it is determined by a risk assessment to be necessary.
- Doors between public areas and treatment areas (excluding ward patient bedrooms/bed areas) must be access controlled (eg swipe card or code entry to minimise unauthorised access).
- The Code Black plan must identify designated entry points to ensure that Code Black teams muster and enter an area from the one point. The designated entry door must be known to the Code Black team and ideally identified with a marking such as an adhesive decal (refer to Chapter 29 Code Black arrangements for more information).

9.1.2 Lockdown procedures are in place

There is a facility lockdown procedure in place consistent with the requirements set out in *Health Care Facility Lockdown – A framework for developing procedures*. Consider using the templates and checklists from the framework. These requirements include:

- roles and responsibilities in relation to remote locking
- under what circumstances lockdown is to occur (eg terrorist incidents, altercations in or outside ED or suspected infant abduction)
- in which departments should lock down be able to occur
- identification of critical assets and threats/hazard assessments
- the use of remote locking on main access doors to Emergency Departments
- system for access and identification during lockdown.

9.1.3 Windows must minimise the opportunity for unauthorised entry and resist breakage

Perimeter windows must minimise the opportunity for entry to, or exit from, a window using one or more of the following options:

- reinforcement of windows
- using heavy gauge glass bricks or laminated glass panels (in areas which require natural light but no ventilation) that are securely mounted in the frame
- fitting security screens or security fly screens to windows that can be opened
- permanently closing unused windows by fixing bolts or screws or designing facilities with windows that do not open
- fitting key operated locks to all other windows
- limiting the extent of window opening
- applying film to glass to resist breakage or fit safety glass as per design guidelines.
- external and internal windows must be constructed to be resistant to physical force and include shatter proof film or security screens (there may be some exceptions eg where the building is covered by a heritage listing).

9.2 Wayfinding assist with limiting access to staff only areas

- All signage must conform with the requirements set out in *Wayfinding for Health Facilities*, and assist workers, patients and visitors to move to public/treatment areas within the facility.
- Signage (and floor markings where appropriate) must clearly identify areas where 'staff only' access is permitted.

9.3 Name Badges must provide easy identification of workers

- Security staff and Health and Security Assistants must always have their full licence displayed while on duty as required by section 36 of the *Security Industry Act*.
- For other workers, full names, worn at chest height, are the default position for NSW Health and this is influenced by several factors including:
  - the right of a patient to be able to identify a worker
  - the benefit of patients being able to relate to a person rather than a role
  - the type of health care being delivered and potential security risks for those delivering the care.
- Workers in emergency departments, mental health units and drug and alcohol units, have the option to display first names and family name initial. In these areas the name badge can be issued with this information only.
- In all other areas, a decision to not display both first and last names on name badges must be based on a documented risk assessment in consultation with workers, be relevant to the department and approved by the facility manager / general manager. The risk assessment will consider the likelihood of particularised threats against staff using the information on the name badge.
- Where full names are not used on name badges care must be taken to ensure that patients and others are always able to see enough information to differentiate between individual workers.
- In a work area where only first names are used, if more than one person has the same first name, there needs to be some distinguishing feature eg a last name initial, and/or variations on the first name eg 'Sue' and 'Susan' so that workers can be individually identified within the work environment.
- In addition to the name badge, workers must also be wearing photo identity / access cards, to be available for checking when requested.

9.4 Identity/Access Systems must limit unnecessary access and be up to date

9.4.1 Determining access for workers must be based on their role/s

- The level of access to be granted to a worker must be assessed and determined by the role they are to perform.
- Members of Code Black teams must be able to access all parts of the facility that they may be required to attend.
- Identity/access cards must only be issued where a new worker's right to access the premises has been verified. This will only occur where appropriate vetting actions (such as identity checking) have been undertaken. Visual identification must also be made at time of issuing the identity / access cards ie check of driver's licence.
- Arrangements for determining access must be in place to support the required access by workers who are working in a casual or temporary capacity (eg locums).
- The department responsible for issuing identification/ access cards must only issue identification/access cards after sighting evidence that the relevant vetting actions have occurred.
- A record of the document authorising access must be kept by the issuing department. The issuing department must arrange updating and re–issue or replacements as necessary.

- The level of access for a worker must be examined prior to expiry of the access rights to determine if reissue is necessary or further access time must be added.
- Review of access must consider whether the photograph is still a good likeness and if any details have changed since the issue of the card.
- Review of access must also occur if a worker changes position.
- Photos taken for the purpose of identification cards must include the person's face, including the area from the bottom of the chin to the top of the forehead and to each ear. Visibility of hair is not required.
- Workers who wear full or partial face covering garments will need to remove the covering for the purpose of taking a photo for the identification card. The request must only be for a face covering to be removed for the period of time needed to take a photo, and to the extent necessary, to establish identity. A person must not be requested to remove garments or equipment that cover the person's hair if their face is otherwise visible. This must be done sensitively. Where operationally feasible, where the face covering is worn for reasons of modesty, it should only be removed in the presence of persons of the same gender preferably in a place where only the identifier can view the face of the person to be identified (Refer to NSW Government *Policy on Identity and Full Face Coverings for NSW Public Sector Agencies)*.

9.4.2 Features of identity/access cards

Identity/access cards may contain any or all of the following features, bearing in mind integration of existing systems and the outcomes of the risk assessment process:

- name, position, title and photograph of the holder
- expiry date (may be displayed on the card or be electronically embedded)
- serial or unique number (this could be the employee number)
- identification of the issuing NSW Health Agency
- a return address
- emergency, WHS or infection control information.

As far as practicable identity/access cards must include unique features that offer counter measures against forgery.

9.4.3 Administration of the Identity/Access System must be secure and up to date

- All documentation and equipment for identity/access systems must be securely stored to prevent unauthorised access.
- Clearance procedures on termination must include the return of the identity/access card. It may be necessary to recover the permanent identity/access card and issue a temporary card valid until the final day of employment only, when it must be returned.
- The department with responsibility for administering the identity/access card system must be advised of workers ceasing duties, to ensure these identification/access cards do not remain active on the system.
- Access rights to the electronic access control system may be assigned separately to the production of the identity/access card (ie human resources may produce the card and the security department may enter the card in the access system).
- The access rights assigned to an identity/access card must be programmed for a predetermined period, set by the NSW Health agency. Workers must be given adequate notice of any action they are required to take as part of a periodic reissue of identification/access cards. This notice must take into account workers who work part-time, are rotating through workplaces or work out of hours.
- Identification/access cards not active within a pre-determined period, set by the NSW Health agency, must be automatically purged or manually deactivated.
- Any lost or stolen identification/access cards must be immediately reported to the department with responsibility for administering the identity/access card system to ensure the card can be deactivated:
  - local arrangements must include procedures for managing access for workers who have had their identification/access cards stolen or have lost them. This may include issuing short term identification/access cards.
  - there must be arrangements for workers to advise, out of business hours, of lost or stolen cards.
- Checking of active cards against current workers must occur at least yearly to ensure access that is no longer required is removed.

9.4.4 Determining access for non-staff members in attendance at the facility

Each facility must have a documented procedure for determining, approving and recording of the type and conditions of access of a non-staff member to 'staff only' areas.

This must include that access and supervision requirements are limited to the role the person is to perform or the purpose of their attendance at the facility.

10. Key Control

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all reasonably foreseeable security risks associated with key control, and code locks are identified, assessed, eliminated where reasonably practicable or, where they can not be eliminated, effectively minimised.

NSW Health Agencies must ensure that the process is appropriately documented and effective key control and keypad code security procedures are implemented.

'Keys' as used in this Chapter refers to metal keys, electronic keys, swipe cards, electronic access cards and keypad codes.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

The purpose of key control is to manage access and movement across a facility or campus.

Electronic locks, and associated swipe cards, are preferred as they have significant security advantages with 'keys' that can be reprogrammed and can also be remotely 'deleted' if lost.

10.1 There must be processes in place for issuing keys to ensure control of access to facilities

- Access to the Great Grand Master Keys (GGMK) / Grand Master Keys (GMK) must be limited to a small number of designated senior executive staff (this may include nominated local incident controllers) who can access it in the case of an emergency.
- There must be a documented process to manage the exchange of shared keys at the change over of shifts.
- The authority to hold and control the issuing of keys must be determined and documented (refer to Chapter 9 Access Control for appropriate standards)
- There must be a **Key Authority Record** which provides record of approval for an individual to be issued with a key. All personnel authorised to draw and return keys must have their name printed and their specimen signature recorded. Key Authority Records in electronic or hard copy must be securely stored to reduce the risk of loss.
- There must also be records kept of the movement (issue and return) of all keys. Completed logs must be reconciled and retained for a period of not less than twelve months from the date of the last entry and must identify keys issued on a daily or temporary basis. It must include the printed name of the person, their signature and the signature of the issuing person. This may be done via a secure electronic log. This must be verified against the Key Authority records.
- The number of keys issued for any one lock, or entry must be kept to a practicable minimum, but not impact on the delivery of services.
- Workers must be advised that keys must not be worn around the neck, particularly in clinical areas, as this is a possible strangulation risk or could be used by a violent person to draw the worker closer. This can include lanyards and bungee cords.
- Workers must be advised that keys must not be left unattended or lying around in view.
- Workers must be advised that they are not to lend their keys to other workers or borrow keys from other workers.
- Swipe card systems are preferable to code locks except in specific circumstances such as ambulance entry to emergency departments. Where codes are used to control code locks they must only be available to those with a legitimate reason for access, including paramedics, police and other emergency services, where necessary.
- Workers must be reminded they are not to disclose individual alarm or door codes to other workers, family members or others (patients and visitors).

10.2 There must be processes to ensure the safe storage of keys and determining access to keys

- GGMK/GMK must be stored in a locked safe accessible only by designated senior executive staff. They are not to be issued to workers for general use.
- Security staff may be issued with building Master Keys as necessary.

- Keys that are not issued must be stored in a locked container, located out of sight of unauthorised persons.
- At the time of installation of locks or electronic access devices, keys must be given to a designated facility worker. A receipt must be received by the designated facility worker (a copy of which is kept by the issuer). That worker must sign for the keys to confirm:
  - the correct numbers of keys have been received
  - a key authority card is raised for each lock or entry (where this system is used)
  - that the keys received work
  - that one original key is retained and stored appropriately.
- All keys for the same lock or entry must be individually numbered to indicate the lock or entry they fit and the actual key number for that lock or entry.
- Digilocks or coded doors need to have master key override hardware and/or software.
- Cutting of additional or replacement keys must only be:
  - authorised by the authorised facility worker
  - cut by an authorised locksmith who is contracted by the facility.
- The designated facility worker authorised to arrange for keys to be cut must ensure that the person is licensed to undertake that activity under the *Security Industry Act*. Approved authorised key cutters must provide a copy of their Master Licence number to the NSW Health Agency as part of the contractual arrangement.
- Where NSW Health Agencies that have their own key cutting/duplication capability, they must ensure that key cutting codes and key blanks are protected at all times.
- If a NSW Health Agency site has a key cutting machine and they have master blanks or restricted blanks, they must be licensed to undertake that activity under the Security Industry Act.
- Key pad access codes must be changed every six months or sooner if the access code may have become available to unauthorised persons to prevent compromise of the facility or department access control system.
- Disused access codes must not be reused for 12 months. This is consistent with reducing potential theft opportunities and unauthorised afterhours/weekend access, and may be needed at some point as evidence.
- Key code changes must be communicated to all relevant workers in a timely way.

10.3 Keys must be audited to identify lost or inactive keys

- The person identified as responsible for facility key control, must:
  - conduct a stocktake, at least annually to audit keys, and record results
  - report any unaccounted keys to the appropriate supervisor/manager
  - where practicable conduct spot checks at intervals not exceeding six months
  - ensure the records from audits are kept securely and made available for inspection as required
  - identify appropriate alternative mechanisms for the return of keys when the responsible person is not available eg after-hours.
- Workers must be advised that they are not permitted to cut keys to their offices or other work environments and this must be randomly checked.
- Where a key is lost, suspected to be lost, or otherwise compromised action must be taken to replace the affected lock/s and the key register updated.

10.4 Keys no longer in use must be destroyed to avoid misuse

- Key Authority Records must be kept up to date.
- Keys that are no longer required must be destroyed and this must be entered into the Key Authority Record and also deleted from the key control card/system.
- Electronic swipe cards that can be recycled are to have any access data removed before being made available for reuse.
- There must be a process to delete access and update the Key Authority Record when workers cease engagement or their access requirements change:
  - workers or others who have ceased their engagement. Confirmation that the return of keys or swipe cards has occurred must be included and documented as part of a termination clearance process
  - workers or others who no longer require access to an area must return their key. There must be a documented process for identifying and activating these changes.
- Keys or swipe cards that are lost, suspected to be lost or otherwise compromised must be reported to the designated person at the facility
- Workers must be advised of the requirement and process to report key losses, including after hours. Workers must also be given information on the importance of immediate notification of loss (ie to avoid unauthorised access)

See Chapter 9 Access Control of this Security Manual for electronic access control standards.

11. Duress Alarm Systems

Policy statement

NSW Health Agencies are required, in consultation with workers and other duty holders, to establish their requirements for duress alarm systems to ensure that workers, patients, and assets are secure.

Duress alarms provide one mechanism to allow workers who feel unsafe to call for assistance. The importance of monitoring the safety of co-workers is still required. Priority must be given to incident prevention. Sound incident response procedures must also be developed (refer to Chapter 29 Code Black arrangements).

Ongoing assessment of all duress alarm systems must occur, appropriate to the level of risk, as part of the ongoing risk management process.

Workers must have unobstructed access to purpose designed equipment enabling them to summon assistance if they are faced with a personal threat or physical assault. This may include the use of personal duress alarms or fixed duress alarms or both, reflective of the nature of the work being performed and level of risk of threats identified.

Workers must wear NSW Health Agency provided personal duress alarms where they are required to answer public access doors after hours eg maternity units.

All workers who are required to work within an emergency department must be provided with a personal duress alarm. The personal duress alarm must be worn at all times while working in this area. In all other workplaces workers must have a way of calling for assistance. In areas where violence or unauthorised access could occur then a risk assessment must be undertaken to determine the need for, placement and functionality of fixed and personal duress alarms. This risk assessment and control measures must be reviewed following any incidents in the area.

Random spot checks of compliance with this requirement must occur and the results documented and reported to the department manager and the Chief Executive of the NSW Health Agency eg monthly.

Requirements for duress alarms for use in the community are covered in Chapter 16 Working in the community.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

11.1 Determining the requirement for duress alarms

In assessing the requirement for duress alarms, NSW Health Agencies must consider, as a minimum, the following issues:

- size, layout and location of the facility/service (including areas with reduced lines of sight or potential for entrapment)
- potential for violence against workers, patients or others within and in the grounds of the facility
- the type of work being carried out by workers, the work practices in place and whether workers move to multiple locations eg campus wide coverage is needed
- type of service being provided
- potential sources, causes of and locations for violence
- whether the service is facility based or community based
- whether the workers may work in isolation
- if workers are required to open public access doors after hours
- potential for theft/armed hold-up eg drugs held on site, radioactive substances, cash handling
- level of external security risks
- potential for assault of persons (eg workers/visitors) in facility grounds and car park areas
- potential for use of grounds and other spaces for illicit drug consumption
- potential for violence and other crimes to result from the facility precinct being used as a thoroughfare or meeting place
- the appropriate mix and features of fixed and personal duress alarms as outlined below.

In assessing the requirement for duress alarms, NSW Health Agencies must consult with workers and other duty holders.

Duress alarm systems need to complement all other protective measures taken by the NSW Health Agency to prevent and manage risk.

Duress alarm system features and configuration must be appropriate to address the identified risks.

When tendering for duress alarm systems, NSW Health Agencies must ensure that:

- all relevant requirements in NSW Health Policy Directives and Guidelines, and NSW Procurement requirements that apply are met
- expert advice is sought when preparing the necessary specifications and system design
- the system can operate correctly under a range of conditions
- training of workers in the operation of the system is included and all operating manuals are supplied
- ongoing maintenance of the system and the use of maintenance contracts is considered
- the supplier guarantees the duress system (ie all equipment and systems will be supported for a period of no less than five years from the date of service and the supplier will provide “urgent and routine” servicing, upgrades and replacement of all parts during that period).

The duress alarm system is expected to have sufficient redundancy to allow continued operation. Downtime procedures must be in place, including back–up power (eg generator or uninterrupted power supply (UPS)) for a period suitable for the risk, for instances where the system does shut down.

11.2 Selecting fit for purpose duress alarms

11.2.1 Determining the most appropriate mix of duress alarms

A risk assessment must consider the appropriate mix of the following types of duress alarms and the need for back–up in the event of system or power failure:

- fixed alarms, with duress buttons strategically located throughout the health care facility. These may be battery operated or hard wired
- personal duress alarms worn by workers
- for community based workers see Chapter 16 Working in the community for equipment to summon assistance when outside the health facility.

Patient emergency buzzers are not to be used in lieu of fixed or personal duress alarms. The duress alarm system solution must consider the operation practices of the entire campus to ensure it is operationally sound, efficient and seamless.

Fixed alarms may be used in well defined areas where:

- the person works from a static position (eg where workers are behind a screen such as a pharmacy distribution window or behind a counter)
- the alarm can be discretely activated without the worker leaving their normal working position
- workers are in rooms alone with patients providing treatment/consultation/procedures. If these rooms do not have secondary egress to prevent entrapment then an additional fixed duress alarm must be available (eg a fixed duress alarm at the front and at the back of the room). These rooms do not include patient bedrooms or spaces that have dedicated staffing (eg operating theatres, IPUs) as other risk controls are in place. These patient treatment spaces are instead all other enclosed spaces where a patient may be taken to and while in that space the worker works alone with the patient (eg consult, interview, treatment or procedure rooms). These locations may include ambulatory care, wards, community health centres or areas within an emergency department
- staff only areas must be fitted with fixed duress alarms to ensure workers can summon assistance in the event of a threat arising from unauthorised access to these areas.

Personal duress alarms are used where the worker is moving around within a building in the course of their work and where there is a risk of being confronted by aggressive behaviour.

- Personal duress alarms for use within a facility and the immediate area must comply with all relevant Australian and regulatory requirements.
- All Emergency Department (ED) workers must have (and wear) a personal duress alarm while on duty. To determine whether a personal duress alarm must also be issued to workers visiting the ED a risk assessment must be undertaken eg considering workers providing food delivery to the department versus food serving to a patient, visiting medical or allied health staff etc. This risk assessment must consider the following factors:
  - What is the frequency and length of the visiting?
  - What locations are visited in the ed?
  - What tasks are carried out?
  - Does the ED have any areas where a worker is concealed (ie poor line of sight from the staff station or other static workers)?
  - Does the work being completed by the visiting workers involve entering these concealed areas.
  - Is there a fixed duress alarm in the location of their work? If yes, could the visiting worker have their access to the fixed duress alarm obstructed?
  - Is the visiting worker using any treatment/consultation/administration rooms that only have one exit?
  - Does the visiting worker complete any role that involves having their back to patients (eg are desks facing away from patients)?

- Does the ED have multiple points of public entry that are not access controlled (ie is public entry/access to the ed actively managed)?
- Does the ED camera surveillance only record footage (ie it is not continuously monitored by someone who can summon assistance for the visiting worker)?
- Does the worker have a role that involves working with patients?
- Can the visiting worker commence their work with the patient without being briefed by ED workers on any risk factors?
- Are there sharps or other implements that are not out of sight or locked away?
- Will there be times that the worker will complete their duties on their own and not in the presence of an ED worker who carries a personal duress alarm?

11.2.2 Features specific to personal duress alarms

Personal duress systems must have a unique identifier to identify an individual and their location. This must be transmitted when an alarm is raised. The quantity of personal duress alarm devices must be sufficient to cater for the largest shift plus allowances for visitors, units being charged, defective and spare units as needed. Arrangements must be in place to repair or replace defective personal duress alarms as a priority.

All personal duress alarm units must have the following features:

- provide activation that can be initiated by the wearer and also activated where the user is not moving or has fallen down. These must not be able to be disabled by individual workers. Where frequent false alarms are occurring discussion with the provider of the duress alarm must occur to identify options for reducing these false alarms
- include a warning when the person down/no movement feature is about to trigger
- have a battery life that is not less than the longest shift
- can display battery status and warns when the charge is low
- an Ingress Protection (IP) rating and operational temperature range appropriate for the circumstances of its use
- that the device represents value for money
- be able to be affixed to clothing and be worn attached to a strong and stable part of the wearer's clothing, and not be worn around the neck (eg clipped to a hip pocket or waistband, or in a location to minimise false alarms and allow quick access)
- have a signal that can be transmitted through clothing. Should workers affix the alarm on a waist band under clothing the design of the uniform and how the worker will wear the alarm must be considered.
- include a "warning indication" if the user is out of range, or there is a communications or battery failure
- provide accurate information on the location of the activated alarm relevant to the physical design of the workplace so that the person can be found without delay every time. For example:
  - in a large open plan workplace with good line of sight location finding capacity must get the response team to the area where the worker is
  - In work areas with limited lines of sight or fixed walls, corridors and/or rooms, room by room location accuracy must be provided.

11.2.3 Features for both personal and fixed duress alarms

- Be able to interface with other local communication and security systems (eg paging systems and camera surveillance monitoring rooms where they are in use).
- Be able to cover all working and amenity areas for the specific location including meal rooms, toilet facilities, stairwells, storerooms and external staff amenities (eg car parking).
- Provide integrity of communication and a system which is not prone to interference or false alarms.
- Include the installation of a fixed backup system.
- Be off the shelf, quality tested equipment rather than customised equipment or software.
- Be of current technology and part of a system that can be easily added to or subtracted from if needs change (eg workers leave or join, without needing to install a new range or design of equipment).
- Be capable of transmitting a duress signal to activate the security system within five (5) seconds of activation and timely (less than 12 seconds) notification to the Code Black response team. The system must activate with a reliability factor of no less than 98%.
- Be user friendly and simple to use.
- fixed alarms must be located and designed to allow easy access by workers and also minimise tampering
- Fixed duress alarms that are not hard wired or personal duress must show the battery status and warn when the charge is low.

Personal and fixed duress alarms **must not**:

- Activate a noise other than a noise to reassure the person wearing the alarm. This is to prevent an audible alarm causing secondary reaction by assailant or create undesirable reactions or concerns among patients or visitors.
- Rely on a form of transmission or communications or any other device that could interfere with the functioning of critical medical equipment.
- Be susceptible to tampering or activation by patients or visitors.

11.2.4 Features for personal and fixed alarm notification

When an alarm is activated the following must occur:

- the person activating the alarm receives some assurance that the alarm has been sent eg low tone, or a vibration, or other means that is not likely to further agitate an aggressor
- the Code Black team receives the alarm in an identifiable tone, identification of the activating alarms, time stamp and text/visualisation of the location
- alert other workers in the work area/facility that a colleague requires assistance, to ensure that assistance is activated and to ensure that another worker does not accidentally walk in on a duress situation thus putting themselves at risk.

11.2.5 Testing to ensure individual units and systems remain operational

- Personal duress alarms must be tested in line with the manufacturer's advice, specified battery life and those factors that may impact on that battery life eg activation of the alarm.
- Personal duress alarm units must include some indication, or be manually tested at the start of each shift, to ensure the individual unit being carried by the worker is working and recognised by the system. Where manual testing has to occur, NSW Health Agencies must seek the advice of the supplier to set up a suitable testing protocol.
- Personal duress systems must be self–testing and notify of any malfunction. If a fault is detected it must notify appropriate workers immediately. Self–testing is to occur at intervals of one hour or less, and have the capability to produce hard copy and electronic evidence of testing (self–testing and programmed maintenance) and the results are to be kept for a minimum of 90 days.
- Fixed duress alarms must be tested in line with the manufacturer's advice and will depend on whether the system is hard wired or battery tested, how the alarms are tested by the system and any automatic notification of issues. A specific testing regime must be documented eg testing occurs at least every 30 days, records are kept (either within the system or by the tester) and audited at least yearly.
- Testing records must be maintained and any faults reported and fixed as a priority. Workers in the vicinity of a faulty fixed duress alarm must be advised of any issues with the function of fixed duress alarm and advised again when it is back in operating condition.
- Where issues are raised regarding identification of “black spots” or lag times in receiving alarms, the supplier must be contacted to conduct appropriate tests/rectify the situation.

11.2.6 Training and information

- Suppliers of any alarm system must, as part of any contract, provide training in an easy to understand manner for workers in the use of the equipment. Suppliers must also provide a copy of written instructions for users on how to operate and test alarm units and how to recognise warning signals, eg low battery, impending person down alert.
- Arrangements must be made by the NSW Health Agency to ensure new workers are provided with instruction on the operation, location and testing of all the duress alarms systems in the area.

12. Lighting

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that internal and external lighting is sufficient to eliminate risks, where reasonably practicable, or where they can not be eliminated, minimise security related risks.

Lighting must be sufficient to eliminate dark areas, and must facilitate the correct functioning of surveillance cameras.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

12.1 General lighting requirements to ensure safety

- Determine the needs of areas requiring special lighting treatment (eg Entrance Foyers, Emergency Departments, Staff Entry and Exit points, Pharmacies and Car Parks).
- Lights used for security purposes must be automatically activated and deactivated at pre-set times (times need to be seasonally adjusted) or at pre-set light levels.
- Lights used for security purposes must be connected to back up power where practicable (including external lighting) eg generator or uninterrupted power supply (UPS).
- Lighting must avoid the creation of dark spots and be sufficiently bright to deter crime and concealment, and to provide sufficient illumination to prevent slips, trips and falls and allow facial recognition.
- The lighting used must meet Australian standards AS/NZS1680 series, AS/NZS1158 series (including 1158.3.1), and AS4485.1 as applicable (see below).
- Lighting must support the use of surveillance cameras. For lighting requirements to support surveillance cameras operation refer to Chapter 13 Workplace Camera Surveillance. Prior to installing or making changes to lighting, ensure that there will not be any adverse impact on surveillance camera performance.

12.2 External lighting must be appropriate to the area being lit

- External lighting must be housed in vandal resistant containers and mounted to restrict tampering (eg too high up to be readily broken).
- Posts for security lights must be designed in such a way that they do not provide a 'ladder' or foothold to allow access to the light fitting or buildings.
- External lights must be sufficient to eliminate dark areas and must allow for faces to be recognised
- External lights must be maintained by programmed maintenance, including regular cleaning during spring and summer, as lighting can be seriously impeded by moths and insects particularly in rural areas.

12.3 Internal lighting must support safety and deter theft

- Some internal lighting must remain on during the night, after the workplace has been closed for the day. Some internal lighting must be available via movement sensors (if needed) after the workplace has been closed for the day. These areas must be identified and documented.
- Emergency lighting/fire exit signs must be working and not obscured

12.4 Car parks lighting must support safety and deter theft and vandalism

- There must be appropriate lighting in car parks. They must be lit in line with Australian Standards (see below)
- Lighting should deter theft and vandalism
- Where the facility does not have dedicated on-site parking, consultation on street lighting must occur with local councils when hazards/risks are identified.

12.5 Checking lights and preventative maintenance must be ongoing and planned

- There must be a process for planned checking that lights are working (external and internal)
- There must be programmed maintenance in place for external lights (see above)
- There must be a process for reporting malfunctioning lights.
- Malfunctioning lights must be replaced immediately.

12.6 Requirements of Australian Standards related to lighting for security

Note: These Standards include other requirements for lighting, unrelated to security, that have not been referenced here.

AS/NZS 4485.1 Security for health care facilities – Minimum lighting requirements

Health care facilities shall establish and maintain an effective internal and external protective security and safety lighting system to enhance security and crime prevention.

All lights shall conform to and meet the relevant security related requirements set out in AS/NZS1680.2.1, AS/NZS1680.4, AS/NZS1680.5, and AS 1158.3.1. The effects of the lighting on the surrounding environment must be limited. The relevant sections of these standards have been incorporated into this chapter. See also AS 4282 Control of the obtrusive effects of outdoor lighting.

After a security risk assessment where lighting is identified as a risk or a new control measure, a specialist lighting organisation shall be engaged to provide a lighting plan based on the security risk assessment.

Lighting assessment based on crime prevention principles shall be conducted as part of the commissioning process for all new developments or redevelopments.

Table 1: Security lighting levels

Situation	Average, lux (lx)	Min. lx
Car parks (outdoor)	20	10
Car parks (Indoor)	40	20
General grounds adjacent to areas used at night	5	3
Walkways	20	10
Areas adjacent to entry/exit	50	30
General grounds used for night activity	20	10

AS/NZS 1680.2.1 – Interior and workplace lighting – circulation spaces and other general internal areas

- Care must be taken with entrance areas to avoid a pronounced change of illumination between inside and outside, both by day and by night. In addition the luminaires used must be of such a type or so located that persons entering or leaving the area will not suffer a significant loss of visibility resulting from glare from the luminaires.
- Care must be taken to avoid light falling on glazing from directions that will produce reflections and obscure views at night
- Appropriate exterior lighting giving good vertical illuminances will be necessary for visibility of person or vehicles passing through controlled areas
- Vertical illuminances are important for the recognition of people and detection of obstacles
- Luminaires must be positioned so that it is possible to see adequately into storage areas

AS/NZS 1158 – Road lighting (AS/NZS 1158.3.1 Pedestrian areas)

An appropriate maintenance regime shall be developed and documented to ensure that the relevant light values will not fall below the applicable values levels.

13. Workplace Camera Surveillance

Policy

NSW Health Agencies are required, in consultation with workers, other duty holders and security experts, to identify locations in buildings and grounds where overt camera surveillance may be of assistance, and clearly identify the purpose for each camera in relation to the security risk management program, ie is the purpose of the camera surveillance to provide a visual deterrent, to support access control measures or to be used to identify an incident where a duress response/code black response is required.

This Chapter is intended to focus on camera surveillance installed as part of a security risk management program.

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that where the camera surveillance is used as part of a security risk management program, effective procedures are implemented that are consistent with relevant legislation, including the Workplace Surveillance Act 2005.

Where a NSW Health Agency is considering the use of covert camera surveillance, approval must be sought from the Secretary of NSW Health prior to a 'covert surveillance authority' application being submitted.

Standards

Within NSW Health Agencies there are potentially two types of camera surveillance that may occur:

- **Overt** camera surveillance, plainly apparent cameras used as part of a security risk management program
- **Covert** camera surveillance, concealed surveillance used to capture suspected unlawful activity.

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

13.1 Determining the need to introduce/add to overt camera surveillance:

Camera surveillance is to be used in conjunction with other control strategies as outlined in this Manual and is not intended as a standalone solution to control security risks.

The purposes of camera surveillance in NSW Health Agencies will include actively identifying incidents that are escalating so a response can be activated, to provide a line of sight into poorly visualised areas or spaces, sighting persons presenting at doors as part of the facility access controls, crime deterrence and protection of assets and recording of evidence only.

Cameras set up solely to capture evidence (ie they are not monitored or used to improve lines of sight into an area) are not on their own an effective security risk management control. NSW Health Agencies must make decisions around placement and number of surveillance cameras in a facility to reflect the security risk management outcomes to be achieved and the core purpose of the facility. This must be documented and clearly communicated to workers.

The following issues, as a minimum, must be considered during a risk assessment:

- history of violence or other crime/incidents in the area and any pattern of times or days where this risk is greater
- history of threats to people and property in that area
- no, or poor, line of sight from populated staff areas into that area
- the activity that occurs in that area eg emergency department waiting room, corridors, entry doors or carpark
- whether the area is used to store valuable property or other items that may be a target for theft. This includes security–enhanced radioactive substances, see Chapter 23 of the Security Manual (ie coverage of entry/exit points and if required (as identified the risk assessment) storage areas)

- cost of properly maintaining and supporting the camera surveillance, and identification of the necessary equipment required to provide camera surveillance that meets the standards set out in this Chapter eg what type of camera, lens and mounting are best for the purpose and what lighting is needed to support proper functioning
- compatibility with existing technology and systems eg can it be integrated into duress alarms systems
- existing controls in place to manage crime prevention through environmental design
- does the introduction of camera surveillance create new or different security risks eg moved potential illegal activity to other surrounding areas
- how surveillance can be used that will minimise the impact on people's privacy
- what expectation workers and others will have if there is a camera in the area ie will they expect someone is watching and assistance will automatically be sent
- requirements for continuous or adhoc monitoring.

Regardless of the reasons for the installation, having a clearly displayed camera in an area can create an expectation from workers and others that a Code Black response will be automatically triggered if a violent incident or criminal behaviour occurs within view of the camera. As a result, this may affect the response of the individual to the situation, eg not retreat as they are expecting assistance. It is therefore essential that the purpose of the camera surveillance, and what they must do in the event of a threat, is clearly communicated to workers.

Where existing camera surveillance infrastructure has not been assessed and implemented in line with the above standards a documented risk assessment must be completed.

13.2 Notifying workers about the use of camera surveillance where it is a security measure

- Where camera surveillance is being installed, following a risk assessment, as a security measure and not for surveillance of workers, the NSW Health Agency must consult and agree with workers/their representatives about how this surveillance will be carried out (refer to Section 14 of the *Workplace Surveillance Act 2005).*
- The camera surveillance must then be used in accordance with that agreement and not for any other purpose.
- Cameras must be visible to people in the area that is under surveillance.
- Signs notifying people that they may be under camera surveillance must be clearly visible at each entrance to the area under surveillance. Signage, wherever practicable, and where they involve words rather than pictures must take into account the different languages likely to be used by people presenting at the facility. Patient information must also include information on the presence of camera surveillance.

13.3 Placement of camera surveillance must be effective

Where, following a security risk assessment, camera surveillance is required in a particular location, a risk assessment must also consider the effective placement of the camera within this location.

The following applies when determining the placement of camera surveillance:

- expert advice on the location of cameras must be sought. This could be provided by internal security staff or by appropriately licenced external parties (the appropriate NSW security licence). Any placement of cameras in a clinical area must be determined via a risk assessment involving relevant clinicians
- placement must focus on areas where there is a higher likelihood for incidents to occur and where the camera will have value as a deterrence
- the location of the camera must not encroach on patient privacy and confidentiality (ie no view of clinical procedures or physical examinations). Surveillance cameras must not be placed in any bedroom, change room, toilet facility or shower or other bathing facility
- where a surveillance camera is located within a seclusion or safe assessment area, for the purposes of ensuring safety of access, images must not be recorded or visible beyond workers supporting patients in the room. NSW Health policy and guidelines for seclusion and restraint, and safe assessment rooms do not allow the use of cameras for patient observation.
- activity levels at pedestrian and vehicular thoroughfares must be considered
- where waiting areas and common spaces (eg main entrance, cafeteria etc) are not continuously monitored by workers when in use, they must be fitted with camera surveillance
- as far as is possible, camera surveillance must be placed at a position that allows for faces to be recognised
- review of the placement of camera surveillance must occur to ensure it remains appropriately placed, and continues to be pointed in the necessary direction
- a maintenance log must be kept by the Health Agency.

Technical installation and operational requirements must be identified including:

- expert advice on the type of cameras must be sought. This could be provided by internal security staff or by external parties
- the lighting levels must be assessed and upgraded where necessary. Assessment would include the potential for shadowing, the minimum lux levels, the type and height including varying lighting levels in open areas as opposed to under awnings and obstructions to fields of view
  - lights must be bright enough and allow for faces to be recognised, and not allow concealment of a person
  - prior to installation of camera surveillance, light levels at different times of day must be considered to ensure that the camera provides a clear image at all times. This must also include the potential for the direction of the sun, including sunrise and sunset, to cause 'blooming'.
- surveillance camera placement must eliminate concealment opportunities. Where it is being used as an access control strategy a second camera or a change of lens needs to be considered if:
  - there is a possibility of line of sight not being maintained, or
  - a suggested placement of a camera does not fully cover the entry point allowing for visual identification prior to allowing access of a person.
- landscaping, including line of sight, potential shadows, type and growth rate of trees and vegetation must be assessed and the risk eliminated
- the height of equipment above ground must be sufficient to deter potential vandalism and damage caused by vehicular traffic (while noting that position height of cameras needs to allow adequate identification of persons). The use of purpose built anti–vandal casings or cages can be considered.
- the view from the recommended camera height, taking into account building structures and awnings must be assessed
- whether private premises would come within the view of the camera
- the accessibility of equipment for maintenance purposes including any safety issues for workers undertaking the maintenance
- possibility of accompanying lighting intruding upon the surrounding area
- access to a continuous power supply
- cabling routes and distances
- availability of existing cables and conduits
- trenching and reinstatement costs
- compatibility with current installation/s. Can the equipment be networked to allow monitoring at another campus or larger hospital? Access to off-the-shelf replacement equipment
- placement of hard drive and monitors – password protection of hard drive, password protected ability to download images and security of the hard drive so it can not be tampered with eg unplugging.

Placement of monitors must occur with consideration of right to privacy and confidentiality. Monitors must be positioned to discourage inappropriate viewing.

13.4 Monitoring surveillance cameras

- Where surveillance cameras are installed, and identified by a risk assessment to be used for the purpose of actively identifying incidents that are escalating so a response can be activated, it must be continuously monitored or managed in a way that ensures an appropriate response is activated in the event of a violent incident.
- NSW Health agencies may also consider establishing an integrated agency wide camera surveillance monitoring operation ie all campuses monitored via a central point.
- Where the continuous monitoring of surveillance cameras in higher risk areas is not assessed as necessary the following alternative controls, as a minimum, **must** be implemented:
  - a duress alarm or another mechanism for summoning assistance is installed within the vicinity of the surveillance camera (except where in a public corridor) *and*
  - a duress response is mobilised where the duress alarm is activated *and*
  - signage advising workers of the need to activate a duress alarm in the event of an incident is displayed in the vicinity of the surveillance camera *and*
  - review of the effectiveness of the above strategies is undertaken, appropriate to the level of risk, to ensure risk is being appropriately managed in a way that maintains the security of workers and others.
- Where continuous monitoring of surveillance cameras is not occurring, in Emergency Departments (ED), regardless of the purpose of the camera surveillance, live feed should be available at staff stations. That is, all ED surveillance cameras should feed into a monitor in view of workers, regardless of whether the footage requires continuous monitoring (eg main public after hours access entry doors).
- Where practicable, surveillance cameras should be connected to the duress alarm system. This would allow the surveillance cameras to pan to the site of an activated duress alarm and/or give visibility to a third party, eg security company or police to see remotely what is occurring. This allows them to make an informed decision as to what type of response is required. This requirement should be assessed and considered in the design of new facilities.

- Monitors displaying surveillance camera images must not be viewable by the public unless relevant to their purpose (eg as a deterrent). Patient confidentiality must be considered.

13.5 Storage of camera surveillance recordings

- All camera surveillance that is recorded must be stored for a minimum of 21 days so that evidence is available following an incident.
- The footage or images must be digitally "watermarked" and time stamped. The use of digital watermarks or similar technologies can help create a clear record of when and where records were accessed. The watermark/time stamp must be checked for accuracy at least when the system is installed, when there is a change (eg daylight savings). The accuracy of the timestamp must also be checked when lawfully providing footage to a third party and any discrepancy noted.

13.6 Use and disclosure of camera surveillance records

NSW Health Agencies must implement clear protocols for determining, in each instance, whether camera surveillance records should be provided to other parties, and identify who within the NSW Health Agency has the authority to approve the release of those records. Requests for camera surveillance records must be written.

Procedures must be in place that require the logging of when, where and why stored footage was accessed. A copy of any surveillance supplied must be kept by the organisation.

The NSW *Workplace Surveillance Act* requires that any record made as a result of surveillance must not be used or disclosed unless the disclosure is:

- to a member or officer of a law enforcement agency (eg Police Force) or SafeWork NSW for use in connection with the detection, investigation or prosecution of an offence
- for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings
- reasonably believed to be necessary to avert an imminent threat of serious violence or of substantial damage to property.

The notification requirements set out in Section 10 of the *NSW Workplace Surveillance Act* must be met before video footage can be used for disciplinary/misconduct or performance matters. There are limited circumstances where footage may be used without notification requirements being met.

NSW Health Agencies are obliged by law to provide surveillance records when issued a warrant by Police or a court order. In limited circumstances surveillance records can also be provided without a warrant.

NSW Health Agencies must assess requests for surveillance records, in the absence of a warrant, on a case-by-case basis. A release of camera surveillance footage to police isn't a breach of privacy (in circumstances where NSW Health Agencies are releasing any information relating to an offence which has or may be committed, provided that information is "reasonably necessary" to assist the law enforcement agency to perform its functions).

In deciding whether to provide surveillance records, the factors that must be considered by NSW Health Agencies prior to disclosing surveillance records without a warrant include:

- the need to balance the obligations in the *Health Records and Information Privacy Act* regarding confidentiality of patients and the often sensitive nature of health information
- the seriousness of the alleged offence and the urgency of the matter (A 'serious criminal offence' is defined as an offence which attracts a penalty of five years imprisonment or more. Health workers must be aware that this covers offences such as drug trafficking, serious assaults, sexual assaults, murder and manslaughter. It does not cover minor possession offences or any offences under public health legislation)
- the degree of evidence available that suggests the surveillance record contains information that will assist with law enforcement
- how well sign posted is the camera surveillance ie will workers and visitors to the area have a reasonable expectation that they will be captured in surveillance records?
- any local arrangements with worker representatives, as the surveillance records may also include footage of workers.

Section 316 of the NSW *Crimes Act* requires that information, that might be of 'material assistance' to securing the apprehension or conviction of an offender who has committed a serious offence, is brought to the attention of police or other appropriate authorities.

NSW Health agencies must always view the footage first, before releasing to police, to review what has been captured. Where other patients are captured in footage and if their presence is unrelated to the offence the NSW Health Agency should consider pixelating their faces. This must be done in consultation with the police, as for the purposes of their investigation they may want to identify workers and patients as witnesses to an offence.

The camera surveillance footage must not be publicly available.

Password protection of recorded footage is required. Downloading access must be restricted to those workers who have been identified within the NSW Health Agency as having the authority to have this access. All surveillance camera monitoring is sensitive and restricted.

There may be multiple levels of access, a read only level that can only view records from a selected camera, read only access that can view all cameras but cannot download or change camera settings, authority to download and adjust camera settings but not delete footage and full access eg for technicians to install and program camera, settings and configure recording devices.

The standards set out in the *General Retention and Disposal Authorities* must be referenced in the retention and disposal of camera surveillance records downloaded and utilised.

13.7 Covert camera surveillance

The approval of the Secretary of NSW Health must be sought prior to the application to a magistrate for a covert surveillance authority. The NSW Health Agency must submit a written request addressing the following:

- why covert surveillance is required
- the actions taken to date to investigate and/or manage the situation
- other options considered by the NSW Health Agency to resolve or manage the situation and why they were not taken or were not successful.

Where the Secretary of NSW Health has granted approval for the NSW Health Agency to apply for a covert surveillance authority, all relevant requirements of the *NSW Workplace Surveillance Act* must be applied.

14. Role of Security Staff in NSW Health

Policy

As part of the facility security risk management process, NSW Health Agencies must ensure, in consultation with staff and other duty holders, that the appropriate level of security staffing is available to respond effectively and in a timely way to security related issues, at all times.

The appropriate level of required security staff must reflect the level of identified risk of security incidents/violence occurring, the size of the facility, the services being provided and the local community and crime demographic.

The role security staff are asked to undertake in NSW Health Agencies must be consistent with the scope identified in this Chapter, and summarised in the information sheet found on the *NSW Health security resources website*.

NSW Health Agencies must ensure other NSW Health workers understand the scope of the role undertaken by security staff.

Reference to security staff includes Health and Security Assistants (HASAs).

Standards

The Policy requirements set out in this Chapter must be achieved through the implementation of the following standards:

14.1 NSW Health security staff must have a current NSW 1A security licence

All security staff must have a current NSW Class 1A security licence. No other licence class is required to undertake a security role in a NSW Health Agency.

Security staff, as part of their Class 1A licence, can lawfully protect people within the premises that are being guarded (note the term 'guard' is used in the Security Industry legislation in the description for a 1A licence).

NSW Health Agencies must ensure that procedures are in place to check that security staff retain a current Class 1A licence and First Aid certificate eg a program of monthly verification on the NSW Government site that a security staff member continues to hold a valid security licence. Resources to assist recruiting managers to select appropriate individuals with the skills and capabilities to deliver security services in a Hospital environment are set out in the *NSW Health Recruitment Toolbox*.

Requirements for security staff undertaking security audits within NSW Health Agencies are covered in the NSW Health *Security Improvement Audit Policy*.

Master licence holders must ensure they comply with their obligations under the security industry legislation. More information about master licence requirements can be found in Chapter 2 Responsibilities and a guide on these obligations can be found at this link.

14.2 Security staffing must be determined by a risk assessment

Each NSW Health Agency must identify and assess hazards and risks relating to security/violence (refer to Chapter 1 Security Risk Management.

NSW Health Agencies must then assess the current identified level of risk of aggression or violence related incidents occurring, whether they are likely to increase or decrease, the security staffing resources required to assist clinicians with managing this risk, the other risk controls in place and the time required for security staff to undertake their other duties. This information will then be used to assist with determining the level of security staffing and the rostering required to address demand.

Determining the current and potential risk of violence and aggression, and therefore the required security staffing, must incorporate an assessment of the following, as a minimum:

- the type of services being delivered at the facility and the identified risk of aggression or violent incidents occurring (eg emergency departments, alcohol and other drug/mental health units or services working with issues related to violence, abuse and neglect, including domestic, family and sexual violence and child protection and wellbeing issues, where there may be a higher likelihood of violent incidents occurring)
- who is likely to use the service, including during local events where there is an increased number of population expected eg large festivals, tourist or community events
- the number of all workers on duty at any one time and their experience and skills levels, particularly in relation to violence prevention and management
- the size and layout of the facility, including those centres that are separate from a hospital, and the impact of this on response times (including when undertaking regular patrols)
- the likelihood and frequency of simultaneous multiple incidents occurring
- the nature of incidents that have occurred previously or are foreseeable (including the nature of incidents that have occurred in other facilities)
- the geographical location of the area and the population demographic
- the crime risk of the locality (Police can advise)
- proximity of local Police services and the response times, eg an isolated community
- the proximity of private security services and their response times, where these external services are utilised by the NSW Health Agency and
- the current security controls in place and their effectiveness in reducing the likelihood of violence occurring (eg patient risk assessment processes, access control measures).

14.3 NSW Health security staff must be an integrated part of a multidisciplinary health team

NSW Health Agencies must ensure security staff (and all other workers) understand the NSW Health security role clearly (including the boundaries between the security role and that of other Agencies such as the Police or Corrective Services) and how the role works within a multidisciplinary team.

It is critical that managers and workers, including security and clinicians, decide on and document (through the development of local procedures that reflect NSW Health policy) the way security staff will undertake the role in that NSW Health Agency and in particular how aggression and violence related incidents will be managed. Local procedures documenting the required role and actions of security staff must be consistent with the role for security staff set out in this Chapter.

Where there are both security staff and HASAs in the one location, action must be taken to ensure both security classifications operate as one integrated team with a strong professional relationship and an ultimate single line of professional reporting.

Security staff have specific expertise in identifying precursors to violent behaviour and it is therefore beneficial that, wherever possible, input from security staff is sought during patient violence/aggression risk assessments, as part of a multidisciplinary team approach to the care of patients.

As with all NSW Health workers, security staff must not (and must not be expected to) place themselves at unnecessary risk in carrying out their duties. In practice there may be times when a patient or another individual is displaying behaviour that may require intervention but **at no time** is this requirement prioritised over the safety of workers.

14.4 NSW Health Agencies must establish and utilise casual security staff pools

The required level of security staffing should be achieved primarily through the employment of security staff or HASAs.

NSW Health Agencies must however create and utilise casual pools of security staff where there is a need to fill a short–term position in a roster or a need for short term 'surge' staffing. Individuals on the casual pool must be given induction, information and instruction to ensure they understand the role of security staff in a health environment, specific duties, training in the required electronic systems and have completed all the mandated violence prevention and management training.

As far as possible priority must be given by NSW Health Agencies to utilising casual pools ahead of contracted security staff.

14.5 Managing the risk of utilising contract security staff

Where NSW Health Agencies have no option but to utilise contract security staff (including for on–call patrols), it must ensure that specific risks arising from this arrangement are identified and managed. This includes:

- ensuring the agency providing the staff and the individual security staff are provided with information of the role to be undertaken and if any changes are made to the role
- ensuring competence in the tasks they are required to perform. For example, if contractors are to be involved in code black teams or deal with violence and aggression, they must complete the violence prevention and management training

- ensuring contract staff understand their obligations to apply the procedures and standards of the Health Agency including the authorisations, consultation and decision making in place
- ensuring an understanding of the unique circumstances around the delivery of security services in a health environment
- understanding NSW Health policy on the role of security staff and standards for the delivery of those services etc
- the WHS obligations for orientation, training, instruction and supervision are managed and documented.

Requirements for ensuring the management of WHS legislative obligations in relation to contractors are found in NSW Health policy for managing WHS risks for other workers and include:

- taking a risk management approach in identifying hazards and assessing risks as required under *NSW WHS Act & Regulation* to eliminate or, where this is not practicable, minimise risk to health and safety that may impact on workers in relation to the work to be carried out
- providing and maintaining records of induction training, information and supervision as appropriate to the nature of the work and the severity of the associated hazards and risks
- ensuring that Personal Protective Equipment, where applicable, is provided, is properly fitted and is appropriate to minimise the risk to health and safety, and is suitable to the nature of work and any hazard associated with the work to be carried out
- ensuring provisions are in place to validate that other workers have the appropriate qualification/experience, licenses, training and skills to carry out the work in a safe manner
- evaluating and documenting, as appropriate, the performance of the the contract provider, and individual contracted staff, throughout and at the conclusion of the engagement as part of the continuous improvement process
- regular communication between the NSW Health Agency and the contract provider regarding the management of risks and issues that need to be addressed, including governance arrangements where subcontractors may be provided.

Procedures must be in place that require all security staff (including HASAs and contracted staff) to complete sign in/out registers and incident reports as required by security industry legislation. The Security Licencing and Enforcement Directorate (SLED) has further information on these requirements at this link.

The procurement procedures in place in NSW Health must be adhered to when engaging contracted security.

There is a **Whole of Government contract for security services (Integrated Security Services) and it is mandatory for NSW Health Agencies to purchase services from that contract.** There are limited exceptions to this mandatory requirement and they are when the NSW Health Agency can document that the services on the contract don’t represent value for money or they don’t cover the skills set required or they do not have security staff available in a particular location.

Any service agreement with a provider of contracted staff must also state that unauthorised sub-contracted staff must not be provided to the NSW Health Agency. Processes must also be in place to facilitate the escalation of issues related to the nature and timeliness of on-call external security contractor responses, where they are being used.

14.6 The role of security staff in NSW Health must have a strong emphasis on assisting with the early identification, prevention and management of incidents.

The frequency of certain duties for security staff may vary according to the type, location, size and local circumstances of the NSW Health Agency. In broad terms security staff work as part of a team in collaboration with other workers, to assist with managing patients, provide assistance to visitors, and assist with protecting workers and securing the assets of the facility.

It is not the role of NSW Health security staff to arrest people suspected of engaging in criminal activity or arrest an individual engaging in criminal behaviour on the direction of another person, search without consent, detain or forcibly retrieve individuals (except in limited circumstances outlined later in this Chapter), or manage high risk incidents such as those involving prohibited weapons or hostage situations.

Security staff, like other NSW Health workers, must contact the Police if there is suspected criminal activity or concerns about public safety in or around a NSW Health Agency.

To assist with differentiating the roles of security staff, paramedics, the police and corrections officers, where individuals are transported to NSW Health Agencies or between NSW Health facilities, reference must be made to the Memorandum of Understanding (MOU) between the NSW Health and NSW Police and Memorandum of Understanding between NSW Health and Corrective Services NSW.

Issues related to the nature or timeliness of the Police response to security incidents must be escalated to both the Chief Executive of the NSW Health Agency and any other appropriate forums, such as the Local Protocol Committee (usually made up of representatives from the NSW Health Agency, the Police and the Ambulance Service), to ensure resolution of issues. Processes must also be in place to facilitate the escalation of issues related to the nature and timeliness of private security contractor responses, where they are being used.

Security staff must be provided with suitable induction information and training consistent with the requirements outlined in the NSW Health Policy Directive on *Violence Prevention and Management Training Framework*, to ensure they understand the role expected of them and how it must be performed within the context of a NSW Health Agency and a therapeutic environment.

Appropriate and ongoing supervision of security staff must occur. This will ensure that support can be provided to security staff, training issues can be identified and standards reinforced.

14.7 When establishing security roles they must reflect the scope and standards set out in this Chapter

An information sheet summarising the scope of duties that may be undertaken by security staff in NSW Health Agency can be found on the NSW Health security resources website. To support this document following are some key areas of the NSW Health security role that require further explanation.

14.8 Physically (Manually) Restraining Patients and Others

The restraint of a patient or an individual in clinical care areas is the role of the clinical team, with supplementary support, if this is necessary, provided by security staff at the direction of clinicians. Prior to restraint all other prevention strategies must be attempted including:

- early identification of escalating behaviour
- use of de–escalation techniques.

Resorting to physical restraint must only be considered when these other strategies have failed or are assessed in the circumstances as not being appropriate. The use of physical restraint in health settings is intended to mean the use of reasonable force (person to person) to restrict a person's movement. Where that decision involves a patient the decision to restrain must be made by clinicians unless they are not available and the restraint is necessary to protect the patient or others (see section 14.8.3).

At all times, all workers involved in a physical restraint, are responsible for adhering to the following three principles:

1. Safety of the person being restrained, as well as the safety of others
2. Using only reasonable force, ie the minimum amount of force required to achieve safety of the person and others
3. Using force for only as long as is absolutely necessary to prevent injury or to allow a clinician to perform a medical procedure or administer necessary treatment.

Local procedures on the use of physical restraint must be developed (see Chapter 26 Violence for required detail). These procedures must be included in orientation/induction programs for individual facilities and communicated to security staff.

Security staff who are required to undertake physical restraint must receive relevant training in restraint techniques that reduce the risk of injury to workers participating in the restraint and to the person being restrained, such as:

- maintaining a clear airway to allow breathing
- grasping limbs, if required, near a major joint in order to reduce the risk of fracture or dislocation of small bones
- avoiding pressure on the persons neck, throat, chest or abdomen
- awareness of positional asphyxia, the population groups at greater risk and the early warning signs and
- monitoring the person's ability to breathe by monitoring movement, colour, respiratory rate and by talking to the person.

Further information on the safe use of restraint is set out in NSW Health Policy Directive *Seclusion and Restraint in NSW Health Settings*.

14.8.1 Using physical restraint on a medical practitioner's directive (referred to in this Chapter as non–capacity patients)

Except in certain specified emergency situations, as outlined in the Section 14.7 above, a decision to use physical restraint on a patient, who is **not** being cared for under the *NSW Mental Health Act* **must only** be made by a medical practitioner, who may then request the assistance of security staff **as part of the restraint team**.

A medical practitioner may seek the assistance of security staff to physically restrain a patient for the purpose of administering urgent and necessary medical treatment to save the life of the patient or prevent serious injury to the patient.

This direction to security staff can occur only where the medical practitioner has determined that the patient is incapable (either temporarily or permanently) of giving consent to treatment, and the medical practitioner has informed the security staff that the patient is incapable of giving consent. The power to provide emergency treatment in these circumstances must meet the requirements of the *NSW Guardianship Act* and this patient is referred to as a non–capacity patient in this Chapter. Issues of related to the giving of consent can be found in the *Consent to Medical and Healthcare Treatment Manual.*

14.8.2 Using physical restraint on patients on a registered health practitioners directive (mental health patients)

Physical restraint may be required for the purpose of managing a patient who is receiving care and treatment under the *NSW Mental Health Act.*

Physical restraint may be required to allow the registered health practitioner to administer urgent and necessary medical treatment, for example, administering sedation.

14.8.3 Using physical restraint on patients in response to threats of, or actual, violence/ assaults

The physical restraint of a patient must occur under the direction of a clinician/medical practitioner, except in **limited circumstances** such as:

- there are no clinicians in the immediate vicinity at that particular moment, and where failure to act immediately will clearly result in injury or trauma; or
- clinicians are unable to issue instructions (eg they are injured or incapacitated).

In the above limited circumstances security staff may need to restrain a patient or another person in situations where:

- a patient has assaulted another person and is, in the reasonable opinion of the security staff member, likely to continue to assault
- a patient is threatening to imminently assault another person
- a patient has destroyed or damaged significant property and, in the reasonable opinion of the security staff member, likely to continue to destroy or damage the property or
- a patient is threatening to imminently destroy or causing significant property damage.

In all of the above situations security staff must also form the view that the use of physical restraint is necessary to defend themselves or others.

Where security staff are involved in using physical restraint on a person this must be recorded after the incident to the standards required by the *NSW Security Industry Regulation* and the NSW Health Policy Directive *Incident Management Policy.*

Security staff are responsible for ensuring that their actions involve only the use of reasonable force.

14.8.4 Using physical restraint on others (non–patients) in response to threats of, or actual, violence/assaults

Security staff may need to restrain a person in situations where:

- a person has assaulted another person and is, in the reasonable opinion of the security staff member, likely to continue to assault
- a person is threatening to imminently assault another person
- a person has destroyed or damaged significant property and, in the reasonable opinion of the security staff member, likely to continue to destroy or damage the property or
- a person is threatening to imminently destroy or damage significant property.

In all of the above situations security staff must form the view that the use of physical restraint is necessary to defend themselves or others.

Where security staff are involved in using physical restraint on a person this must be recorded after the incident to the standards required by the *NSW Security Industry Regulation* and the NSW Health Policy Directive *Incident Management Policy*.

Security staff are responsible for ensuring that their actions involve only the use of reasonable force.

14.9 Using mechanical restraint on patients

Mechanical restraints must only be used on patients as a last resort. Chapter 26 of this manual outlines other strategies that may be implemented to reduce the need for mechanical restraint. The NSW Health *Seclusion and Restraint in NSW Health Settings* must also be applied.

The decision to apply mechanical restraints to a patient must only be made by the senior clinician designated to care for the patient or the medical officer, although security staff may assist with the application of the mechanical restraints.

In limited circumstances mechanical restraint can be used to manage the risk of serious imminent harm and where other appropriate, alternative options have been considered. Mechanical restraint can only be used for the briefest period required to allow the patient to safely regain control of their behaviour.

The team managing an incident where mechanical restraint is being used must be led by a senior nurse or a medical officer. The senior nurse on duty is responsible for ensuring that staff observing the patient in mechanical restraint are relieved regularly, preferably with no more than an hour at a time without a break, and that all required obligations including documentation are maintained ie restraint register. See Section 14.10 and 14.11 below.

The following NSW Health Policy Directives provide further standards relating to the use of mechanical restraints, including obligations and documentation requirements:

- *Seclusion and Restraint in NSW Health Settings*
- *Management of Patients with Acute Severe Behavioural Disturbance in Emergency Departments*

NSW Health Agencies must standardise the type of mechanical restraint in use, as far as practicable. See Chapter 26 Violence for detail on appropriate mechanical restraint.

14.10 Legal issues – Restraint as an act of self defence

Wherever possible workers must take evasive action to escape from a violent situation, including removing themselves, other workers, patients and visitors to safety, isolating the site where possible and withdrawing to await a Police response.

Where evasive action is not possible and there are no other options available, the law recognises that the use of force to protect oneself or others may be necessary if a person is under attack or attack is imminent. The use of force includes restraining an individual, where this is the only reasonable action.

Section 418 of the *NSW Crimes Act*, Section 52 of the *NSW Civil Liability Act* and the common law defence of self-defence provide legal protection where conduct is carried out by a person in order to defend themselves or another person in the event of actual physical assault (battery) which is likely to continue, or in order to prevent a battery that has not yet occurred but is threatened and imminent.

Conduct is carried out in self defence where the person believes the conduct is necessary to defend themselves, or another person, or to protect property and the person believes that the conduct was necessary and the conduct is a reasonable response to the circumstances as perceived by the person.

Restraint must be an act of last resort, and occur only until the risk has passed, such as when the person regains control of their behaviour or the Police are in attendance. The use of restraint in these circumstances must involve the minimum amount of force necessary to respond to the threat. Such a restraint is an act of self defence, not a citizen's arrest.

The use of force must be defensive rather than aggressive, controlling rather than punitive and with no more force than is necessary in the given situation. Force must not be applied for longer than is reasonably required to control any risk.

14.11 Legal issues – Restraint of a patient who is incapable of giving consent to medical treatment

Section 100 of the *NSW Guardianship Act*, as well as the common law defence of necessity (sometimes known as the common law defence of justification) provide protection where conduct is carried out by security staff in respect of a patient who is (in the opinion of a medical practitioner) incapable, either permanently or temporarily, of providing consent to medical treatment and where in the opinion of the medical practitioner the medical treatment is necessary, as a matter of urgency, to save the life of the patient or to prevent serious injury to the patient.

Security staff are not able to assist in the restraint of a patient, where the intended purpose of the restraint is to administer medical treatment, where the patient is legally capable of giving consent to treatment but who chooses not to have treatment.

This defence will be available where the medical practitioner informs the security staff the patient is incapable (either temporarily or permanently) of giving consent to the medical treatment and the medical treatment is urgent and necessary to save the life of the patient or to prevent serious injury to the patient.

14.12 Arresting without warrant – making a 'citizen's' arrest

Security staff cannot arrest individuals who they merely **suspect** have committed a crime. Security staff cannot be directed to arrest an individual who has committed a crime.

While Section 100 of the *NSW Law Enforcement (Powers and Responsibilities) Act* confirms that **any individual** may arrest a person (commonly referred to as making a citizen's arrest) if that person is in the act of committing an offence or has been observed by that individual committing an offence, it is the NSW Health position that in these circumstances the Police must be contacted to attend rather than NSW Health workers engaging in arrest.

Where there is suspected criminal activity on or around a NSW Health Agency, security staff must contact the Police, then depending on the circumstances, and the risks:

- make their presence known, without approaching or intervening, to deter ongoing activity or
- intervene by asking the person to desist in the behaviour or leave the NSW Health Agency or
- monitor the behaviour until the Police arrive, recording details for reporting to the Police.

Attempting to make an arrest, rather than reporting the crime to the Police, may carry an unnecessary risk of security staff being assaulted themselves or creating a potential for a complaint of false imprisonment.

A claim of false imprisonment arising from the arrest may occur if the person believes that they have been detained even for a short time, by the use of force or threat of force without lawful reason. A claim of false imprisonment may occur if:

- the security officer's belief that the person had committed a crime was unreasonable
- the arrest was based on a mistake and
- the security officer has acted beyond their lawful powers of arrest (such as keeping a person detained for an unreasonable amount of time).

14.13 Detaining Patients under the NSW Mental Health Act

Division 2 of Part 2 of the *NSW Mental Health Act* (the Act) (sections 19 to 26) sets out the circumstances in which a person may be lawfully detained in a facility. These include:

- on a mental health certificate given by a medical practitioner or accredited person (Section 19)
- after being brought to the facility by an ambulance officer (Section 20)
- after being apprehended by a Police officer (Section 22)
- after an order for an examination and an examination or observation by a medical practitioner or accredited person (Section 23)
- on the order of a Magistrate or bail officer (Section 24)
- after a transfer from another health facility (Section 25)
- on a written request made to the authorised medical officer by a primary carer, relative or friend of the person (section 26).

The Act is silent with respect to matters such as how a person can be detained. However the power to use reasonable force to detain a patient is generally assumed. If a person is detained under the Act in the above circumstances, there is an implied power that the facility, acting through its workers (including security staff) have the power to ensure the detention of the patient. Security staff may be required to assist with the detention. This power of detention would include the use of reasonable force to (i) detain the patient; (ii) prevent the patient from leaving the facility; or (iii) prevent the patient from harming themselves or others. What is reasonable will depend on the circumstances but in all circumstances only the minimum amount of force required to respond to a situation must be used.

14.14 Retrieving a patient who is attempting to abscond from a facility

If a patient has been legally detained in a mental health facility (as per the circumstances outlined in Section 14.13 above) and the patient is unlawfully attempting to escape or abscond from the facility that patient may be prevented from leaving the facility. As a way of actively assisting in the prevention of a successful attempt to abscond security staff must be advised in advance of patients who are not able to leave the facility.

Security staff must only assist in stopping a person from leaving a hospital where directed to by a registered health professional, and where that person is lawfully detained and unlawfully attempting to escape or abscond from their detention. The onus is on the registered health professional to ensure the direction to retrieve the patient is lawful.

Excepting non–capacity patients or patients lawfully detained under the *NSW Mental Health Act*, a patient must not be prevented from leaving a NSW Health Agency by security staff.

Where a patient proceeds off the NSW Health Agency property and where there are serious concerns about the safety of the person and/or others, the Police must always be informed. Security staff must not pursue an absconding patient after they have left NSW Health property.

Corrective Services, Youth Justice, Department of Home Affairs or Police patients in their custody must not be retrieved by security staff. This is the role of the relevant Agency.

14.15 Assumption of Care Orders

NSW Health Policy *Child Wellbeing and Child Protection Policies and Procedures for NSW Health* outlines the role to be undertaken by NSW Health Agencies where an Assumption of Care Order is made.

Where an Assumption of Care Order is in place NSW Health staff, including security staff, have no legal authority to detain a child or young person should the parent or carer attempt to remove that child or young person from the premises. In these circumstances the Police and the appropriate agency must immediately be informed.

As with all other situations that have the potential to become violent, action must be taken to identify any risks to workers or others and eliminate or minimise these risks as far as is practicable.

14.16 Code Black Response

Security staff, play a key role in the prevention and management of violent incidents, however this is most effectively achieved as part of a multidisciplinary team.

NSW Health Agencies must have procedures in place that provide for Code Black teams (also known as Emergency Response teams or Clinical Aggression Response teams), to assist workers and others who are at risk. Chapter 29 of this Manual provides standards for the identification, training and implementation of Code Black teams.

14.17 Increased security presence to assist clinicians

Where a patient needs increased clinical observation (eg specialling) or where the patient is being treated involuntarily eg under the Mental Health Act, or in seclusion (*refer to NSW Health policy on Seclusion and Restraint*) this must not be undertaken by security staff alone. Security staff are not trained (nor do they have a duty) to recognise patients whose physical or mental health condition could deteriorate.

It is appropriate for security staff to provide increased security presence to support the clinicians undertaking 'specialling' to observe the behaviour of a patient and to anticipate and prevent absconding or to assist with managing aggression, however this must occur under the direction of the clinician undertaking the 'specialling'.

Where rostered security staff are providing an increased security presence to assist clinicians providing increased clinical observations, arrangements must be made to ensure the remaining security team is fully staffed.

All security staff accompanying clinicians undertaking increased clinical observation must be provided with relevant information. This will include information about the patient being observed, including a summary of the possible behaviours related to the patient's clinical condition, and any known triggers that may indicate an escalation. Updates must be provided when/if changes occur.

The above does not preclude having security staff being present in a work area where an aggression risk related to a patient/s or others is identified. This proactive presence may occur through an increase in patrolling through the work area or with the planned placement of security staff in that area. At no time must the security staff member/s be expected to provide one on one observation (eg specialling as described above).

14.18 Searching patients and visitors and their property

To ensure the security of workers, patients and other visitors to NSW Health Agencies, there may be circumstances where the searching of patients and visitors is considered an important risk control strategy. Those searching must be cognisant of the potential for searching to be confronting for the individual and must therefore ensure the process of searching where ever possible is undertaken with respect, the persons dignity is protected and that during the search advice is provided to the individual about what is being done.

The power to search an individual, their bags or other property in their possession, is restricted in narrow circumstances under criminal law, requires the consent of the individual and must only be a frisk search.

A frisk search is defined as:

- a search of a person conducted by quickly running the hands over the person's outer clothing or by passing an electronic metal detection device over or in close proximity to the person's outer clothing or
- an examination of anything worn or carried by the person that is conveniently and voluntarily removed by the person (including an examination conducted by passing an electronic metal detection device over or in close proximity to that thing).

In these circumstances a search must be conducted by more than one person, who should both be of the same gender as the patient.

Security staff must not attempt to search a person without their consent, except in the limited circumstances outlined in the Section 14.19 Searching mental health patients.

In all other circumstances, a search may be considered illegal and an assault upon the person if:

- consent was not provided and
- there were no reasonable grounds to search the person and
- security staff did not introduce themselves and inform the person of the reason for the search and
- security staff are not the same gender as the person being searched and
- the search is excessive or conducted in any way that may be considered inappropriate.

Under the *NSW Inclosed Lands Protection Act* a NSW Health Agency, as occupier of its premises, has the right to determine who may enter its premises, and is entitled to impose conditions of entry.

Conditions of entry must be signposted at public entry points to the facility. An example of what they may include can be found at this link.

Where, after a risk assessment, a NSW Health Agency determines the need for procedures to deal with searching, where the individual consents to such a search, these procedures must be clearly documented.

The procedures must contain clear advice for clinicians and security staff involved in searching about:

- how to ensure consent
- how to maintain personal safety
- how to reduce distress / trauma for the person who is the subject of the search
- issues to be considered before conducting a search such as whether Police involvement may be more appropriate
- what to do where there is a suspicion that an individual is carrying a concealed weapon
- when and how searches may be conducted.

People entering the NSW Health Agency must be made aware of the conditions of entry, through clear and appropriate signage.

NSW Health Agency workers must be aware of their right to ask a transporting agency eg NSW Police, (that has existing powers to conduct searches) to search a patient on arrival at the hospital /health facility and a record of such a search should be kept.

As an alternative to searching visitors, the NSW Health Agency may provide lockers and require belongings to be placed in the locker prior to the visit or ask the visitors to show workers anything they want to bring into a clinical area.

14.19 Searching mental health patients

The situation is somewhat different in relation to mental health patients under the *NSW Mental Health Act*.

The searching of involuntary patients without consent is permitted, but only where such a search is pursuant to a direction by an authorised medical officer in circumstances where the medical officer thinks the action is necessary to protect a patient or person from serious physical harm, and the search is conducted appropriately in accordance with the NSW Health Agencies' procedures for searching patients.

Where a search is deemed necessary by the authorised medical officer, security staff or nursing staff can conduct a 'frisk'/pat down search (see Section 14.18) or an 'ordinary' search of a mental health patient. An 'ordinary' search means a search of a person or of articles in the possession of a person that may include:

a. requiring the person to remove his or her overcoat, coat or jacket and any gloves, shoes and hat; and
b. an examination of those items;

Under no circumstances must clothing be asked to be removed or lifted by security staff (apart from those outer layer garments specified above).

Where the Police or paramedics bring a patient who has been detained under the *NSW Mental Health Act* into a NSW Health Agency it must be established if a thorough search has already occurred. This search must be documented by the receiving NSW Health Agency eg in the medical record. NSW Health Agency workers, including security staff, may request that an initial or another search of the patient is performed by the Police or paramedic, and a record of the search must be kept.

Any workers, including security staff, involved in searching must be provided with instruction on searching. Security staff must not participate in any other form of bodily searching.

14.20 Accompanying patients being treated under the NSW Mental Health Act and who are being transported between and within NSW Health facilities

Security staff must only be expected to accompany a patient (without a registered health professional or paramedic present) when that patient has been assessed as low risk and is not sedated.

Patients who require transport and who have been sedated must be accompanied by a registered health professional. Security staff doing this transport are doing so under section 80 and 81 of the Mental Health Act.

Security staff must not be expected to accompany any other patient without a registered health professional present also. In these instances security staff are not responsible for the patient, rather they are there to assist the registered health professional.

NSW Health policies require a risk assessment to be done prior to transport so patients are only transported when it is safe to do so – thereby limiting the potential for them to become violent while in transit between facilities.

Section 81(4) of the *NSW Mental Health Act* allows for a patient to be frisk searched prior to transport if it is reasonably suspected that the patient is carrying anything that would present a danger to the person or any other person or that could be used by the person to abscond.

The following NSW Health documents provide further standards relating to the transport of patients:

- *NSW Health – NSW Police Force Memorandum of Understanding*
- *Mental Health for Emergency Departments: A Reference Guide*
- *Management of Patients with Acute Severe Behavioural Disturbance in Emergency Departments.*

14.21 Escorting Individuals (non-patients) from NSW Health Premises

As the preferred response it is not the role of security staff to escort individuals from NSW Health premises. In all but the most urgent circumstances the action to escort an individual (non-patient) from NSW Health premises must be undertaken by Police.

However in circumstances where the removal of an individual is immediately necessary and can not wait for the arrival of the Police and the individual's continued presence on NSW Health property is potentially creating a risk to any other person, a properly delegated/ authorised worker may exercise judgement and action to escort a person, under the powers provided by the *NSW Inclosed Lands Protection Act*.

A Chief Executive, through an instrument of authority/ delegation, can authorise individual NSW Health worker to exercise judgement and action to escort individuals from NSW Health premises. Where Chief Executives elect to authorise their security teams to undertake this activity, they must ensure that there are authorised individuals on each shift.

The Chief Executive, in authorising a NSW Health security staff member in this way, must be satisfied they have the competence and judgement to exercise the authority in an appropriate way. **As a minimum** authorised workers must have undertaken:

- de-escalation and evasive self-defence and personal safety techniques training (eg HETI Violence Prevention and Management – Personal Safety Training) and
- 3 day program *Security in a Health Environment* (if they are a security staff member).

The authorised workers can not be directed to take this action if the authorised worker does not deem the situation safe or necessary. If a risk to safety is identified the person should be accompanied from the premises by the Police. If during an escort the behaviour of the individual escalates the authorised person must summon the local Code Black team or Police as necessary.

The individual must be escorted to the NSW Health premises boundary. They must not be taken beyond this point.

14.22 Retention and Restoration of Weapons / Implements or Illicit Substances

On occasion people may present to a NSW Health Agency carrying items that give rise to security fears. This can occur, in particular, in emergency departments where due to the emergency nature of the presentation patients have not necessarily had an opportunity to properly secure or remove items, and the discovery may only arise once the person has been admitted as a patient.

Weapons / implements or illicit substances can also be discovered as part of a search to which a person has consented or from the searching of an involuntary mental health patient.

A weapon or implement may not be prohibited but still give rise to concerns for safety and security should a person retain it in their possession while on the premises of a NSW Health Agency.

While a person may be lawfully carrying a weapon, this does not entitle them to retain a weapon on NSW Health Agency property if it creates risks for workers, patients or others.

NSW Health Agencies must have procedures in place to manage issues associated with the identification, removal and retention of items from patients.

When developing these procedures, the following risk control strategies must be considered:

- people who handover custody of items to NSW Health Agency workers must, where practicable, be given a receipt for their property
- all items must be placed in an unused paper bag (or plastic if a liquid), to protect any forensic evidence.
- in the case of weapons or implements
  - where there are any concerns that the weapon or implement may fall into the category of a prohibited weapon, as defined by the *NSW Weapons Prohibition Act*, or carrying the weapon is against the law (eg juvenile with a knife), the Police must be contacted and advised of the nature of the weapon and circumstances of retention. Security staff must fill out an incident report describing all details
  - this weapon must then be placed immediately into a designated safe until collected by Police (refer to section 14.22 below on Storage and Disposal of Weapons)
  - if the weapon or implement does not fall into the category of a prohibited weapon but there are concerns regarding the nature of the weapon or implement (large knives, screwdrivers, slide hammers, etc), the Police must be contacted and advised of the nature of the weapon or implement and the circumstances of retention. An incident report describing all details must be completed
  - this weapon or implement must then be placed immediately into a designated safe until collected by Police (refer to 14.22 below on Storage and Disposal of Weapons)
  - under section 79 of the *NSW Firearms Act*, a health professional who is of the opinion that a person to whom they have been providing professional services may pose a threat to their own safety or to others if in possession of a firearm must notify Police of their concerns. Where a clinician identifies that a

patient has a prohibited weapon or other weapon and they are concerned about the risk from that patient to themselves or to others, they must notify Police immediately. Section 38 of the *NSW Weapons Prohibition Act* and Section 79 of the *NSW Firearms Act*, provide protection from civil or criminal liability, including breach of confidentiality when a clinician discloses information to the NSW police. Security staff must inform clinicians about patients who have weapons in their possession when they arrive at the facility

- should the person have lawful rights to that weapon or implement and it is necessary to return it to them on their departure from the premises of the NSW Health Agency, then the usual practices for managing patient's valuables must apply including:
  - Locking the weapon or implement into a safe and entering the details into a valuables book or equivalent, including the name and address of the owner. The owner must be advised that they have a period to claim the weapon after which time it will be destroyed
  - When returning the weapon or implement to the owner ensuring the item is signed for in the valuables book/or equivalent.

14.23 Storage and Disposal of Weapons or Implements

NSW Health Agencies must have procedures in place for storing weapons or implements awaiting collection by the lawful owner or by Police. The procedures must reflect the relevant requirements of the *NSW Evidence Act*.

When developing these procedures, the following risk control strategies must be considered by NSW Health Agencies:

- the weapon or implement must be placed into a designated safe which must be located in the Security Department (or other appropriate area) where access is restricted to security staff or facility managers only. Minimum standards for gun safes of this type are included in NSW Health Guideline *Management of NSW Police Force Officers Firearms in Public Health Facilities and Vehicles*
- the designated safe must be key operated. Security staff or facility managers must have access to the safe to ensure that weapons or implements are secured immediately
- the safe must be emptied by a nominated senior security staff member on a daily basis and the contents of the safe transferred to another safe which can be accessed by this senior worker only
- weapons or implements are to be kept in this safe pending collection by the lawful owner, police or disposal
- where a weapon or implement has not been collected by the lawful owner, and the required timeframe for keeping property has expired, arrangements must be made by the NSW Health Agency for its disposal.

15.Designing out Security Risk in the Clinical Environment

Policy

NSW Health Agencies must have a process in place for providing workers with information about risks and the controls in the physical environment.

Many risks can be effectively 'designed out' during the planning, design/ redesign of refurbishments or renovations and construction of new health facilities. Designing out workplace hazards must be the highest priority for controlling workplace risks.

NSW Health Agencies must ensure that they comply, as far as practicable, with the *Australasian Health Facility Guidelines (AusHFG)*, especially Parts B and C, which deal with security features in specific clinical environments and with the other NSW Health standards, as set out in NSW Health Policy Directives referenced throughout this Chapter.

The AusHFG and NSW Health policy are regularly reviewed to incorporate emerging best practice. These documents must be reviewed by NSW Health Agencies to identify any additional or new standards. If the current environment doesn't meet the standards and it is not practicable to make a change to the physical environment then other controls must be identified, by a risk assessment, to reduce the risk. Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all reasonably foreseeable security risks associated with the clinical environment are identified, assessed, eliminated where reasonably practicable, or where they can not be eliminated, effectively minimised.

Design must integrate where practicable and safe the guidance in Chapter 7 of *Elevating the Human Experience* and enhance the principles of trauma informed care.

Note: This chapter is related to the design of the clinical work location, for the management of a violent person refer to Chapter 26 of this Manual.

Note: For issues relating to workers in community settings refer to Chapter 16 Working in the community of this Manual for additional information.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

NSW Health Agencies must develop procedures, in consultation with workers and other duty holders, to effectively manage security risks in every clinical area.

The physical design/layout must reflect the specific risks identified for the clinical environment and be supported with clinical protocols/models of care that incorporate the assessment and management of risk, to both patients and workers, of potential or actual violence. This will include, where necessary, reviewing the design of the external environment to reduce risk associate with patients who are seeking to abscond/self-harm eg falls form height, crossing busy roads.

15.1 Designing out hazards in clinical areas reduces risk to workers and improves patient outcomes

Well designed areas that improve the human experience of both patients and workers can assist with reducing stress and anxiety, improve clinical outcomes and reduce aggressive behaviour. In addition to the standards set out in this Chapter refer to Chapter 4 Health Facility Design for further standards.

15.1.1 Design of desks and counters

The design of desks and counters must be determined by:

- their purpose of the counter and the services provided (including if cash is handled)
- the identified risk of aggression and violence and how/ when/where these incidents occur
- whether the desk is always staffed and within the line of sight of other workers (ie is there potential for isolated working)
- the requirement for a worker to be able to face a patient at all times

- whether workers are based behind the counter/desk and/or move around the workspace
- the availability of dual points of egress and safe retreat spaces
- the required security of records and information held in the area
- the confidentiality of the discussions that take place
- the equipment being used.

Staff working at desks/counters must have access to fixed and/or personal duress alarms to summon assistance (refer to Chapter 11 Duress Alarm Systems for additional standards).

Where the risk assessment identifies the need for the use of barriers/screens (eg in emergency department reception or other at risk areas) they must be fit for purpose eg safety glass, allow adequate communication to occur in the setting, and prevent a person climbing or reaching through and grabbing at workers.

15.1.2 Waiting areas (including sub–waiting areas) and common spaces must be designed to reduce risk

Waiting areas and common spaces where people need to congregate must incorporate the following standards:

- be comfortable, culturally appropriate, decorated in muted colours and be free of unnecessary clutter
- have adequate lighting, seating, ventilation and temperature control
- be fitted with furnishings that cannot be moved and/or used to cause injury eg linked rows of seating
- be sufficiently sized to give people 'space' and avoid the stress of overcrowding
- be fitted with camera surveillance if the area is not continuously monitored by a worker or where there are blind spots
- have a clear path to commonly used amenities (eg phones, water and vending machines, toilets etc)
- allow for a direct route between waiting areas and clinical areas to minimise access and risk to other areas
- in **emergency departments and other high risk areas**, have controlled access to clinical areas eg doors are locked and access controlled from reception/triage or other treatment areas (this may not be necessary in sub–waiting areas)
- in emergency departments, have signage that clearly directs patients and carers to the reception area, triage and the waiting area. Refer to:
  - *A Practical Guide for Improving Emergency Department Signage*
  - *Wayfinding for Health Facilities*
  - *Emergency Department Patients Awaiting Care*

Signage and regular communication that explains the stages of a patient journey and updates on waiting times may also reduce the risk of aggression.

15.1.3 Reception, write–up areas (including clinical workrooms) must be designed to reduce unauthorised access, entrapment and isolation risks

These spaces must incorporate the following standards:

- two exit points and a design that does not create entrapment or concealment points
- an appropriate barrier where there is a requirement for protection from violence, security of property or records, or privacy of clinical discussions
- layout must prevent the position of the patient and furniture/equipment from blocking workers access to an exit route or safe area
- the main entrance reception desk must allow for surveillance of everyone entering the facility
- speed of access/egress – doors must be designed to facilitate rapid exit
- must include duress alarms – fixed and/or personal alarms, as appropriate. Fixed duress alarms must be positioned to allow easy and unobstructed access by workers
- must include safety glass in any windows
- must not be in isolated areas, but close to and in view of other workers eg do not isolate work areas that are 24 hours 7 days a week by separating them with work areas that are only occupied in the day time or Monday to Friday.

15.1.4 Staff stations must be designed to reduce entrapment and isolation risks

Staff stations must incorporate the following standards:

- two exit points and a design that does not create entrapment points (they must be situated to prevent a person blocking both simultaneously)
- an appropriate barrier where there is a requirement for protection from violence or security of property or records
- doors that are locked and access controlled if the staff station is enclosed. These doors must be designed to facilitate rapid exit
- must include duress alarms – fixed and/or personal alarms, as appropriate. Fixed duress alarms must be positioned to allow easy and unobstructed access by workers
- must be located in a place that allows for good lines of sight ie not be in isolated areas, but close to and in view of other workers.

15.1.5 Rooms where patients and their carers/ family are seen by workers must be designed to prevent entrapment and support safety

Every room where patients and their carers/family are seen by workers eg triage rooms, family rooms, treatment/examination/consultation/procedure rooms, interview rooms and enclosed bays (but excluding bedrooms on wards, and class S and class N isolation rooms) must incorporate the following standards:

- two exit points
- incorporate space and formwork that allows the room to be laid out for workers to face the patient at all times
- positioning of furniture such as examination beds, desks, computers (including those on wheels) and telephones must be arranged so that the worker does not turn their back to the patient to use the computer or other equipment, or allow the patient to be between them and a point of egress
- access to fixed duress alarms as appropriate. Fixed duress alarms must be positioned to allow easy access by workers (where there is no dual egress fixed duress must be available at the front and back of rooms). In **emergency departments and mental health units** fixed duress alarms are used to supplement personal duress alarms not as an alternative to individual personal duress alarms
- access to lockable storage for equipment/implements, as necessary. Items laying in view and unsecured may be used to cause injury and must not be left unattended, and must be removed or secured when not in use
- windows and glass doors are constructed to be resistant to physical force ie use lamination, shatterproof film or security screens.

Rooms are not be used for a purpose other than what they were designated for unless they meet the requires standards as set out in this Chapter eg having multiple patients in a room designed for one patient or turning an administration or storeroom into a treatment space.

In bedrooms and isolation rooms, risks to staff and patient safety must also be identified, assessed and managed (see 15.1.7.2).

15.1.6 Open clinical treatment areas must be free of concealment and entrapment risks

Treatment areas (other than rooms) must incorporate the following standards:

- the layout does not create entrapment or concealment risks
- there is a line of sight from staff stations into all areas of the open plan clinical areas
- reduce the need for workers to turn their back on the patient to use the computer or other equipment
- separation between adult and paediatric beds and amenities (refer *to* NSW Health policy on *Children and Adolescents: Safety and Security in Acute Health Settings*)
- lockable storage for equipment.

15.1.7 Clinical areas for safe assessment of patients with Acute Severe Behavioural Disturbance (ASBD) must be identified

15.1.7.1 Safe assessment spaces in Emergency Departments must be fit for purpose

Dedicated clinical areas in an emergency department (eg safe assessment rooms) must be available to provide a safe area for the assessment and management of patients with ASBD.

These clinical spaces must be designed in consultation with workers, including mental health workers. NSW Health policy and guidelines for the design of Safe Assessment Rooms and the models of care to support these spaces can be found in the following:

- NSW Health *Guideline for Safe Assessment Rooms* developed by the Agency for Clinical Innovation (ACI) and
- NSW Health Infrastructure Design Guidance Note 039 – *Safe Assessment Room Design Requirements* (available on request from NSW Health Infrastructure)

15.1.7.2 Bedrooms, isolation rooms and other common spaces on wards for high risk patients must be fit for purpose

Wards may, from time to time, provide treatment to a patient who may also have behaviour that could deteriorate (or risk factors present that indicate this is possible). In order to ensure risks to these patients, other patients and workers are able to be controlled appropriate room/s must be identified in the design of wards. These identified rooms must incorporate the following standards:

- room location
  - single room, if possible
  - close to staff station
- have appropriate fixtures eg vents that are secure, mirrors appropriately affixed to the wall and made of a material to reduce shattering, have covered electrical outlets etc
- allow for limited access to cupboards (that aren't used for a patient's personal property).

When a patient is receiving treatment on a ward and is at risk of, or has, deteriorating behaviour the following standards must be applied:

- remove items that could be used as weapons
  - remove excess furniture from the room or common areas that can easily be used as a weapon or fit the ward with furniture that can not be easily moved
  - remove excess equipment (not required for immediate medical care) from the room, this includes IV poles, cables and leads, scissors. Do not leave equipment in the room if it is not in current use
  - check corridors and remove adjacent equipment that may be used as a weapon.

Areas in mental health units must be fit for purpose and require additional design features to keep patients and workers safe. Refer to the AusHFG for mental health units.

15.1.8 Staff only areas including meal rooms, offices and toilets must have controlled access (to ensure they cannot be accessed by patients or the public).

Staff–only areas such as meal rooms, tutorial rooms, offices and staff toilet and locker rooms must incorporate the following standards:

- have access controls to ensure they are secured from areas accessed by patients or others
- have signage to clearly identify these areas as staff only areas to reduce the likelihood of people 'being lost' as an excuse for trespass
- be fitted with fixed duress alarms to ensure workers can summon assistance in the event of a threat arising from unauthorised access to these areas
- have appropriate storage for items that could be used as weapons, particularly when adjacent to public access or patient care areas.

15.1.9 The design of all clinical areas must prevent unauthorised access and egress

Clinical areas and staff only areas must be appropriately signposted and secured to ensure access is controlled and to reduce the likelihood of people using 'being lost' as an excuse for trespass.

Assess the need to install:

- video surveillance at external entrances and entrances to units with a need for security or heightened vigilance (eg ICU, MHU, Maternity and Paediatric Units), internal access points such as unit entrances, waiting areas, car parks, and potentially high risk areas, eg where cash or pharmaceuticals are handled
- intercoms at entrances (internal and external)
- access control to the facility and units (eg ICUs, paediatric units, maternity units, geriatric units)
- consider how cameras are positioned, eg where there is a risk that babies or children might be removed, position (additional) cameras so that they show the faces rather than the backs of people leaving the unit.

Emergency Department public entry doors must have the capacity to be locked from a remote location that includes from a location that is within the line of sight of the door (this includes camera vision line of sight).

Other public entry doors, such as the main entry door to a hospital (if different to the Emergency Department entry), must be fitted with remote locking where it is determined by a risk assessment to be necessary.

Refer to *Chapters 9 Access and Egress* and *13 Workplace camera surveillance* for further standards.

15.1.10 Security of Medications (refer to Chapter 18 for standards)

Medications must have appropriate access controls in place.

15.1.11 Duress alarms

Workers must be provided with appropriate duress alarms as determined by a documented risk assessment and consultation.

Where personal duress alarms are provided, workers must wear them in accordance with local procedures.

Workers must wear personal duress alarms where they are required to answer public access doors after hours eg maternity units.

See Chapter 11 Duress Alarm Systems for further standards.

Other references:

Australasian College for Emergency Medicine Design Guideline

16. Working in the Community

Policy

NSW Health Agencies are required to ensure, in consultation with staff and other duty holders, that all reasonably foreseeable security risks associated with working in the community are identified, assessed, eliminated where reasonably practicable or effectively minimised.

NSW Health Agencies are required to ensure that the process is appropriately documented.

At all times workers carrying out duties in the community must have access to appropriate field equipment that allows workers to communicate and signal duress.

Workers must not carry out community visits alone where there is a history of violence by either the patient or other residents in the home, or the risk of violence is unknown.

NSW Health Agencies must ensure that a risk assessment is undertaken prior to a first visit to any client/patient and that the risk is evaluated before each ongoing visit to ensure any change is known and the control measures for safety are reviewed and remain appropriate. Where a risk of violence (including identified deterioration of the patient's behaviour) is identified before a community visit, or the risk is unknown, the need to provide the service in the community must be reviewed.

Workers must be continually aware of changing risk during visits and remove themselves from the environment, or summon assistance if that is not possible. At any time during a community visit if the risk escalates and/or a worker feels unsafe and decides to terminate the visit, this decision must be supported. Any change to risk must be documented in the risk assessment and the medical record. All incidents or near misses must be reported in ims+.

Standards

Working in the community involves work that is carried out in patients' or clients' homes, on the street or elsewhere outside of the NSW Health Agency premises, within community health centres and public venues such as schools or community halls and in mobile units.

Workers in the community may face a particular set of risks associated with working in environments that are not within NSW Health Agency premises. Workers in the community can work alone or in isolation, away from access to rapid support from other workers or even emergency services such as police.

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

16.1 Procedures to minimise security risks to workers must be in place

NSW Health Agencies must have in place procedures, developed in consultation with relevant workers, to ensure worker security, as far as possible, when working in the community.

These procedures must be documented, communicated and must cover:

- obtaining relevant client information from the referring clinician/service
- ensuring workers have access to patient information and records, including risk assessments, prior to the visit (ie home visits, community contact or contact in the community)
- the provision of adequate information to a worker away from the workplace who receives notification of another/unplanned visit, so they can assess the risk (eg verbal handover or access to laptop/internet coverage to look up patient notes) prior to arriving at that additional visit

- conducting documented patient and environmental risk assessment(s) to identify risks (including violence) and develop an appropriate care plan that addresses safety of workers. This must include information about who else is likely to be at the premises, the geographical location of the premises (eg what are the local crime demographics, relevant to risk of robberies/assault in the vicinity of the location/damage to vehicles), if the location is geographically isolated, and has reduced accessibility to/availability of police. It must also include issues identified with communication due to limited coverage for mobile phones/duress beacons etc.
- risks must be reviewed before every visit
- during the community visit workers must continue to evaluate/assess risks (ie environmental scans and dynamic risk assessment) and respond to ensure their own safety.
- after a visit any new risks identified must be documented in the clinical record and the risk assessment (as above) updated
- outline the personal threat response (Code Black) procedures while in the community. This includes calling 000 in an emergency. Equipment to raise a duress call/personal location emergency beacons must be fit for purpose (refer to section 16.4 Planning for and responding to personal threat – Code Black in the community).
- the appropriate ongoing support for workers which must occur. This is particularly where a real or perceived threat may arise in the event of an incident or where action is taken such as cancellation of a visit or redirection of a patient to a designated facility in a controlled environment include procedures for transfer of relevant clinical and risk information on a client when the client changes services or when the risk changes. This includes providing information to relevant external services such as the National Disability Insurance Scheme (NDIS) workers, Department of Communities and Justice (DCJ) workers etc.
- the means of tracking workers and check in/out procedures to ensure safe return and follow up if they don't return including procedures for responding to duress calls/alarms or triggered emergency beacons. This must include recording of vehicle registration and contact details for the workers (mobile phone number or other communication device provided)
- set out the requirement to report any incidents and update any risk assessments as needed.

The risk assessment referred to above must identify actions to be taken to control any identified hazards/risks:

- where issues are identified the controls must be discussed between the worker and their supervisor or senior colleagues before each visit eg in the safety huddle (See 16.2 and and the Checklist: General security precautions in for workers in the community at this link for more detail)
- collaboration (eg by phone) with the patient and their carer (as relevant) must occur, where appropriate, when developing the care plan/risk minimisation strategies.

Arrangements for developing and maintaining good communication and co-operation with local police and other local services must be established.

It is essential for their safety that workers have access to accurate, up to date information regarding contacts and locations. It is also important that patients and other clients have information about the purpose of visits, so they know what to expect.

16.2 Establishing and utilising plans and actions to manage any identified risk

16.2.1 Before the community visit

Where a risk of violence (including identified deterioration of the patient's behaviour) is identified before a community visit, or the risk is unknown, the need to provide the service in the community must be reviewed.

If a decision is made to see the person in the community then a range of controls must be in place, including that in no circumstances must the worker attend a patient alone. Additional controls will vary depending on the service to be provided and the level of risk identified, and may include:

- collaboration (eg by phone) with the patient and their carer (if relevant) to develop strategies to mitigate any violence (these may include those listed below)
- provision of care in a hospital facility (eg outpatient or ambulatory care)
- provision of care in a community facility
- provision of care in a public place eg coffee shop, local doctors surgery
- attend the visit with police or security escort
- attend the visit with additional workers
- provision of virtual care.

Strategies to control risk must be discussed between workers and their supervisor eg in the safety huddle, or as required when unexpected referrals/visits or changes to the risk occur.

16.2.2 During the community visit

If a risk of violence is identified during a community visit workers must:

- make an excuse not to enter the premises if the person answering the door gives cause for concern eg if they appear intoxicated, if the patient is not in, or if a potentially dangerous relative or other unknown person is present
- terminate the home visit if there is an obvious increase in numbers of people on arrival at or during the visit, or if there is any other overt or implied threat. The pre–attendance risk assessment must include information on who inhabits the premises on a regular basis
- immediately leave if firearms or other weapons are seen (the presence of weapons must be noted in the client's file and communicated to police and management). Workers must not return to these premises until the matter is resolved.

See the NSW Health security webpage for a checklist regarding general security precautions to help manage the risk for workers when community visiting.

Where there is a risk of violence and the available risk control strategies will fail to control the risks or resolve the issues, a NSW Health Agency representative must write to the household indicating that visits will not be made to that address and that alternative arrangements will need to be made.

Where a visit is occurring in a place where cars may be vandalised or where a worker have to travel through areas that are unsafe, arrangements must be made to allow the worker to travel and leave the area. This may include providing a driver or taxi for the worker to make the visit. This arrangement must consider how to ensure that the workers can immediately exit from the area safely. Where cars are used for community visits, auto locking vehicles are preferred.

Documented and practised plans to respond to workers who signal duress (Code Black) or do not follow check–in procedures must be in place. See sections below 16.2.4 and 16.5.

Patients, clients and/or carers must be given instructions to ensure that the house is illuminated (if required) and easily identified, access gates are unlocked and animals have been restrained when they are expecting the visit.

Ensure procedures for the safe transport of medications are in place as required. These must include the use of a locked unmarked bags/boxes while on a visit and the prompt return of medications to the patient care area on completion.

16.2.3 Equipment provided must be fit for purpose

Workers must be provided with adequate equipment, including:

- appropriate vehicles or other methods of transportation (eg boat):
  - suited to the terrain
  - appropriately fitted for the environment/location. This includes having emergency supplies including torch, blanket, water, and where terrain and /or remoteness indicate, a first aid kit, second spare tyre and/or tyre inflation pump and a spotlight on the side
  - vehicles must not have any markings identifying them as health service vehicles so as not to attract persons with intent to obtain drugs or other items of value and to protect patient privacy
  - fuel cards provided must be appropriate to the area (not all brands of fuel are available in all towns) or another method of paying for fuel identified.
- effective communication devices and a way to charge them, with reception in the areas to be visited (may require UHF radio, satellite phone or two devices such as radio and telephone to provide coverage)
- equipment that allows the worker to signal distress/duress, for example a personal duress device, mobile phone or personal locator beacon as appropriate to the locality and risk assessment
- reflective jacket/vest and torch
- maps, directories and/or GPS navigation devices. GPS devices are preferable (where GPS maps cover the relevant area) as they are hands free and therefore less distracting and safer to use when driving.

Consultation must occur with relevant workers when making decisions about the suitability of equipment (including communication technology).

16.2.4 Monitor worker movement and know what to do if they don't check in

NSW Health Agencies must establish a system where prior to commencing community based activities, the worker completes a movement sheet or similar so the base knows:

- the name, address and telephone number of the clients being visited
- the expected times of appointments
- the expected length of appointments
- any alterations to the schedule of visits or changes in daily routine (where the worker does not know these in advance they must be communicated to base as they occur) and
- the proposed route and map references eg for remote off road locations
- mobile phone number of the worker
- make and model and registration number of the vehicle.

The system must include procedures for checking return of workers and procedures to follow in the event of the workers failure to return or call in.

Tracking/movement sheets must not be left where they can be viewed, accessed or removed by unauthorised persons.

Local procedures must be developed and implemented to address requirements for communicating with base when visits are completed, if delays are encountered, if an incident occurs, or at other agreed times (eg end of shift). This must include the response when a staff member does not check in or answer communications.

16.2.5 Managing security risks related to after hours visits in the community

In addition to the requirements outlined above, workers who are required to visit clients in the community outside normal business hours, including in an emergency situation, can be particularly vulnerable.

A client must not be registered with the after hours community service prior to being visited and assessed by workers during business hours, unless all the controls for safe community visit are met. Existing processes for community visits must incorporate specific arrangements for after hours visits, including:

- two or more workers attend and/or security and/or police are present
- a monitoring system is in place to identify that workers have returned to base or proceeded home
- reliable information is known about whether:
  - the person needs to be seen after hours
  - the patient has a history of violence
  - the patient is currently being violent
  - the patient has access to a weapon
  - the patient has any known violent family members or associates
- duress response arrangements are in place.

Where a clinical need for a first visit after hours has been identified the manager, in consultation with the relevant workers, must be satisfied that the visit can be undertaken safely and that there is adequate information available, including about the risk of violent behaviour.

Where workers arrive at a site and identify a potential risk or workers feel their safety is at risk they must leave, or if that is not possible then they must immediately summon assistance eg call police. Workers are to withdraw until the arrival of assistance. Workers must not put themselves at risk.

If necessary, arrangements can be made for the person to be seen in an emergency department or police station or alternative safe venue.

16.3 After the visit

Procedures for workers must to take into account:

- arrangements for check out/report to base
- any incidents are reported as per local reporting protocols, eg via ims+, as soon as possible after the event
- any new or changing risks/hazards identified during the visit must be documented in the clinical record and the patient/environment risk assessment updated
- any other issues eg domestic and family violence or child protection must be reported/referred to the appropriate service.

16.4 Working in Isolated Clinics and Community Health Centres

Isolated sites can include clinics situated in school buildings (which are unattended at weekends, after hours and school holidays) and early childhood centres situated in community premises such as community halls.

NSW Health Agencies must ensure:

- at least two workers members are rostered on simultaneously
- clinic premises are secure, appropriately located and have a means of communication. In some circumstances it may be appropriate to also provide security services (where premises are leased from other agencies refer to Chapter 5 of this Manual for more information)
- workers carry a mobile telephone and, where required, a remote alarm, emergency radio and/or locator beacon in the event of an incident while travelling
- emergency and evacuation procedures are developed and communicated to workers (including pre–programming emergency numbers into phones, if possible)
- all major emergency phone numbers are prominently displayed and an effective contact network is established within the local community prior to the workers being at the site
- that doors are locked when clinics are not in session and that the doors are locked when workers are working alone out of clinic hours
- the facility is designed or cameras are installed to see people seeking entry to the facility without workers having to open the door (eg installation of a video intercom system)
- that all door and window locks are in good working order and maintenance problems are responded to and resolved promptly
- that blinds are placed on windows and workers close blinds after hours to reduce the likelihood of break–ins
- the visibility of computers, equipment etc is limited by placing them away from windows and doors

- a system is established where workers who are visiting external locations complete a movement log which establishes arrival and departure times, routes taken and any foreseeable difficulties with travel to and from the clinic
- a system is established where a workers leaving an isolated workplace advises another worker (including at another site) of destination, purpose and anticipated return. This will include procedures for what to do in the event of an incident or if the worker does not check in by the advised time
- the procedure for dealing with a worker that has "failed to notify or return" is practised. This procedure is to include a finalisation process (stand down) when the worker has been safely located. A worker nominated to be responsible for this task for each shift
- signage is displayed (eg that indicates that 'no drugs or money are stored on these premises' and that 'these premises are protected by alarm') that can act as a deterrent to would be thieves
- if medications are kept on a community health site in a patient care area/clinic they must be in a locked room or cupboard. If they are taken on a community visit they must be in a locked bag or box that can be taken on the visit and immediately returned to the patient care area (see NSW Health policy *Medication Handling in NSW Public Health Facilities*)
- prominently display signage about what is expected from clients relating to their behaviour (eg aggression is not acceptable)
- written information is provided to patients about appropriate behaviour and their responsibilities. This must form part of their service contract
- a duress response is planned, tested regularly and activated when the worker requires it
- that there are escape routes from the consultation room, ie two exits
- that room layout is such that the worker cannot be trapped and so that they do not sit with their back to the patient while accessing computers, telephones and other equipment
- all fire safety standards are met and that any fire extinguishers, hose reels, etc are appropriate and regularly inspected
- workers have safe and well illuminated access to ability to park and pack a vehicle given that services and vehicle packing may occur in the hours of darkness
- action is taken to establish an afterhours/weekend security presence where a risk assessment determines this is required.

16.5 Planning for and responding to personal threat – Code Black in the community

Workers must carry device/s to call for help on their person and not leave in a bag or other location that they may become separated from.

NSW Health Agencies must ensure a duress response is planned, tested regularly and can be effectively activated when the worker requires it.

Workers must be aware of how to initiate a Code Black – personal threat response procedures while in the community, including where this involves calling 000 in an emergency.

NSW Health Agencies must provide fit for purpose equipment to allow workers to signal a duress situation and if appropriate to support location finding, see 16.5.1 below.

Personal locator beacons, in particular, must be considered, particularly for rural and remote workers, to assist in locating a worker who has had an accident, a mechanical breakdown or is experiencing some other misfortune or injury.

Procedures for responding to a Code Black situation must be developed where this is a designated part of a worker's role.

In circumstances where clinics are located away from main buildings on health campuses and may therefore be considered isolated, Code Black arrangements must include a plan for how the response is provided for these workers.

16.5.1 Field Communication Technology

Workers in the community must have access to effective field technology to allow them to communicate and signal duress.

More than one device may need to be provided depending on local coverage and identified risks. The devices must be selected to give as complete communication coverage as possible. Suitable devices can include mobile telephones, satellite telephones, two–way radios, long–range duress alarms, personal location beacons and tracking devices that can provide the location of the person.

NSW Health Agencies must have procedures in place to locate workers in the community and may be effectively achieved through the use of appropriate field technology. These procedures and any technology to be used must be developed/decided in consultation with workers.

Any technology must be field tested prior to purchase to understand and manage any limitations.

When providing field technology the following elements must be addressed in local procedures and in training of workers:

- how to communicate with designated support systems (eg base, other workers, police)
- how to use/activate equipment correctly (including in Code Black situations)
- refresher training and emergency drills
- the limitations of the equipment
- testing, maintaining and operating equipment
- responding to Code Black incidents where this is a designated part of the workers role

Where a mobile phone is provided consider including use of the 'Emergencyplus' app to assist with providing critical location details when calling 000.

16.6 Training

Workers must be trained in:

- relevant policies and procedures (including adequate completion of the risk assessment, how to escalate issues/when not to visit, and alternatives to visiting), back to base communication, verbal de–escalation and defusion, evasive self–defence, negotiation and conflict resolution. Where possible these must include trauma informed approaches to assist in prevention of triggers for further distress/violence
- the correct use and maintenance of security equipment and field technology provided eg vehicles if off road driving is required, safety features of the vehicle, breakdown procedures, use of communication equipment including any features to call for help, use of GPS (if provided)
- what to do in the event of a Code Black situation
- Guidance and information for workers can be found at this link.

17. Security in Rural Health Services

Policy

NSW Health Agencies are required to identify and consider the factors specific to rural workplaces when ensuring, in consultation with workers and other duty holders, that all reasonably foreseeable security risks are identified, assessed, eliminated where reasonably practicable or, if they can not be eliminated, minimised and the process appropriately documented.

Where worker accommodation is provided it must be included in the facility risk management process and in the NSW Health *Security Improvement Audit* process (SIAT).

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

17.1 Risk assessments must take account of the specific additional risks arising from rural health settings

A number of factors are unique to the rural operating environment and can impact on of the level of risk experienced and the controls that are put in place to eliminate or mitigate these risks eg physical design controls such as locked perimeters and safe havens or airlocks where assessments can occur before a person gains entry into the facility after hours. These must be integrated into risk assessments where relevant.

Some of the factors that impact on the level of risk and on risk controls are:

- the type of work being undertaken
- geographical remoteness
- the timeliness of access to police and other emergency services
- communication difficulties/multiple devices required (eg no mobile phone coverage/blackspots/reliability and communicating with dispersed teams)
- access to training to build worker capacity to manage violence and security related risks
- small populations, close community ties and lack of anonymity
- road standards and driving times including risks from wildlife and farm animals on the roads
- climate (eg extreme heat or cold) and associated hazards including natural disasters (eg fire and flood)
- worker isolation and skill mix
- working arrangements such as on call and after hours services
- access to experts to maintain/repair equipment, vehicles and buildings
- timeliness of transporting victims or perpetrators out of the community, where that needs to occur
- access to services to transfer patients scheduled under the *NSW Mental Health Act* to gazetted inpatient facilities
- conflict between reporting requirements and community sensitivities
- facility design, including co-location of residence and clinic.

17.2 Appropriate Code Black arrangements must be in place and practised

A facility Code Black response plan must be developed and tailored to reflect what is available at the location in terms of workers and emergency services to respond when an incident occurs. A Code Black plan in a rural facility may require workers to retreat to a safe zone (when de-escalation is not effective), lockdown the key parts of the facility from this safe zone and call and wait for a police response. Where there is not an adequate number of trained workers available the Code Black response plan can not safely include provision for a patient restraint to be activated.

Rural health services can work in partnership with other community organisations and businesses to explore opportunities to combine resources (eg security patrols).

See Chapter 29 Code Black arrangements for more detail.

17.3 Further reference

Additional resources for both Health Agencies and rural workers are developed by CRANAplus and can be found at *www.crana.org.au*

18. Security of Medications

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all reasonably foreseeable security risks associated with pharmacy and other areas where medication is stored or dispensed are identified, assessed, eliminated where reasonably practicable or, where they can not be eliminated, effectively minimised.

NSW Health Agencies are required to ensure that the process is appropriately documented and effective procedures are developed and implemented.

Pharmacies and medication areas on wards must be constructed in accordance with the standards set out in the Australasian Health Care Facility Guidelines as amended from time to time.

This must be read in conjunction with the NSW Health policy *Medication Handling in NSW Public Health Facilities*.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

A risk assessment must consider at least the following:

- accessibility via window or door breaches
- security of the drugs safe and storage
- ability to detect intrusion – intruder alarms
- accessibility of the pharmacy from the roof / underfloor and availability of access to the roof / underfloor
- security of workers including duress alarms and duress response and camera surveillance, particularly for monitoring Pharmacies, Schedule 8 medication storage unit(s) and automated dispensing cabinets
- the ability to control, record and identify persons accessing pharmacy
- supervision where other workers require access to pharmacy and medication rooms for other purposes eg cleaning
- safe transport of medications.

18.1 Processes must be in place for Schedule 8 accountability

These processes must include the requirements to:

- maintaining a Schedule 8 drug register
- recording regular Schedule 8 accountability checks
- disposal of medications – approved workers, Schedule 8 destruction by authorised officer and is registered
- reporting Lost or Stolen Accountable Medication
- reporting a Lost, Destroyed or Tampered Schedule 8 Drug Register.

18.2 The physical design of Pharmacies must prevent unauthorised access

- Construct walls, floor and ceilings of the pharmacy out of solid material, with as few windows as possible. Any service windows must be constructed of safety glass (has features that make it less likely to break or pose a threat when broken eg toughened, laminated or wired) while being designed to provide for communication. Pharmacies and medication rooms incorporate measures to prevent unauthorised entry eg steel mesh or locked access panels or extended walls, to the underside of the floor slab above to prevent any intrusion over the wall or from the ceiling cavity.
- Reinforce windows on the perimeter walls to prevent entry. Existing windows may be reinforced by adhering a shatter resistant film or by replacing the glass with safety glass.
- Incorporate safety glass windows into the design of the front of the pharmacy to enable workers to carry out transfer operations with safety, while maintaining communication with workers and patients. The framework must be securely anchored, and anchor points concealed. It must not be possible to climb in between the window frame and the top of the wall/roof.
- Design a two door entry approach (ie one door for the public and one for hospital workers to enter to access front glass transaction windows and a separate door for the entry of pharmacy workers to the pharmacy).
- Ensure external lighting, camera surveillance, and restricted access are provided and are appropriate to workers accessing pharmacy after hours.
- Ensure adequate duress alarms and security response.
- Incorporate provision for closing off open areas at the front of the pharmacy when closed, (eg by a locked door from the corridor or locked shutter doors that do

not pose manual handling risks).

- Fit doors to the pharmacy with quality single cylinder dead locks to comply with fire regulations. Where practicable locks are to be key code or card operated externally and fitted with either a turn snib or handle internally to enable occupants to escape in emergencies
- Ensure that all door hinges are housed internally and cannot be accessed from the outside of the pharmacy
- Ensure doors are kept closed and locked to restrict entry. Fit doors with self-closing devices, and have the door connected to an intruder alarm. If the door is alarmed – it must emit an audible alarm as well as report to the portable communication/duress equipment carried by security and other incident response workers as relevant
- Ensure drugs of addiction are locked away and stored separately (apart from documents or cash) in a separate safe or vault securely attached to part of the premises and kept securely locked when not in immediate use. It must be out of the line of vision of patients and the general public.

18.3 The safe or vault for drugs of addiction (s8) must comply with the requirements set out in *NSW Poisons and Therapeutic Goods Regulation*

Unless otherwise approved by Director General (now Secretary of Health) the safe/vault must have the following characteristics:

a) it must be made of black mild steel plate at least 9 millimetres thick with continuous welding along all edges,

b) it must be fitted with a door made of mild steel plate at least 9 millimetres thick, the door being flush fitting with a clearance around the door of not more than 1.5 millimetres,

c) it must have a fixed locking bar, welded to the inside face of the door near the hinged edge, that engages in a rebate in the safe body when the door is closed,

d) it must be fitted with a five lever key lock (or a locking mechanism providing at least equivalent security) securely fixed to the rear face of the door,

e) if mounted on a brick or concrete wall or floor, it must be attached to the wall or floor by means of suitably sized expanding bolts through holes 9 millimetres in diameter drilled in the rear or bottom of the safe,

f) if mounted on a timber framed wall or floor, it must be attached to the wall or floor frame by means of suitably sized coach screws through holes 9 millimetres in diameter drilled in the rear or bottom of the safe,

g) if mounted on any other kind of wall or floor, it must be attached to the wall or floor.

Where a key is used to unlock the safe/vault, it must be retained by a registered pharmacist, or the authorised officer of the Pharmacy Service at a facility where no registered pharmacist is employed/contracted, on his/her person. After-hours, the key may be retained in a safe/key safe to which only a registered pharmacist/authorised officer of the Pharmacy Service has access. Where a code or combination is required to unlock the safe/vault, this must only be known to authorised registered pharmacists, or the authorised officer of the Pharmacy Service at a facility where no registered pharmacist is employed/contracted

A drug of addiction that requires refrigeration may be kept in a refrigerator rather than a safe if all of the following requirements are met —

a) the refrigerator must be in a room (which includes a part of a room or an enclosure) to which the public does not have access,

b) the refrigerator, or any cupboard or receptacle in which the refrigerator is kept, must be securely attached to a part of the premises,

c) the refrigerator, or the room, cupboard or receptacle in which the refrigerator is kept, must be kept securely locked when not in immediate use,

d) keys must be managed as for a safe (above).

e) the refrigerator must not be used to store any other item that is not a substance listed in Schedule 2, 3, 4 or 8 of the Poisons List or is not a therapeutic good.

Install an intruder alarm system that meets Australian Standard AS2201 and incorporates a duress alarm/s to enable workers to activate the alarm in the event of an emergency. Install intruder alarms to pharmacies and drug safes. Intruder alarms must include detection of breaches to doors and windows including glass breakage detection where relevant.

Access to the Pharmacy Service must be restricted to workers authorised by the director of pharmacy, or the authorised officer of the Pharmacy Service at a facility where no registered pharmacist is employed/contracted. Protocols for authorising and auditing access to the pharmacy by keys or other means must also be implemented by the Director of Pharmacy/authorised officer of the Pharmacy Service.

Restrict access to the pharmacy to authorised workers only and controlling this by:

- fitting single cylinder key, code or card operated dead locks to perimeter doors
- having a restricted keying system fitted to the locks in order to prevent duplication of keys

- strictly regulating the issue of keys, codes or cards at all times, including provision for after hours access
- keeping doors closed and locked to restrict entry
- installing closed circuit television monitors at access doors to screen entry of personnel and record any access to the pharmacy after hours
- entering the Pharmacy Service after hours should rarely be necessary. When required, access must be in accordance with procedures approved by the Drug and Therapeutics Committee and restricted to delegated senior nursing and/or medical workers. Such entry to the Pharmacy Service must not include access to Schedule 8 medications
- the facility's security staff may enter the Pharmacy Service after hours at times of an emergency, such as during a fire or an alarm sounding. Any keys or codes used for emergency access to the Pharmacy Service must be held under maximum security
- facilities must develop appropriate systems for recording every occasion of after–hours access to the Pharmacy Service, including documenting the purpose of this access.

Ensure, where the risk assessment warrants it, that mobile workers have personal duress alarms.

Processes must be in place for stock management:

- receipting deliveries (both in and after hours)
- maintaining a register for reporting lost, destroyed or tampered Schedule 8 drugs
- regular checks of stock.

18.4 Medication storage in hospital wards/ patient care areas

18.4.1 Storage of Drugs of Addiction (Schedule 8)

- Drugs of addiction that are kept in a hospital ward must be stored apart from all other goods (other than prescribed restricted substances) in a separate room, safe, cupboard or other receptacle securely attached to a part of the ward (floor or wall). The lock must be a five lever lock, or have a locking mechanism which provides at least equivalent security.
- The medications must be out of line of sight of the general public and patients.
- When new facilities are built, or existing facilities renovated, any remaining wooden Schedule 8 cupboards should be upgraded with the installation of metal safes.
- Stock levels of Schedule 8 medications should be kept to the lowest practical level

The registered nurse or midwife in charge of a hospital ward must ensure that:

- the room, safe, cupboard or receptacle is kept securely locked when not in immediate use, and
- any key or other device by means of which the room, safe, cupboard or receptacle may be unlocked is:
  - kept on the person of a nurse or midwife in–charge whenever it is in the ward, and is removed from the ward whenever there is no nurse or midwife in the ward, or
  - it is kept in a separately locked safe to which only a nurse or midwife has access, and
- any code or combination that is required to unlock the room, safe, cupboard or receptacle is not divulged to any unauthorised person
- the key should be kept separate to all other keys
- the registered nurse/midwife in charge of the patient care area would hold the Schedule 8 medication storage unit key/s, and hand the relevant key to each registered nurse/midwife or authorised prescriber requesting access to the Schedule 8 medication storage unit as required. When the particular task is completed, the registered nurse/midwife or authorised prescriber must immediately return the key to the registered nurse/midwife in charge of the patient care area
- if the nurse/midwife in charge is not available eg on a break, the key can be handed to a delegated registered nurse/midwife. However, in the case of a Schedule 8 medication storage unit within an operating theatre, a delegated registered nurse/midwife in charge or an authorised prescriber (such as an anaesthetist) should hold the key on behalf of the registered nurse/midwife in charge
- when a patient care area is closed for any purpose, any keys to that area's Schedule 8 medication storage units should be either:

  a) Stored in a metal torch and drill resistant key safe, securely attached to the wall or floor of the patient care area, or

  b) Handed over to the registered nurse/midwife in charge of the facility, or

  c) Handed over to the facility's Nursing and Midwifery Administration for securing in a safe or a key safe, or

  d) Handed over to the facility's security service for securing in a safe or a key safe.
- any spare keys to a patient care area Schedule 8 medication storage unit should be retained in a safe or key safe at the facility's Nursing and Midwifery Administration. A code or combination required to unlock the Schedule 8 medication storage unit must only be provided to a registered nurse/midwife or an authorised prescriber, in accordance with local protocols. Regular changing of this code or combination is required, also in accordance with local protocols

- Schedule 8 medications must not be transferred to medication trolleys for administration during a medication round, except where provided for in accordance with protocols approved by the facility's Drug and Therapeutics Committee. Where this practice is approved, at the conclusion of the medication round the Schedule 8 medication packs must be returned to the Schedule 8 medication storage unit
- patient care areas that are routinely closed over short periods of time (for example on weekends) must be securely locked to prevent unauthorised access. When a patient care area is closed for longer periods, the Schedule 8 medication packs should be sealed with tamper evident tape or in tamper evident packs, and transferred in accordance with local protocols to another appropriate patient care area Schedule 8 medication storage unit or to the Pharmacy Service.

18.4.2 Storage of Schedule 4 Appendix D Medications

- Schedule 4 Appendix D medications must be stored apart from all other medications and goods (such as keys, cash and documents), except:
  a) When stored in the Schedule 8 medication storage unit, or
  b) When stored on an emergency trolley, anaesthetic trolley, or operating theatre trolley. In these cases, Schedule 4 Appendix D medications must be kept at minimal levels and the trolleys kept in a locked room when the patient care area is closed, with access only by authorised persons.
- Where Schedule 4 Appendix D medications are stored apart from Schedule 8 medications, this must be in a separate safe or cupboard securely attached to the premises, and which is kept securely locked when not in immediate use. This can include but is not limited to the 'Schedule 8 drug cabinet within a Schedule 4 Appendix D drug cupboard' model.
- A code or combination required to unlock the Schedule 4 Appendix D medication storage unit must only be provided to a workers authorised to access the medication. Regular changing of this code or combination is recommended, in accordance with local protocols.
- Where the same key is used to access both Schedule 4 Appendix D and Schedule 8 medications, this key must be kept separate from all other keys (other than another key used to access a separate Schedule 8 medication storage unit).
- Where Schedule 4 Appendix D and Schedule 8 medications are stored in the same storage unit, the procedures for the custody of the Schedule 8 medication storage unit key must be followed as above. This will restrict access to the key to a registered nurse/midwife or an authorised prescriber. Where provided for under local protocols approved by the facility's Drug and Therapeutics Committee.
- Schedule 4 Appendix D medication packs may be moved to a medication trolley for the purpose of administering doses during a medication round. At the conclusion of the medication round, the Schedule 4 Appendix D medication packs must be returned to the Schedule 4 Appendix D medication storage unit.

18.4.3 Storage of Unscheduled, Schedule 2, Schedule 3 and Non–Appendix D Schedule 4 Medications

- These must be stored out of patient and public access, preferably in a locked room or a locked cabinet securely attached to the wall or floor of the premises, with the following exceptions:
  a. On a medication trolley used for medication rounds, which should be kept in a locked room when not in use, or
  b. On an anaesthetic trolley or operating theatre trolley which is kept in a locked room when not in use, or
  c. Minimal quantities of medications on an emergency trolley, or
  d. In a secure cabinet (such as a bedside cabinet), including that used for patient self administration in an approved program, in situations for which it may be impractical to attach the cabinet to the wall or floor of the premises. (Note: Schedule 8 medications must not be included in a bedside storage unit for self–administration. Local protocols should determine whether Schedule 4 Appendix D medications are included for patient self–administration and if so, provide for the requirement for these medications to be stored apart from the other medications).
- The key, code or combination used to unlock the room, cabinet, or trolley must only be provided to a registered nurse, registered midwife, an enrolled nurse, or authorised prescriber, as approved by the registered nurse/midwife in charge of the patient care area.
- In accordance with local protocols approved by the facility's Drug and Therapeutics Committee, the registered nurse/midwife in charge of the patient care area may also approve access to the room, cabinet or trolley by Pharmacy Service workers.

- Separately stored Non–appendix D Schedule 4 Medications.
- In accordance with local protocols approved by the Drug and Therapeutics Committee specific Non–appendix D Schedule 4 medications may be stored in separate (discrete) medication storage areas with similarly separate key, code or combination access to all other medications to minimise the likelihood of misappropriation.

  Examples of medications that may be considered for separate storage include propofol, methoxyflurane and the Schedule 4 codeine phosphate compound preparations. Non–appendix D Schedule 4 medications that are also accounted for in a register at the patient care area must also be managed as accountable medications, with any loss, theft or deficit reported to Pharmaceutical Services Unit.

18.4.4 Storage of Medications in Automated Dispensing Cabinets

The use of automated dispensing cabinets in patient care areas should include the following:

- the automated dispensing cabinet(s) must be securely attached to the wall or floor of the patient care area in a manner approved by the facility's security service
- an alarm monitoring system approved by both the facility's Drug and Therapeutics Committee and security service should be included to detect and alert any tampering or unauthorised movement of the automated dispensing cabinet(s)
- the automated dispensing cabinet system should be evaluated against the Core Processes detailed in the Institute for Safe Medication Practices 'ISMP Medication Self Assessment for Automated Dispensing Cabinets' to confirm the safe and quality use of the system
- separation of Schedule 8 and Schedule 4 Appendix D medications from all other medications is required
- medications must be stored in the automated dispensing cabinet in the packs received from the Pharmacy Service
- electronic access to the particular medications in the automated dispensing cabinets must be restricted to workers authorised to administer those medications and approved by the registered nurse/midwife in charge of the patient care area. However, in accordance with local protocols approved by the facility's Drug and Therapeutics Committee, Pharmacy Service workers may be permitted access to the cabinets for the purpose of stocking medications, other than Schedule 8 medications
- Schedule 8 medication stocking must be completed by a registered nurse/midwife with a witness (second person) authorised by the registered nurse/midwife in charge of the patient care area
- each workers must be assigned unique electronic access to the respective medication receptacles within the automated dispensing cabinet that the person is authorised to access
- the use of an authorised 'second person' to witness medication administration must include that person logging into the automated dispensing cabinet system to access the particular medication required
- all access events by workers must be recorded and retained in the automated dispensing cabinet system for the purpose of audits
- the automated dispensing cabinet system must include back–up provisions to access medications in the case of a power failure or electronics malfunction
- the implementation of protocols for conducting regular audits to detect unauthorised use, review the safety of the system and review the efficiency of the system.

18.5 Transport of medications

Ensure a procedure is in place for the safe transportation of drugs to wards and other clinical areas.

- Transportation must be under the direction of a registered pharmacist, or the authorised officer of the Pharmacy Service at a facility where no registered pharmacist is employed/contracted. The package containing the Schedule 8 medication must be handed by the facility worker to a registered nurse/midwife, who must sign and date a receipt confirming the quantity of the medication supplied. This receipt must be returned by the facility worker to the Pharmacy Service for retention. A copy of this receipt must also be retained at the patient care area.
- Alternatively, a registered nurse/midwife from a patient care area may collect Schedule 8 medication ordered from the Pharmacy Service by the registered nurse/midwife in charge of the patient care area. The registered nurse/midwife collecting the medication must sign and date a receipt confirming the quantity of the medication supplied, and again the receipt must be retained at the Pharmacy Service. A copy of this receipt must also be retained at the patient care area.
- In both scenarios, the registered nurse/midwife receiving the Schedule 8 medication must immediately record the acquisition in the patient care area Schedule 8 drug register and immediately store the medications in the patient care area's Schedule 8 medication drug storage unit. A witness must be present to confirm both actions by the registered nurse/midwife and sign the relevant entry(s) in the patient care area drug register.

When transporting medications within a facility consider the ability for a person to recognise that medications are being transported, the need for provision of a duress alarm, the need for an escort, maximising surveillance camera coverage on their route, not to stop for a break during transport, using a safe and direct route and if possible vary the route within these principles.

Ensure a procedure and equipment (e.g. a safe bolted to the boot of the vehicle) for secure transportation are in place for the secure transportation of drugs to other facilities within area of responsibility or hub. Procedures must ensure that drugs are accounted for and itemised receipt signed by the receiving facility. Procedures must be in place to track worker whereabouts relevant to workers transporting pharmaceuticals to other facilities.

Where a courier is used to transport schedule 8 medications:

- the Schedule 8 medication must be packed by the Pharmacy Service separate to any other goods and the outside of the package must not indicate that it contains Schedule 8 medication, and
- the courier must sign and date a document to confirm he/she has collected the package, and this document be retained at the Pharmacy Service. The courier must obtain a ‘proof of delivery’ receipt (either electronically or in hard copy) for the unopened sealed parcel from the person to whom the parcel is delivered
- collection of medication or delivery must happen in secure environment. If not possible, arrange collection/delivery in conjunction with other workers
- the courier must then arrange for this ‘proof of delivery’ receipt to be forwarded to the Pharmacy Service that supplied the medication
- the registered nurse/midwife who receives the medication at the patient care area must sign and date a receipt confirming the quantity of the medication(s) received
- this receipt must be forwarded by the registered nurse/midwife to the Pharmacy Service within 24 hours, for retention at the Pharmacy Service. A copy of this receipt must also be retained at the patient care area.

Chapter 16 Working in the community of this manual deals with *security of medications* when used in the community and includes standards in relation to the need to have locked bags/containers for transporting medications and tracking workers.

19. Security in Car Parks

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all reasonably foreseeable security risks associated with car parking are identified, assessed, where reasonably practicable eliminated or, where they can not be eliminated, effectively minimised.

The risk assessment is appropriately documented.

NSW Health Agencies must ensure contractors/external parking service providers who are responsible for parking arrangements on NSW Health Agency sites have procedures in place to control security risks, developed in consultation with the NSW Health Agency.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

19.1 Location of car parks must be assessed for security

- Car parks must be designed and located for maximum security for workers, patients and visitors as far as practicable.
- Car parks located on hospital grounds must be assessed for risks associated with falls from height and these risks eliminated or minimised. This includes screening around the perimeter at levels above the ground floor and reducing foot holds close to the perimeter at height.
- All access routes between the car park/s and facility building/s are well lit, under camera surveillance and have good line of sight so that persons approaching can clearly be seen.

19.2 Designating car parking for workers and others

- Afternoon and night shift workers are, where reasonably practicable, to be provided with designated, controlled parking spaces as close as possible to the facility in a well lit, easily observed area connected to the facility by well lit paths.
- To manage allocated car spaces for afternoon and night shifts, NSW Health Agencies must ensure entry to designated worker parking areas in dual purpose car parks is controlled.
- Where in use, exit boom gates should operate automatically (eg after a certain time a card is needed to enter, but exit can occur any time).
- NSW Health Agency fleet vehicles must be parked in a secure overnight car park with good lighting and regular security patrols. A fenced compound or lock-up garage is preferable.
- Facilities that provide treatment to custodial or forensic patients must identify dedicated parking arrangements for Corrective Services NSW, Youth justice and relevant NSW Health fleet vehicles arriving for scheduled medical/mental health appointments or emergencies. This is to assist with limiting the opportunity for a custodial patient to abscond.

19.3 Security in car parks

- Security personnel must undertake frequent high profile patrols in car parks associated with the facility.
- Security personnel must undertake random checks on vehicles in a car park (eg door unlocked, window down, valuables exposed etc) and secure the vehicle if possible.
- Vehicles left in the car park for a number of days are to have the registration checked with NSW police to determine if they are stolen.
- Signs must be displayed in car parks reinforcing theft awareness
- Signs must be displayed that advise that regular patrols are undertaken and surveillance camera monitoring is in place, where that occurs.
- Security escorts for workers at the conclusion of afternoon and night shifts between the facility and the carpark may be provided. This would include designating a mustering spot for workers to assemble.

- All car parks (and access routes as relevant) must have:
  - good lighting (refer to AS1158.3.1, AS4485.1.5.2 and Chapter 12 of this Manual) throughout the car park. Lighting fixtures must be vandal resistant
  - emergency telephone or intercoms direct to security personnel or switchboard
  - landscaping and design which leaves the area open and does not intrude upon line of sight. Including routine garden maintenance to maintain line of sight
  - flexibility to close some entrances and exits during low traffic periods
  - approved locks on exits intended for emergency exit only
  - camera surveillance
  - emergency/assistance call points
  - routine maintenance of lighting and other systems.
- Restrict the parking of delivery vehicles to a parking dock.
- All facility vehicle keys must be held by the designated custodian when the vehicle is not in use, and taken by the driver when the vehicle is required.
- Areas for secure storage of bicycles and motorcycles must be provided (ie lockers or storage areas, a stationary rack that secures the frame and both wheels without a chain, or a stationary object the user can lock the frame and wheels to with their own cable chain and lock).

Workers must be provided with information about safe parking. A sample of information to be provided to workers can be found at this link.

See Chapter 16 Working in the community of this Manual for more advice on parking away from a health facility.

20. Security of Property

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all potential for theft and wilful damage is identified, assessed, eliminated where reasonably practicable or, where it can not be eliminated, effectively minimised.

NSW Health Agencies are required to ensure that the process is appropriately documented and effective security procedures are developed and implemented to minimise theft.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

20.1 Prevent theft and damage of property

Every case of theft and wilful damage must be reported to the police. If the theft involves a worker, no arrangements must be entered into to accept settlement eg resignation on condition that the NSW Health Agency refrains from instituting legal proceedings.

- Assets and property registers must be kept up to date, providing full descriptions of each item, including serial numbers where they are required. This is for assets over $5000 or items considered attractive as outlined in the *NSW Health Accounting Manual for Public Health Organisations* (pages 1.16 and 1.17).
- Separate registers of donated items, equipment of historical value, antique furniture or other items of historical, heritage or cultural significance must be kept.
- A register of property theft and wilful damage must be kept to assist with identifying problem areas or patterns of behaviour. (This could be a report from ims+ or from security logs).
- All theft must be investigated.
- The possibility of impersonation of a worker if uniforms/work identification are stolen must be considered.
- All assets must have a unique physical marking, such as barcode, micro dot systems, digital photography, nano marking, invisible marking pens or chemical identification. This includes items of historical, heritage or cultural significance which must be invisibly coded.
- Attractive portable items must be stored (laptops, iPads, mobile phones and other electronic devices etc) separately in a locked area. Only designated workers must have access.
- An effective key control program must be in place and enforced (for more information refer to Chapter 10 of this Manual).
- Surveillance camera monitoring of identified high risk areas may be utilised (refer to Chapter 13 Workplace Camera Surveillance).
- Alarm systems must be installed (refer to Chapter 11 of this Manual for more information).
- Effective perimeter and internal access control must be in place (refer to Chapter 9 Access Control of this Manual for more information).
- CPTED principles must be applied when designing/refurbishing facilities (refer to Chapter 4 Health facility Design of this Manual for more information).
- Risk of theft must be reduced by ensuring that obsolete equipment with no historical value is written off and disposed of correctly and promptly.
- Items of historical, heritage or cultural significance displayed must be kept in secure display cabinets with shatterproof glass, secure locks and, where risk assessment indicates a need, alarms that respond to any breach of locks or glazing. The cabinets must be under camera surveillance and located in high traffic areas to reduce opportunities for unobserved theft.
- Security screens must be installed in areas that are not continually staffed, eg reception areas, so that valuables such as telephones and computers are secure.

20.2 Specific Areas for Attention

20.2.1 Engineering/Maintenance

- Controlled access must be in place to areas where tools or equipment are stored.
- All tools or equipment must be branded or stencilled to show ownership.
- Written record of tools or equipment on loan from one section to another must be kept.
- Workers must understand their responsibility for the equipment allocated to them.

- Vehicles must be parked away from storage areas to reduce opportunities to steal items.
- Regular checks of inventory must occur.

20.2.2 Transport

- Fuel pumps must only be operated by authorised workers. The fuel pumps must be locked when not in use.
- Regular audits of fuel pump use must occur and unauthorised use reported.
- Purchased vehicles must have a secured fuel cap cover (key (remote or physical) locked or other internal car release) and inbuilt security devices (eg data dot technology, ignition locks).
- Vehicle running sheets and fuel purchase details must be monitored and compared to distance travelled.
- Where practicable ensure that vehicles are securely garaged or parked in compounds. Garages and compounds must be subject to security inspections on a regular basis.
- All property transported in vehicles (eg laptops) must be removed or secured when the vehicle is unattended.
- Conduct frequent and random inspections which include attention to:
  - complete and current compilation of vehicle running sheets
  - replacement of original parts, accessories or tyres.
- Inspect and recording details of each vehicle's condition, including an inventory of all accessories fitted before the vehicle is sent to the dealer or auction for disposal.

20.2.3 Laundry/Linen

- Deliveries must be met and signed for.
- Delivery weights (quantities) must be checked against delivery dockets. A signed copy in the Linen Supply Area must be used to check against amounts and quantities charged for.
- Linen must not be left on open trolleys in areas where it can be pilfered unobserved, eg loading docks, infrequently used corridors or corners, unsecure bays. Where practicable, linen must be stored in a lockable room or linen bay.
- Access to linen stock rooms in wards and facility areas must be limited, and have minimum stock levels.
- Vehicles must be parked in areas away from the linen supply area.
- Individuals must not take personal bags into the linen supply area.
- Spot checks of linen levels held against stock records must be conducted.
- Spot checks of facility areas which have been allocated linen must be conducted to look for:
  - excess stock, above the agreed imprest levels
  - shortage of stock.
- Soiled linen bags must not be left outside wards or in easily accessible positions.
- Keep records of the quantity of soiled linen bags picked up from each area.
- Display posters relating to the theft of linen and the consequences. These must be placed in strategic areas where they are visible.
- Ensure babies are not discharged in NSW Health Agency clothing or blankets.

20.2.4 Catering

- Regularly review work areas and levels of stores held, querying large stocks.
- Check supplies ordered against menu cycle to determine if quantities ordered are comparative with the menu cycle.
- Check comparable deliveries for quantity, quality and delivery dockets signed. Deliveries must be immediately moved to secure storage areas.
- Ensure that fridges and store areas are locked at all times when not in use, and only opened for stocking or to take supplies necessary for the meal that is to be cooked. Consider installing time delay alarms to alert when a door is not secured or is opened without authority.
- Ensure that lockers are provided for workers personal bags and that these are not stored in kitchen areas.
- Restrict the amount of food retained in the kitchen to minimum quantities.
- Ensure that windows are screened to prevent goods being passed outside.
- Order commercial sizes of items to limit theft. However packaged quantities must not be of such a size that they pose a manual handling risk to workers.
- Do not allow utensils or equipment to be borrowed by kitchen workers. The facility name must be stencilled or marked on portable items (eg food preparation knives and food trays).
- Do not allow leftover food to be taken home. This can cause over–cooking to create a surplus and encourages taking more than just leftovers. Ensuring additional meals that may be diverted for non–patient consumption are not provided as part of the meal run.
- Prevent unauthorised access to the kitchen. Unauthorised persons are not allowed in the kitchen area unless accompanied by a senior kitchen worker.
- Ensure that all stores and fridges are locked when maintenance work is being carried out (except when workers are working in the stores/fridge).
- Regularly check trolleys used to transport food from the kitchen for food or other goods that should not be there.
- Ensure that stocks of food held in wards are kept to a minimum.
- Food equipment must not be left lying around or reserves of cutlery maintained in clinical areas.

- Knives fitting the description of Cleaver, Chef's knife, Paring Knife, Carving Knife, Utility Knife or Boning Knife must be stored in a dedicated lockable drawer to secure these items when not in use.
- Ensure vending machines are in high traffic/populated areas to create a passive surveillance situation.

20.2.5 Stores

- Ensure workers are aware of stock control procedures for incoming and outgoing goods.
- Conduct stock takes of consumable stores and check all items listed in the assets register – both quarterly and when there is a change of management.
- Keep stock levels to workable minimums.
- Check invoices against the stock card to ensure goods received are marked on records, and requisitions for store goods against stock cards.
- Ensure that all goods received are signed for and compared against orders in the Goods Inwards books.
- Ensure that goods being delivered to facility areas are not left in accessible places and vehicles are not left unattended. Goods received must be immediately located in a secure area.
- Ensure that goods to be distributed to areas within a facility are receipted/signed for at the receiving area with copies of signed paperwork kept with the receiving area and stores area. Goods must be checked to ensure they have not been tampered with, where possible full boxes must be ordered to reduce the opportunity for theft.
- Check altered requisitions for accuracy before acceptance. Internal requisitions that have been altered must not be acceptable under any circumstances.
- Conduct physical checks to look for broken packages or seals, and to ensure that all packages of large stocks have not been tampered with.
- Prohibiting bags being taken into the store area.
- Locate, as far as practical, stores away from public areas and change and lunch room areas.
- Ensure that products such as detergents are issued in commercial sizes to restrict theft, though packages must not be so large as to create a manual handling risk to workers.
- Ensure that vehicles are parked in an area away from the store (unless unloading).
- Restrict entry/exit to the store to only one door which is able to be observed by supply/stores workers.
- Ensure that only authorised persons are allowed in store areas.
- Examine garbage removal devices to ensure stock articles are not being transported out of the store area. Garbage removal areas must be separate from stores areas where possible to prevent articles being transported out.
- Lock away items such as batteries.
- Ensure that stocks held in areas are securely stored and not easily accessible to patients and unauthorised workers. Where possible, ward stores need to be locked and accessible only to the nurse or unit manager or their delegate.
- Regularly review imprest system to ensure stock levels are appropriate.
- Ensure stores returned dockets are used and signed by the ward area if goods are returned from areas to the store.
- Conduct regular checks of areas to ensure there are no hidden stores.

20.2.6 Administration

- Secure administration areas to prevent access to unauthorised persons.
- Ensure that the administration area is not left unoccupied during work hours or securing the area if it is to be left unoccupied.
- Keep records containing sensitive information secured at all times. They must only be made available to authorised persons (Refer to Chapter 21 of this Manual for additional information).
- Ensure laptop computers are password protected and securely stored when offices are left unattended.
- Store bulk office consumables in a lockable area and nominating one member of the administrative workers to issue bulk stationery requirements. Only keep minimum necessary amounts of stock in accessible locations.

20.2.7 Mail Deliveries

- Ensure receptacles for mail are clearly labelled and cannot be accessed or opened by unauthorised persons.
- Limit the access to the mail areas or use a sign–in / access card system.
- Ensure deliveries of mail are made in a restricted, defined area with appropriate access control.
- Keep the area for receiving incoming/outgoing mail separate from other operational/public areas.
- Ensure that incoming mail (including registered mail/ courier packages) is kept in a secure location to prevent loss and unauthorised access until it can be delivered to the addressee.
- Keep registered mail/couriered packages separate from other incoming mail and establish procedures for receiving and promptly securing registered mail/ couriered packages.
- Ensure pigeonholes are in secure areas accessible only by workers.
- Ensure all mail work areas are visible to supervisors.
- Ensure emergency procedures as per Chapter 25 Bomb threat (Code Purple)/Terrorist Threats are in place.

20.2.8 Cash Handling

Where cash is collected by third parties (eg armoured car transport of Health monies, ATMs and vending machines) arrangements with these parties must include identification of responsibility for record keeping and for safety and security, including arrangements for cash in transit

Where cash is managed by the Health Entity the following standards apply:

- Ensure cash handling, receipting and banking practices are consistent with the document entitled *Accounting Manual for Public Health Organisations*. These and further requirements are outlined below:
  - each hospital must have reviewed its cash services with a view to rationalisation. For hospitals with an adjusted daily average over 100 – a review of the cash services must be performed at least annually to determine appropriateness of services, procedures being complied with, suitable workers employed etc
  - one person must be responsible for processing and storing cash
  - the person responsible for cash must not be in an openly accessible position, there must be adequate barrier to prevent unlawful access to cash
  - cash and valuables must be stored in a safe located in a closed office. At a minimum the safe must have a single lock with the key being the responsibility of the person responsible for the cash. For hospitals with an adjusted daily average over 100 – if several people have access to the safe/cash storage facility, a system must be in place so that responsibility for shortages can be identified to any one person or any particular time by means of access records. Ensure workers with access to the safe understand that records of access are kept
  - Each hospital is to maintain a record of all locations where workers handle cash. If there is only one cash collection point then this is not required
  - procedures must be in place to ensure: receipt procedures are checked, supervisors check all cash handling duties, receipts and revenue are reconciled daily, cash handling workers are provided with information and understand their duties and responsibilities, and worker rotation is introduced where practicable
  - there is to be a central cash depositing facility. For hospitals with an adjusted daily average over 100 – the central cashier is to issue a covering receipt for all monies received from cash services or cash collection outposts
  - a receipt (manual or cash register entry) is to be issues on every occasion cash or property is received. Each receipt is to be accountable and pre numbered, and have provision for the date, the name of the issuing officer and location (if a cash receipting outpost), payment type (eg cash, cheque) and what the receipt is for
  - cash is to be banked at least weekly and more frequently if monies received total $400 or more
  - all deposits are to be reconciled between the total of receipts and the bank deposit advices
  - if the hospital has cash operated machines the undermentioned functions are to be undertaken:
    - machines where possible are to have two-key access
    - two or more workers are to clear machines
    - workers who collect cash are to reconcile the total amount of cash collected with the amount of cash deposited by using a daily balance sheet and signed receipts
    - amounts collected and receipted from coin machines are to be checked against accounts, meter readings or stock records. Where meters exist a book is to be maintained recording meter readings when cash is collected and said book is to be reconciled against amounts receipted on a regular basis by a supervisor.
  - for hospital/facility managed cash collection points two workers are to transport cash within the hospital/facility and to the bank.
  - workers transporting cash are to vary times and routes where and when possible. Routes must be in public places (not isolated), where possible they must be designed to maximise CCTV coverage, be well lit, avoid areas where people could hide, workers are to be aware of people around the workplace and suspicious vehicles. Do not carry cash in bags or containers that can be identified as containing valuables. Consider if communication or duress devices are required. Also consider other hazards such as slip/trip/fall or hazardous manual tasks eg if transporting bulk coins
  - each hospital is to have an Accountable Books Register:
    - all accountable books and documents, eg receipts, are to be numbered with all documents being recorded in the register
    - distribution is to be recorded, viz. date, name, section
    - completed documents are to be returned, with said return being recorded
  - each hospital is to have a formal (written) procedure for taking action and reporting thefts and or any other possible fraud. The procedure is to have as key elements the requirement to report to the Board and Police
  - each hospital is to conduct a surprise audit of cash handling procedures at least annually (internal audit)
- Ensure emergency procedures as per Chapter 29 Code Black arrangements, which include armed hold up response) are in place.

20.2.9 Patients' Property

- Information given to patients before admission must advise that:
  - Large sums of money, items of significant value, monetary or otherwise, must not be brought into the facility and that the facility will not accept any liability for their safekeeping and that monies and valuables are kept in the ward by the patient at their own risk
  - While the facility will take all due care to ensure the safekeeping of a patient's valuables or monies, it will not be financially liable for any loss of money or valuables.
- NSW Health Agencies must have procedures for the receipt of patient property which include:
  - when they accept patients' property or valuables for safekeeping, including where there is an emergency admission, must ensure that there is a list of that property. Money or valuables must be placed in an envelope with the patients' identifying details (eg MRN)
  - a receipt provided to the patient with the details of the items, signed by the worker in the presence of the patient or another worker countersigning as witness and a copy attached to the envelope
  - The valuables or money must then be placed in a safe in a centrally secure location, Note: Where money is placed into the Patients' Trust Account the details must be entered into the Patients' Valuables Register
  - Property held in safekeeping must be checked against the original list / receipt on discharge of the patient
  - All discrepancies or reports of such valuables or money going missing must be fully investigated by the facility, and where required, notifications made to the NSW Police and / or the Independent Commission Against Corruption (ICAC).
- Ensure that random checks are made of the Patient's Valuables Register against the envelopes held in the safe and against the Patient's Trust Account ledger, to ensure monies and valuables are secure
  Note: This may be subject to a patient's authority if the patient has explicitly indicated no–one is to have access to items held on their behalf.
- Make random checks on withdrawal authorities to verify the balances of monies held and that all valuables are accounted for
- Provide a means of securing individual wardrobe lockers or closets for clothing (if lockers are provided)
- Ensure that patients mark items that will be laundered by the facility with their name
- Issue receipts if a facility accepts patients' clothing for safekeeping. A locked cloakroom must be used to store the clothing.
- Routine ward level checking of food trays and linen, for patient property such as hearing aids/dentures must occur.

For further information refer to the NSW Health *Accounting Manual for Public Health Organisations.*

20.2.10 Workers' Property

- Discourage workers from bringing large sums of money, personal documents or belongings into the workplace.
- Ensure that workers are provided with a lockable storage area (eg individual locker or cupboard) for safe keeping of their property.
- Signpost areas such as locker rooms and cafeterias to warn workers to keep their valuables secure.
- Workers must notify if uniforms or work identification / access cards are stolen.

21. Security of Information

Policy

NSW Health Agencies are required to ensure that all reasonably foreseeable security risks associated with the protection of information and material (including electronic information*) from unauthorised disclosure are identified, assessed, eliminated where reasonably practicable or, where they can not be eliminated, effectively minimised.

NSW Health Agencies are required to ensure that the risk management process is undertaken in consultation with workers and other duty holders, is appropriately documented and effective plans and procedures developed and implemented which ensure compliance with relevant legislation, information security standards and Government policy.

For policies about protection from cyber–attack please contact eHealth or local information technology (IT) departments. Refer to the *NSW Cyber Security policy*.

**** 'Electronic information' is defined as information that is electronically created, processed, held, maintained and transmitted by NSW Health. It also refers to information held for, or on behalf of, other government agencies and private entities. This includes emails.***

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

- Ensure procedures, and a management structure with responsibilities up to the executive level, for information security management is in place.
- Procedures must include arrangement for backing–up of records to ensure business continuity.
- Buildings/spaces where paper and electronic records are kept must be access and climate controlled and have inbuilt, where practicable, automatic fire suppression systems.
- Arising from the risk assessment, an information security plan is developed, documented and implemented which outlines risk control strategies.
- Training is provided to workers on information systems and the controls in place to manage security information risks.
- A data custodian is identified with the responsibility for establishing and maintaining an acceptable level of data protection, for managing the disclosure of data, for ensuring the data is used in accordance with the reasons for which it was collected and that the data is complete and of acceptable quality and is available to authorised users.
- System administrators must follow acceptable procedures for granting/revoking access, ensuring that access rights for individuals are commensurate with the nature of the role being undertaken, identifying and resolving known vulnerabilities and monitoring system access.
- The record-keeping system includes information on the location of records within storage areas and the tracking of the movement of records.
- Procedures include the retrieval, handling, safe transport of records, and the return of records to storage.
- Inspection logs/documentation confirm that records are being retrieved from storage and handled correctly.
- There must be a process to ensure IT technical staff correctly and securely configure systems such as servers, networks firewalls and routers.
- IT technical staff must understand the business use and risks associated with technology being used so that security solutions match the criticality and sensitive nature of the systems.
- Procedures that ensure sensitive information is only released to organisations and individuals who demonstrate a need–to–know. The need to know will vary depending on the type of record. Procedures must also cover the arrangements in place for access audit logs where records have been accessed.
- Information is to be stored and processed away from public access.
- Information can only be removed from agency following a documented process and approval of that identified need.
- Disposal of information is by secure means.
- Information transmission and transfer are by means which deter unauthorised access.
- Workers who have access to sensitive information are aware of their responsibilities and provided with information regarding these.

Note: NSW Health Agencies are required to ensure that where external parties have access to NSW Health information they understand information security requirements and ensure that adequate security controls are in place.

Internal procedures must outline any standard processes for protectively marked material, including:

- creation and storage
- dissemination and use
- archiving and disposal.

21.1 What is sensitive information and how it is labelled

Sensitive official information must be protected from unauthorised access. NSW Health Agencies must use dissemination limiting markers (DLMs) to mark such information, whether it be in electronic, paper or other format. See Appendix 21.1 for the minimum handling requirements of DLMs.

Consistency in labelling will ensure that confidentiality and consistent controls are implemented for sensitive information within a NSW Health Agency and across NSW Health.

The *NSW Government Information Classification, Labelling and Handling Guidelines* set out the requirements for labelling.

The key aspects of the Guidelines are as follows:

- **UNOFFICIAL information is not work related.**
- **OFFICIAL information** is related to the agency's business but does not have security or sensitivity issues. This information does not need to be labelled but agencies may choose to do so. This information is still important to government and may still need security measure to protect the integrity and availability of this material.
- Sensitive information, if compromised, may cause limited damage to individuals, organisations or government. The Australian government uses one DLM (OFFICIAL: Sensitive). NSW uses six DLMs to describe the type of sensitivity of the information.
  1. OFFICIAL: Sensitive – NSW Cabinet
  2. OFFICIAL: Sensitive – Legal
  3. OFFICIAL: Sensitive – Law enforcement
  4. OFFICIAL: Sensitive – Health information
  5. OFFICIAL: Sensitive – Personal
  6. OFFICIAL: Sensitive – NSW Government.
- These DLMs can also be used with security classifications.

In addition to the above there are three security classifications under the Australian Governments Protective Security Policy Framework (PSPF):

1. PROTECTED
2. SECRET
3. TOP SECRET.

The *NSW Government Information Classification, Labelling and Handling Guidelines* provides standards for the preparation, handling, removal, auditing, copying, storage, disposal and transmission of sensitive information and must be utilised by NSW Health Agencies when developing local procedures.

21.2 Security of Employee Records

There must be processes in place to ensure security of employee information related to employment records, including:

- recruitment records
- payroll and banking records
- leave records
- performance management
- grievances and misconduct
- workers compensation records
- medical condition and illness records.

21.3 Security of Personal Health Information

Personal health information must have appropriate security safeguards to prevent unauthorised use, disclosure, loss or other misuse. 'Appropriate' will be defined by the circumstances in which the information is stored and used.

The *NSW Health Privacy Manual for Health Information* and the *NSW Health Privacy Management Plan* provide guidance material to assist NSW Health Agencies to comply with the security requirements established in the NSW *Health Records and Information Privacy Act*.

21.4 Security of electronic information storage

Where official information is stored on equipment, including laptop computers, action must be taken to ensure:

- all access to information is password protected
- equipment is appropriately and securely stored ie kept under lock and key in office areas,
- equipment is only left in cars where absolutely necessary, if it must be left it is locked in the boot
- computer system servers must be located in secure, climate controlled locations away from public corridors where possible
- all records are removed from equipment prior to disposal
- computers are locked when not in use.

21.5 Disposal of information

NSW Health Agencies must have a local procedure for the disposal of information.

NSW Health Agencies must refer to the *General Disposal Authority* (General Retention and Disposal Authority (GRDA) No.17: Public health services: Patient/Client records and General Disposal Authority No.28: Administrative Records) issued by State Records NSW in determining how long to retain worker, clinical and client/patient records.

The NSW State Archives and Records authority outlines the process for the disposal of records at this link.

An appropriate disposal/destruction process for sensitive records must consider the use of locked bins, in-house shredding and sanitisation (for digital records). The destruction of records must only be done following a local approval process. An authorised officer must view and record the destruction. If the destruction is carried out by a contractor they must specify the method of destruction, destruction must be on the same day as collection and certificates of destruction must be provided.

21.6 Further Reference

- NSW Health Policy Directive *Electronic Information Security Policy*
- Department of Premier & Cabinet Circular M2012/15 *Digital information security policy*
- NSW State Archives Standards for the physical storage of state records
- *NSW Health Privacy policies*
- *NSW Health Privacy Internal Review Guidelines*
- *Australian Government Information Security Manual*
- *Government Information (Public Access) Act 2009*

Standards:

- AS/NZ – HB231:2004 – Information Security Risk Management guidelines
- AS/NZS ISO/IEC 27000 series – Information Security Management
- AS ISO 55001:2014 – Asset management – Management systems – Requirements

Appendix 21.1

Minimum handling requirements for NSW DLMs (taken from NSW Government Information Classification, Labelling and Handing Guidelines | August 2020)

A set of minimum handling requirements for sensitive information applies to DLMs. Each NSW DLM describes a different category of information sensitivity and each refers to different NSW Government legislation. The legislation drives the purpose of the information collection, how this information should be managed and who can and cannot access this information.

Whether intentional or unintentional, unauthorised disclosure of OFFICIAL: Sensitive information can have serious consequences. All agency staff are employed under a code of conduct which imposes obligations of confidentiality.

All sensitive information is important, and a set of minimum handling requirements are set out below:

Key ✓ Do ✗ Don't ? Check

Collecting

✓ Collect information only for a lawful purpose that is reasonably necessary, and directly related to a function or activity of the agency. Collection methods, including online surveys, must have secure storage.

✓ Label digital information that is collected. This includes information captured via automated processes, for example via batch processes or API. This information should be labelled in metadata if the system allows and/or via system documentation ideally at the time the system is developed.

Labelling

✓ Label sensitive or security classified information at the time of collection or creation. Labelling is not retrospective, if information is not in use, there is no need to re-label with new labels. Information in use should be re-labelled. Agencies with large volumes of information with out-of-date labels should re-label information according to its risk profile.

✗ If receiving information that is already labelled, do not re-label. If there are questions about the validity of the label consult the data originator.

? Labelling of entire systems and large datasets needs to be carefully considered as this could restrict access to information unnecessarily. Labelling at field, case or record level may be more appropriate if the system has the capability. Access to field, case or records with higher sensitivity within a system or large dataset can be managed via user access permissions, only giving access to users that need-to-know.

Monitoring

✓ Monitor information over time to determine if the sensitivity of the information has changed. Change the label and security classification if required.

✓ Keep access audit logs for the appropriate retention period to assist in future audit and access control monitoring. Protect these logs from accidental or deliberate modification.

Storing

✓ Store hard-copy records and information in a designated location, in lockable storage or secure access areas. Store digital records, information and data in your agency's designated corporate recordkeeping systems or business systems. For more specific guidance check your agency's internal policies and legislation relevant to your work.

✓ Maintain inactive sensitive data to reduce risk of loss or theft. The risk of exposure of sensitive data increases when applications are retired or migrated, or SharePoint sites and file shares are abandoned at the conclusion of a project. For specific guidance about migration or retiring applications, check with your agency's information management team.

Accessing

✓ Apply the need-to-know principle to all information labelled with a NSW DLM and to any security classified information.

✓ Access to information labelled with a NSW DLM should be restricted. The information (or data) custodian at each agency has overall accountability for access provided (to hard copy, digital records, information and data).

✓ Ensure access to information labelled with a NSW DLM is only provided for a clear and legitimate business reason.

✓ Manage user access on an ongoing basis as roles and personnel change. The need for ongoing access or a time limited period of access should be considered.

✓ Review access to information systems containing information labelled with a NSW DLM by directly linked 3rd party applications. Information made available to these 3rd party applications must be limited to need-to-know. User access of the 3rd party applications need to be controlled as does the level of information that the users of this application can view. Examples of third-party applications are business and data analytics programs.

✗ Access rights cannot be transferred. Usernames and passwords should be kept confidential and not shared.

✗ Security clearances are not required for access to information labelled with a NSW DLM.

Securing

✓ Agencies must assess all data transiting and at rest and make an assessment whether it should be encrypted.

✓ Protect assets which contain sensitive information such as laptops or mobile devices.

✓ Secure mobile devices after use in a lockable container within agency facilities and if possible, outside of agency facilities, for example if working from home.

✗ Do not use your device unless it is safe to do so. Be aware of your surroundings. When sensitive and security classified information is being used, that can be read, viewed, heard or comprehended, it may be at a higher risk of compromise. Different physical environments pose different risks for information compromise.

Using

✓ Lock your computer screen or log out of secure systems when you leave your desk and make sure hard copies are secure (clear desk and clear screen policies should be implemented).

✓ Train all staff using sensitive information or using a secure system, so they are aware of the nature of the sensitive information and the rules which apply to use the information. Rules include whether they can view, print, share, or email information.

✓ Manual transfer of information labelled with a NSW DLM may be passed by hand within a discrete office environment provided it is transferred directly between members of staff who need-to-know and there is no opportunity for any unauthorised person to view the information.

✓ When carrying physical information labelled with a NSW DLM outside an agency facility, this information is to be carried in an opaque envelope or folder.

✗ Do not access information labelled with a NSW DLM using public networks.

✗ It is best practice to not copy information labelled with a NSW DLM onto local drives nor removable mobile storage devices such as USBs. Check your agency's internal policies.

? Follow your agency security measures if accessing information labelled with a NSW DLM outside an agency facility such as from home, via mobile devices. Where appropriate, ensure multifactor authentication is enabled and use only approved agency VPNs. For more specific guidance check your agency's internal policies and legislation relevant to your work. An example of this is your agency's work from home policy.

? When travelling outside Australia with mobile devices that can access, store or communicate information labelled with a NSW DLM, seek permission from your agency. Circular C2016-4 outlines the NSW Government policy for overseas travel.

? Copying, faxing, scanning, photographing and printing of information labelled with a NSW DLM should only be carried out if permitted by your agency and then only on a printer or device that has controlled access. For more specific guidance check your agency's internal policies and legislation relevant to your work.

Using - *Reports, Dashboards, Products*

✓ Handle system generated reports, dashboard and products with legacy marking of "Sensitive" as per these guidelines and update labels when able, based on risk assessment. For example, the most sensitive or most viewed reports should have their labels updated first. Labelling is not retrospective.

✗ Do not display products such as reports or dashboards containing sensitive information unless the audience need-to-know, and permission has been sought from the data custodian.

Sharing

✓ If sharing data externally, reducing the sensitivity of the information by de-identification techniques is recommended, for example removing personal information or information revealing law enforcement procedure. The DLMs indicate why the information is sensitive and which legislation may be limiting the use of the information.

✓ If sharing information externally, it is preferable that the source information is redacted to conceal the sensitive information where possible. This ensures that the source information remains inviolate and that the information can be safely shared. Care must be taken that the redaction does not alter the source information.

? Agencies will each have their own policies about emailing sensitive information internally and externally. Best practice when emailing sensitive information from one agency to another agency, or from one location to another within an agency, should be done via secure file transfer protocol, or via a secure system that is recommended by your agency. Sensitive information should not be stored in emails or as attachments to email in your inbox. Email systems are at higher risk of compromise than approved corporate business systems and are at risk of accidental forwarding. For more specific guidance check your agency's internal policies and legislation relevant to your work.

? Share information labelled with a NSW DLM for authorised purposes only. Agencies must establish their own rules on how their sensitive information is to be disseminated and what the approval process is. In some cases, agencies require written approval before information can be shared. Other agencies can share information if there is a memorandum of understanding in place. Legislation also has dissemination limiting clauses. For more specific guidance check your agency's internal policies and legislation relevant to your work.

Archiving, Retention and Disposal

? Records, information and data are covered by the requirements of the *State Records Act 1998*. Procedures for disposal and archiving are agency specific. Sensitive information must be disposed of securely. For more specific guidance check your agency's internal policies and legislation relevant to your work.

22. Security of Medical Gases

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all reasonably foreseeable security risks associated with storing and piping medical gases are identified, assessed, eliminated where reasonably practicable or, where they can not be eliminated, effectively minimised.

NSW Health Agencies are required to ensure that the process is appropriately documented and effective procedures are developed and implemented.

Medical gases can take the form of gas cylinders of a range of sizes including bulk tanks, and gas delivery plant and piping.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

- Ensure access to any storage and gas plant areas is restricted by use of locked doors, barriers and signs. Medical gas sources are to be secured against unauthorised removal, tampering, vandalism and misuse.
- Ensure appropriate access control procedures are developed and implemented, including restricted keys or other measures.
- Document the location of medical gases both in the bulk storage facility and at the ward level (this could be in the facility chemical register).
- Ensure records are kept for medical gases used for fieldwork. See 22.4.2 for further detail.
- Ensure procedures are implemented for reporting suspicious behaviour, theft, tampering and damage to medical gases and their containers.

22.1 Bulk Medical Gas Storage

- Bulk storage facilities must be subjected to a risk assessment prior to being used for the storage of medical gases.
- Bulk storage facilities are housed within a secure compound that can be locked and has been signposted in accordance with relevant Standards, and Dangerous Goods Regulation. Bulk gas storage is considered to be a single container over 500L or a net mass of over 500kg, or a cylinder/container storage compound that exceed the amount required for placarding. This amount varies depending on the type of gas stored (see Schedule 11 of the *NSW WHS Regulation*).
- Signpost the compound in accordance with Schedule 13 of the NSW WHS Regulation –included in the signposting must be dangerous goods class diamond, HAZCHEM notification, No-smoking signposting, naked flame warnings, parking restrictions.
- Sign posting must include the description of parking restrictions around the compound as well as a dedicated sign advising heavy frosting is a normal function of the bulk storage facility.
- Clear and unobstructed sight around the compound is required to prevent opportunities for unobserved interference with equipment.
- It is important to take into account the location of the compound and consider the possibility of vandalism, tampering or intentional interruption to service delivery.
- Ensure the compound security cannot be compromised by climbing over the fence.
- If the compound is located in an area where there is a possibility of vandalism or theft consider camera surveillance monitoring.
- Consider fitting bollards at strategic points as a protection measure against damage (either accidental such as backing into the fence or purposeful). Bollards will also act as a deterrent or enforcement mechanism to parking restrictions.
- When deciding on location of bulk gas storage areas consider evacuation and access by emergency services.
- Access to bulk medical gas compounds is to be restricted to selected persons such as the contracted supplier, maintenance workers and security staff.

- Filtering systems for bulk medical gases are to be housed in a secure area with restricted access.
- Fit locking devices to exposed valves.
- Flammable gases must not be stored near combustible materials or near entries/exits to facilities.
- Facilities must develop contingency plans for bulk service failure and include a predetermined supply of portable cylinders.
- Internal emergency shut off valves are to be located at strategic points within each facility – operating independently – to allow gas isolation in the event of a fire.
- Workers are to be educated as to how to isolate bulk medical gas supplies in the event of an emergency (such as a fire) via accessing the internal isolation valves.
- Ensure appropriate emergency services are orientated to the bulk storage compound and receive appropriate levels of education in respect to shutting down in the event of an emergency.
- Encourage all workers through the security education program to report suspicious behaviour, unusual vehicle parking/movements or loitering in the vicinity of the medical gas storage area.

22.2 Central Storage of Portable Medical Gas Cylinders

- Storage compounds/areas must be subjected to a risk assessment prior to being used for the storage of medical gases.
- Identify workers to have responsibility for accepting new/replacement cylinders and loading of spent/exhausted cylinders.
- On changeover with the supplier, workers must accept only cylinders in good structural condition, correctly labelled and identified, including date tags. The cylinders must be rejected if they have:
  - damaged valves,
  - no identification labels, and
  - with no or damaged date tags.
- The area is to be located in a secure purpose dedicated area position in a well-ventilated external area – the area must be weatherproof, stable level ground, and free of ignition possibilities.
- Discourage internal compounds or storage opportunities lower than ground floor level (basements).
- Storage of oxidising gases such as oxygen must be more than 3 metres in distance from flammable liquid storage areas.
- Storage is to be in a vertical position secured to a solid wall (accepted manner is a chain link per cylinder) or in a holder. Both full and empty cylinders must be secured.
- Ensure portable medical gas storage compound is adequately illuminated – to include paths of travel of collect and return, within duress alarm coverage, and consider camera surveillance monitoring and access alarms.
- It may be appropriate to separate some medical gases rather than store commonly in one area.
- Separate full and empty medical gas cylinders.
- Where appropriate, fit bollards to prevent damage and unauthorised parking, possible vandalism opportunities and allow accessibility for changeover of cylinders.
- Removable pressure gauges and regulators must be stored internally.
- Encourage all workers through the security education program to report suspicious behaviour, unusual vehicle parking/movements or loitering in the vicinity of the medical gas storage area.
- Instruct workers to remove and arrange replacement of any cylinder that has fallen over or been exposed to extreme heat related conditions.
- Changing valve assembles must only proceed once hand cleaning agents have completely dried. Some alcohol based hand gels used in Healthcare facilities contain a lubricant. There is a slight possibility of alcohol based hand gels coming into contact with the male thread of the valve which in turn if threaded into the female coupling – can create a leak possibility.

22.3 Portable Medical Gas – storage at a Ward/Department level

- Store in a dedicated area – where patients and visitors cannot tamper with full cylinders.
- Store in closed valve position.
- Portable gas cylinders must be secured and not left free standing eg must be in a holder, chained to the wall or in a cylinder trolley.
- Entonox and Nitrous Oxide must be stored in a secure manner ie lock and key to discourage misuse.
- Ensure appropriate access control procedures are developed and implemented.
- Document the location of medical gases at the ward level eg in the department chemical register.

22.4 Transport of medical gas cylinders

22.4.1 Within facilities

- If transporting cylinders to a ward or other area ensure cylinders are secure.
- Ensure cylinders are not exposed to shock by dropping.
- Use a purpose built trolley or holder as required.
- If using a tug the cylinders must be in a purpose built container that will not allow any to fall out or be bumped.
- Use open vehicles or trailers in preference to enclosed.

22.4.2 To an external location eg patient home visit or small clinic

Ensure records are kept for medical gases used for fieldwork. They must include:

- who is using the source and who is responsible for it
- where has the source been taken
- how is it stored/secured
- date and time of issue
- date and time of return
- any unusual circumstances.

Only transport gases that are safe to breathe in an enclosed vehicle (eg medical oxygen, medical air).

- Transport cylinders in dollies or other carrying device to the vehicle.
- Cylinders must be adequately secured in vehicles, in an upright position, to prevent movement during transport.
- Plan the trip and book a vehicle which is fitted with an adequate means of restraining the cylinder, for example a secure bracket, purpose installed straps or other method to secure the cylinder into position.
- Transport only one cylinder at a time unless an appropriate way to secure all the cylinders is available.
- To prevent build–up of oxygen within the cabin of the car when oxygen is in use, the car windows must be slightly open and the air conditioning vent set to fresh air.
- If not planned to be in use during the trip:
  - Check the valve assembly to ensure the cylinder is completely turned off. Try to transport a new cylinder rather than a cylinder that is partly full, a full cylinder will be factory sealed and have the pin assembly covered.
  - Check the cylinder for leaks (eg soap bubble test).
- Remove the medical gas cylinder as soon as possible on arriving at destination – unload and move to a secure, cool, well ventilated area.
- Procedures in the event a motor vehicle accident must include arrangements for advising emergency services of the presence of cylinders, where they are and what type of medical gas is in the vehicle.

Do not:

- transport with a removable valve assembly/regulator fitted (unless in use)
- store any portable medical gas cylinder in the front passenger compartment
- leave a medical gas cylinder/s for extended period in a closed unventilated vehicle
- attempt to use seat belts to secure medical gas cylinders or lay a medical gas cylinder on the back seat. The safest position is in a secure holder
- drop a cylinder or allow things to bang into them
- allow cylinder/s to roll around in the car.

23. Security of Radioactive Substances

Policy

NSW Health Agencies must make sure, through consulting with workers and other duty holders, that all reasonably foreseeable security risks associated security-enhanced radioactive substances are identified, assessed, eliminated where reasonably practicable. Where they cannot be eliminated they must be effectively minimised.

A security-enhanced radioactive source is one that requires appropriate management in order to decrease the likelihood of unauthorised access to, or acquisition of the source by persons with malicious intent.

NSW Health Agencies must document the process and develop and implement effective procedures.

Standards

A person who is responsible for a security-enhanced radioactive source specific legal obligations such as

- ensuring that security measures are taken relating to security-enhanced sources
- making security plans for security-enhanced sources
- managing who has access to security-enhanced sources
- reporting security incidents.

Generally, the 'person responsible' will be the NSW Health Agency that holds an Environmental Protection Authority (EPA) management licence that includes the source. If in doubt about responsibilities for a security-enhanced source, contact the EPA for advice.

23.1 Security measures

A person responsible for a security-enhanced source must ensure that the source has security protection measures relevant to the categorisation of the source and must:

- ensure stores (including waste stores) are properly marked with approved warning signs, and regulations regarding their use are posted at access points.
- ensure access to any storage areas is restricted by use of doors, locks, barriers and signs. Sources are secured against unauthorised removal and tampering.
- ensure access control procedures are developed and implemented. This includes consideration of surveillance camera coverage of entry/exit points and if required (as identified by risk assessment) storage areas.
- ensure unauthorised access to radioisotopes is not permitted.

See Appendix 23.1 to determine procedural and administrative security requirements and controls set out by Australian Radiation Protection and Nuclear Safety Agency (arpansa) that must be implemented. Use the national threat level and the categorisation of the radioactive source (source category) for this.

23.1.1 Security measures for category 1 security-enhanced sources

Category 1 sources are considered to pose the highest risk and are subject to the most stringent security requirements. Category 1 sources include industrial irradiation facilities, larger blood or research irradiators, and gamma knife devices.

Where a category 1 security-enhanced source is in use or being stored or transported, the source must be protected by, at a minimum, physical security measures. These measures must be capable of providing:

- sufficient delay to allow immediate detection and assessment of an intrusion and
- interruption of any unauthorised removal of the source by a worker or police officer.

23.1.2 Security measures for category 2 security-enhanced sources

Category 2 sources include most other blood and research irradiators and industrial radiography sources.

Where a category 2 fixed or mobile security-enhanced source **is in use**, the source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of unauthorised access to the source.

Where a category 2 security-enhanced source **is being stored**, the source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of unauthorised access to the source location.

Where a category 2 security-enhanced source **is being transported**, the source must be protected by, at a minimum, physical security measures capable of providing sufficient delay to allow immediate detection and assessment of unauthorised access to the source.

23.1.3 Security measures for category 3 security-enhanced sources

Category 3 sources include sources used in brachytherapy and larger fixed industrial gauges.

Where a category 3 fixed or mobile security-enhanced source is in use, the source must be protected by, at a minimum, physical security measures capable of preventing unauthorised access to the source by human force. ***Human force*** means any force that can be exerted by a person, including by using tools (except power tools).

Where the security-enhanced source is being stored or transported, the source must be protected by, at a minimum, physical security measures capable of preventing unauthorised access to the source by human force.

In the case of category 1, category 2 and category 3 sources, the appropriate procedural and administrative actions determined in accordance with Schedule D to the Security Code must be undertaken.

23.1.4 Category 4 and 5 sources

Categories 4 and 5 sources include low-dose brachytherapy units, most industrial gauges, and portable soil moisture and density gauges used in road building and agriculture.

Those responsible for these sources should apply safety-based security measures for Categories 4 and 5 sources, which are outlined in the EPA licence conditions.

23.2 Source security plans

The person responsible for a security-enhanced source must prepare a security plan that accounts for each source location in the NSW Health Agency.

The source security plan must set out how the source is to be protected from unauthorised access and nominate a natural person who is to be responsible for implementing the plan.

Specifically, the plan must deal with

- the category of the source and how the source has been categorised as a security-enhanced source
- how the plan has been developed using a risk-based approach, with particular regard to:
  - the nature of the source and any dealings with the source, the environment in which those dealings occur
  - identification of any credible threats to the source in relation to any such dealings and the likelihood and consequence of the threats eventuating
  - an assessment of the effectiveness of existing security measures, and
  - identification of further action required to achieve compliance with the prescribed security measures for the source
- how compliance with the prescribed security measures for the source is to be (or is being) achieved
- a description of the source including the:
  - isotope
  - activity
  - date of measurement of that activity
  - source serial number
  - physical and chemical form
- a description of the allocation of responsibilities for security to persons (including how those persons are competent, qualified and authorised to carry out their responsibilities)
- a description of any specific risks to the security of the source (such as, for example, theft, sabotage or mechanical or electronic failure of a physical security measure)
- a description of the physical security measures that will be used to ensure compliance with the prescribed security measures for the source
- arrangements for review and revision of the plan
- a description of the radiation practice for which the source is used
- the specific location of the source
- a plan of the building or facility in which the source is used or stored
- a description of any surveillance or monitoring measures implemented to ensure compliance with the prescribed security measures for the sources (for example, camera surveillance, personal surveillance or security patrols)
- a description of the administrative and procedural measures that are to be used to ensure compliance with the prescribed security measures for the source, including:
  - access controls (including key controls)
  - any identification and security checking carried out in accordance with the Act

  - inventories and records related to the management of sources
  - information security
  - procedures to be followed before, during and after a technical service
  - contingency and security response arrangements, including notification of security breaches
  - security education and awareness
  - the action to be taken in the event of a change in the **threat level**.

The person responsible for a security-enhanced source must ensure that any source security plan in respect of the source is

- implemented and complied with
- made available to the EPA at such times as they may require
- is reviewed at least every 12 months.

23.3 Source transport security plans

A person who is responsible for a security-enhanced source that is being transported must prepare a source transport security plan. This applies where transporting by road, rail or waterways, eg between facilities.

The source transport security plan must set out how the source is to be protected from unauthorised access and nominate a natural person who is to be responsible for implementing the plan.

A source transport security plan must also deal with the following:

- the purposes or reasons for which the source is being transported
- a description of the conveyance in which the source will be transported and the arrangements for securing the shipment during transfer between different conveyances or during other stops en route
- the name, address and business and after hours contact details for the consignor, consignee, carrier and, where used, guard or police services
- a description of the administrative and procedural **security measures** that are used to meet the security outcomes relevant to the source, including:
  - contact details for local police and the EPA and arrangements for notifying local police or the EPA, or both, depending on the issue
  - contingency and emergency procedures for vehicle accidents or breakdown (including, for category 1 sources, a planned principal route and an alternative route)
  - security response arrangements, including notification of any security breach to local emergency services (police, fire and ambulance) and the EPA as appropriate
  - security briefings for persons involved in transporting the source, including the nature of any threats, the threat level and contingency and security response arrangements
  - any identification and security checking carried out in accordance with the Act and Regulation. Ensure only authorised persons undertake the escort of radioactive substances when being transported within an organisation
  - information security
  - the means of communication between persons involved in transporting the source
  - actions to be taken in the event of a change in the **threat level**.

A person responsible for a security-enhanced source must ensure that any source transport security plan in respect of the source is provided to the EPA:

a. in the case of a category 1 source – at least 7 days prior to transportation of the source, and

b. in the case of a category 2 or 3 source – at least 7 days prior to transportation of the source or, if the source is to be transported on a regular basis, at least 7 days prior to the first transportation of the source.

If a source transport security plan is amended for any reason, the person responsible for transporting the source must provide the EPA a copy of the amended plan, as soon as reasonably practicable after the plan is made or amended.

23.4 Identity checking

A person who is responsible for a security-enhanced source must ensure that the following persons have undergone and satisfied an identity check that ascertains the identity and residential address of the person (in accordance with the document *Requirements for identity checks* published by the EPA)

- the person nominated as being responsible for implementing a security plan in respect of the source
- a person who deals with the source
- a person who transports the source.

A person who deals with a source (other than to transport the source) is not required to have undergone a check if they are under the direct supervision when dealing with a source and the person providing supervision has undergone and satisfied an identity check.

23.5 Security incidents

If there is a breach of a prescribed security measure that results in a security–enhanced source being lost or stolen, intentionally damaged or accessed without authority, the person responsible for the source must:

- immediately notify the EPA (ph 131 555) and the NSW Police Force of the incident, and
- within 7 days of the notice, submit a report of the incident to the EPA that contains the following information:
  - the circumstances of the loss, theft, damage or unauthorised access
  - the steps taken to rectify the loss, theft, damage or unauthorised access
  - if the source is lost or stolen – any information that may assist in the recovery of the source.

If there is a breach of a security measure (other than an incident as described above) relating to a security–enhanced source, the person responsible must submit a written report of the incident to the EPA within 7 days.

Notification of security incidents must also be to

- The NSW Health Agency person responsible for radiation safety.
- The health organisation Chief Executive and the Facility Manager.
- The Secretary of the Ministry of Health.

Note: In emergency situations involving suspected or actual damage, spillage, loss or theft of radioactive substances the Radiation Control Section of the EPA should be contacted on (ph 131 555)

Notifying pollution incidents – for a leak, spill or other pollution incident the following organisations must be notified

- appropriate regulatory authority (ARA)
- EPA (if they are not the ARA)
- Ministry of Health
- SafeWork NSW
- local authority, if they are not the ARA
- Fire and Rescue NSW

23.6 Resource documentation

- Code of Practice for the Security of Radioactive Sources (2019)
- Code for the safe transport of radioactive material Radiation Protection series c–2 (Rev. 1)
- EPA Radiation regulation documentation

Appendix 23.1 Determining procedural and administrative security requirements

From ***Security of Radioactive Sources, Radiation Protection Series No. 11***, January 2019 (arpansa)

To determine procedural and administrative security requirements use the *threat level* and the *categorisation of the radioactive source* (source category).

Step 1 – Determine the Threat level

- The threat level is an indicator of the likelihood of a perceived perpetrator to acquire radioactive sources for the purposes of malicious use in Australia. Threat levels are set by the Australian Government's National Threat Assessment Centre in relation to specific people, places, events, sectors and interests. Local threat levels may also be informed by intelligence gathered at the State and Territory level. Responsible Persons will be informed of an escalation subject to jurisdictional arrangements. Procedural security measures for protecting a security enhanced source escalate in accordance with the threat level (see step 3).
- The threat levels are:

CERTAIN

Certain – a terrorist attack is certain, the government has concerns that a terrorist attack will soon occur or is underway.

EXPECTED

Expected – a terrorist attack is expected, the government has concerns of a specific threat.

PROBABLE

Probable – a terrorist attack is probable, the government has concerns of a plausible threat.

POSSIBLE

Possible – a terrorist attack is possible, the government has concerns a threat may exist.

NOT EXPECTED

Not expected – a terrorist attack is not expected, the government has no specific concerns.

Step 2 – Categorise the radioactive source

- To categorise the source see Schedule B of the Radiation Protection Series 11 – code of practice – security of radioactive sources to categorise a radioactive source or aggregation of radioactive sources.
- The categorisation of the source may vary due to the situation and must be considered separately for security purposes because the categorisation of sources when in storage might be different from that when they are in use. This means that the physical security requirements for sources in storage might be different from those required when they are in use.

Step 3 – Determine security actions required

Once you have determined the threat level and the source category use the legend to identify which security action is required. The requirements must be reviewed at least when the threat level changes or the source category changes.

Scalability of procedural and administrative security requirements with threat level for a security enhanced source

Source category	Threat Level			
	Not expected or possible	Probable	Expected or certain	Row 1
1	A, D	A, B, D, E	A, B, C, D, E	Row 2
2	A	A, B, D, E	A, B, C, D, E	Row 3
3	A	A, B	A, B, C, D, E	Row 4
Column 1	Column 2	Column 3	Column 4	

Legend

Group	Security action
A	Annual review of Source Security Plan and Source Security Transport Plan
	Annual review of intrusion detection, event assessment and communication measures
	Annual review of access controls and physical barriers
	Annual review of worker access requirements
	Event specific review of worker access
	Worker induction security awareness briefing
	Annual worker security awareness briefing
	Event specific worker security awareness briefing
	Annual audit of all sources
	Monthly accounting or check to confirm present of the source
	Visitors to be signed in and escorted while present inside the secure area defined in the Source Security Plan
B	Weekly accounting or check to confirm presence of the source
C	Visitors to be refused entry to the inside of the secure area defined in the Source Security Plan, unless authorised by the regulatory authority police
	Goods deliveries to be dispatched and received off–site with movement of goods only to be undertaken by personnel satisfying the appropriate identify check or is accompanied at all times by someone with the appropriate identity check
	Half yearly worker security awareness briefing
	Daily accounting or check to confirm presence of the source
D	Annual exercising of guard force or police service response arrangements
E	Half yearly review of worker access

24. Fire (Code Red), Evacuation (Code Orange) and other Emergencies

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all reasonably foreseeable security risks associated with fire and other events that may result in evacuation or significant impact on service are identified, assessed, eliminated where reasonably practicable or, where they can not be eliminated, effectively minimised.

NSW Health Agencies are required to ensure that the process is appropriately documented and effective procedures to manage security during fires or other emergencies that may affect a facility are developed and implemented.

Procedures must also be incorporated into disaster and service continuity plans.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

Risk assessments and any resulting procedures must include consideration of the following:

- evacuating and accounting for workers, patients, visitors and other occupants of the building or facility in a safe area away from the source of risk
- securing (evacuated) patients who may be cognitively impaired, and who may be at risk of absconding or harm
- securing any (evacuated) patients in custody, scheduled patients, patients with cognitive deficits and (unaccompanied) children and babies
- isolating the fire scene until the police and the fire brigade assume control of the site
- ensuring the Fire Brigade is directed to the fire by the quickest route and
- operating any Emergency Warning and Intercommunication System (EWIS) or other emergency communication equipment.
- the possibility of the fire being a diversionary tactic for criminal activity
- theft of assets, malicious property damage or looting of other parts of the facility during a fire
- prior to, during and after evacuation, controlling crowds and traffic until the police can assist

What to do in the Event of a Fire or other emergency:

NSW Health Agencies must develop local procedures that outline what to do in the event of a fire and other emergencies. These procedures must reflect the following elements:

- details on who must be contacted in the event of a fire or other emergency and when this contact must occur
- the specific role of NSW Health Agency workers and emergency services. This includes the roles of unit workers, eg paediatric unit
- a nominated emergency co-ordinator and deputies (in the absence of the co-ordinator)
- guidelines on the use of fire equipment
- the evacuation process (including priority for the removal of patients) and
- details on assembly points.

NSW Health Policy Directive ***Fire Safety in HealthCare Facilities*** provides detailed information on fire safety management, statutory requirements, fire protection, fire safety emergency response procedures, training and evacuation and advisory services.

This must be read in conjunction with Australian Standard *4083:2010 Planning for emergencies in Health Care Facilities* for other fire management requirements.

The requirements of this chapter will be audited in the NSW Health WHS Audit.

25. Bomb Threat (Code Purple) / Terrorist Threats

Policy

NSW Health Agencies are required to ensure that all reasonably foreseeable security risks associated with receiving explosive devices, National Security Threat Level rating or terrorist threats are identified, assessed, eliminated where reasonably practicable or, where they cannot be eliminated, effectively minimised.

Consultation with workers, other duty holders and emergency services must be undertaken to ensure risk assessment processes are inclusive of local knowledge, custom and practice, available resources and response agencies.

NSW Health Agencies are required to ensure that the risk assessment process is appropriately documented and effective bomb/terrorist threat emergency procedures are developed and implemented, including for NSW Health workplaces located away from a hospital campus. Implementation is to be inclusive of an education strategy and procedural testing to ensure facility preparedness.

NSW Health Agencies are required to implement a program of routine security checks (white level inspections) at all workplaces, where the government security alert is at probable or above.

Standards

A threat brings with it a range of security considerations including but not limited to:

- the possibility of a secondary device being placed in areas of assembly
- the possibility of the bomb/terrorist threat being a diversionary tactic for criminal activity
- the possibility that the threat could be with the intent of gaining access to a person or persons who become more accessible during the evacuation, eg a patient in custody.
- theft or looting of an evacuated facility
- securing any (evacuated) patients in custody, scheduled patients, patients with cognitive impairment and (unaccompanied) children and babies.

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

NSW Health Agencies must implement procedures for assessing and managing potential threats to persons and service delivery, and security issues that may arise from such a threat. Local procedures must incorporate the following:

- the relevant outcomes of the risk assessment undertaken in the workplace and must be consistent with the Australian Standard Planning for Emergencies in Health Care Facilities (AS4083) codes for emergencies (as set out in the local Emergency Flipchart). See the Australian National Security website for resources
- provide for job specific training on the response to and management of threats
- where there is a direct written or verbal threat of terrorism or violence against a person or place within NSW Health, it is imperative that it is reported to the appropriate senior manager, security staff and that NSW Police are contacted immediately by accessing an external line and calling 000
- where a written or verbal threat is non–specific or does not pose any immediate threat to a person or place, the local Police station must be called and advised of the threat. Where the local police station is not able to be contacted, calling the police assistance line on 131 444 may be the more effective strategy to ensure notice of the threat is recorded
- documentation of requirements for the preservation of written threats for police assessment and forensic analysis (letter or email), and the recording of information associated with a verbal threat is to be incorporated into response procedures.

25.1 Australian National Terrorism Threat Level

The National Terrorism Threat Level is a scale of five levels (see diagram below) that tells the public about the likelihood of an act of terrorism occurring in Australia. Whenever the Government makes a change to the National Terrorism Threat Level it will explain why there is a change. The National Terrorism Threat Advisory System informs about the likelihood of an act of terrorism occurring in Australia and provides an indicator to government agencies enabling them to respond appropriately with national threat preparedness and response planning. This ensures that an appropriate level of precaution and vigilance is maintained to minimise the threat of a terrorist incident.

CERTAIN	**Certain** – a terrorist attack is certain, the government has concerns that a terrorist attack will soon occur or is underway.
EXPECTED	**Expected** – a terrorist attack is expected, the government has concerns of a specific threat.
PROBABLE	**Probable** – a terrorist attack is probable, the government has concerns of a plausible threat.
POSSIBLE	**Possible** – a terrorist attack is possible, the government has concerns a threat may exist.
NOT EXPECTED	**Not expected** – a terrorist attack is not expected, the government has no specific concerns.

The National Terrorism Threat Advisory System:

- comprises a five tier, colour coded, National Terrorism Threat scale to inform the public about the level of the terrorist threat facing the nation
- includes public advice on the nature of the threat we face and what it means for them
- will help inform the public so they can decide on what measures they can take to protect themselves, families and friends
- guides national preparation and planning to protect against the threat of a terrorist incident
- rebalances the threat levels to reflect the current security environment that the country is facing.

25.2 Security and Housekeeping

Requirements include

- good quality door fittings, locks and alarms to deter after hours penetration of the workplace must be installed (refer to *Chapters 9 Access and Egress Control and 11 Duress Alarm Systems* of this Manual for more information)
- entry/exit points must be restricted or minimised (refer to Chapter 9 Access Control of this Manual for more information)
- assessment of the need to install surveillance equipment (camera surveillance and monitors) must be undertaken. This assessment must include identifying the recording quality and capability required, locations, monitoring supervision and access limitations to monitoring and recording functions (refer to Chapter 13 Workplace Camera Surveillance of this Manual for more information)
- visitor registration and identification procedures must be in place (refer to *Chapter 9* of this Manual for more information)
- lock–up or security check procedure at the close of business each day/night must occur. Daily open–up procedures must complement close of business procedures
- an emergency lock down procedure must be developed that includes unit by unit and facility wide processes that incorporate a communication and containment strategy. Testing and exercising this procedure must be conducted to enhance employee learning and to evaluate systems and processes
- daily internal physical security inspections eg white level inspections must be conducted
- the services and resources of professional advisory bodies such as the Australian National Security resources, ASIO outreach resources, NSW Police and security professionals etc must be utilised to assist with assessing the threat to the workplace
- organisational storage practices and workplace cleanliness including regular disposal of rubbish must occur as it has several highly desirable benefits:
  - the number of potential target areas is reduced
  - searchers are not distracted unnecessarily by extraneous objects
  - hygienic/sanitary conditions encourage thorough searching.
- secure buildings, rooms and storage areas not in regular use as it reduces sites for caches of potentially dangerous items and the opportunity for hiding

explosive or incendiary devices. Car parks are to be monitored for vehicles parked for an extensive period of time with checks made to ascertain if they are stolen (see Chapter 19 Security in Carparks for further detail).

25.3 Routine security checks in the workplace (white level inspections)

A white level inspection involves inspecting an area for anything unusual, suspicious, or that can't be accounted for. Workers who know and work within an area are best placed to do this.

White level inspections may be completed:

- routinely – by workers or the occupant of an area because they are familiar with their surroundings. This type of inspection is relatively fast and efficient
- in response to a specific threat – this may be done discreetly, without alerting other workers to the threat. Supervisors inspect their own areas of responsibility and report back to a chief warden or duty manager. Alternatively, a supervisory inspection can involve designated wardens to oversee and plan the inspection.

An inspection in response to a threat may also involve partial or full evacuation depending on the credibility of the threat.

Create a plan that assigns workers certain areas, including communal areas such as public concourses, foyers, cloakrooms, stairwells and corridors. Pay particular attention to evacuation routes and assembly areas. Having a plan will assist in ensuring the white level inspection is conducted in a safe, thorough and timely manner.

It is important that workers are routinely vigilant about unexplained changes in their working environment. Where the Federal Government determines that the national terrorism threat level is probable (or above), a structured routine white level inspection program to inspect workplaces and common/public areas must be implemented. This program must include the following:

- inspections occur at the start of each shift
- workers conduct a visual check of their work areas (and any common/public areas they have been assigned to check) looking for any articles that are unusual, suspicious or unable to be accounted for
- workers advise their manager, or a designated contact person, that they have conducted a check and advise them if something is out of place
- completion of the inspection is documented.

Workers are given instruction on how to carry out a 'white level inspection', including what to do if they discover a suspicious item (see section 25.5).

25.4 What to do if there is a Bomb Threat or Threatening Telephone call

NSW Health Agencies must develop procedures that outline what to do in the event of a threat being received (Refer to the *NSW Health Security resource webpage* for a model procedure). These procedures must be consistent with the standards outlined in the Australian Standard on planning for emergencies in health care facilities – AS4083 for Code Purple and reflect the following elements from that Standard:

- details on who must be contacted in the event of a threat and when this contact must occur including the Health Services Functional Area Co-ordinator (HSFAC) and/or the nominated position with responsibly for local emergency/incident co-ordination)
- if there is a direct threat against a person the NSW Police must be contacted immediately by accessing an external line and calling 000. If the threat is not specific or does not appear to pose any immediate threat to a person or place the Police Assistance line 131 444 must be called. If the immediacy of the threat is unclear the 000 number must be used. Local senior management and security staff must also be notified
- the role of NSW Health Agency workers and emergency services
- a nominated position with responsibility for local emergency/incident co-ordination and their delegates (in the absence of the nominated co-ordinator)
- guidelines on the non-use of safety equipment and communication devices during an incident ie do not use mobile phones, radios, duress alarms, pagers or flash photography within a 25-metre radius (electronic frequencies or light sources may cause a device to detonate)
- guideline for conducting a search of premises
- documented protocols for evacuation (including prioritisation of patients and identifying multiple evacuation routes). Protocols must include:
  - information on assembly point locations
  - identification of alternate assembly areas to be determined by the nominated position with responsibility for local emergency/incident co-ordination or their delegates (in the absence of the nominated co-ordinator) or Police Site Controller
  - evacuation and assembly point routes must be searched prior to evacuation to ensure staff, patients and visitors are not unnecessarily exposed to danger during evacuation.
  - the requirement for move-on arrangements in the case of concerns about the safety of the assembly areas. The move-on arrangements must not be publicly displayed.

Samples of a *Bomb, Terrorism or Other Threat – Telephone Call Incident Report* and a *Bomb/Terrorism Threat Procedure* are found on the *NSW Health Security resource webpage*.

25.5 Procedures for Identifying and Handling Suspicious Items (including Mail)

During the risk management process special attention must be given to those areas where:

- mail delivery, opening, and sorting are carried out
- the public has direct access
- suspicious items could be introduced unnoticed.
- procedures for handling suspicious items must include the identification of screening areas, criteria for identifying suspect items, isolating the suspicious item without moving it, positioning of contamination spill kits, and emergency responses where suspicious items are identified.
- specific disposal procedures and advice may need to be sourced from external agencies (NSW Police or Fire Rescue NSW).

25.5.1 Screening areas

Secure screening points for all mail must be established, that is, a central processing point for all mail for the workplace. Visual/manual screening process must serve to identify as 'clear' the majority of mail items processed through the screening point.

Where a suspect item is detected through the initial screening, the area must be cleared of workers and a call made for assistance, in line with local procedures.

25.5.2 Identifying suspicious items

To determine whether an item is suspicious, apply the 'HOT' principle. Under the HOT principle, anything that is **hidden**, **obviously suspicious**, or **not typical** to its environment could be deemed a security risk.

Suspicious items (including suspicious mail) may display a combination of the following characteristics:

- excessive securing material ie tapes and wrapping
- excessive weight
- protruding wires or tin foil
- oily stains and discolorations
- visual distractions ie packages marked as "Fragile–Handle with Care", "Rush–Do Not Delay," "Personal," or "Confidential."
- chemical or solvent smells or unusual odours
- common words misspelt
- incorrect titles, names or addresses
- either unusual or foreign origin
- excessive postage
- no sender address
- does not fit with the usual type of mail received by the facility
- lopsided or unevenly weighted or in a stiff or rigid envelope.

If a suspicious item is found, workers must:

- not touch tilt or tamper
- attempt to locate the owner of the article by inquiring with people in the area
- if available, check surveillance camera footage to determine who placed the article
- inform supervisor, manager, or police if the article cannot be accounted for
- record a detailed description of the item, including size, shape, location, and whether it is leaking liquid or unusual odours
- take a photo (NO FLASH PHOTOGRAPHY) of the article if safe to do so
- consider moving people away from the suspicious item and/or restricting access.

25.5.3 Responding when an Item is assessed as suspicious

If an item is considered suspect, local procedures consistent with the stan dards outlined in the *Australian Standard on planning for emergencies in health care facilities – AS4083*, must be developed and include the following steps to ensure the security of workers:

- contact the nominated position with responsibility for local emergency/incident co-ordination or, in the absence of this person, a supervisor and inform them:
  - that a suspicious item has been found
  - their name, department and telephone number
  - the exact location of the item
  - the description of the item
- **DO NOT USE RADIOS, MOBILE PHONES, DURESS ALARMS, PAGERS or FLASH PHOTOGRAPHY WITHIN A 25 METRE RADIUS OF THE OBJECT.** (Electronic frequencies or light sources may cause a device to detonate)
- For mail items
  - confirm that the item has come through the postal system. An item that has come through the postal system usually does not have the same degree of sophistication as a device that has been placed or delivered by a courier.
  - check with the addressee if they are expecting the item. If a return address is on the article, check with the originator
  - isolate the article
- consider whether evacuation is necessary. Evacuation must always be considered in the event of a potential bomb threat. Evacuate and cordon off the immediate area. Ensure no re-entry until the 'All Clear' is given
- obtain as much information as possible (without handling the suspect item) in relation to dimensions, balance, stains, history or threats, type or construction of the package and its exact location to pass on to the nominated position with responsibility for local emergency/incident co-ordination or their delegates (in the absence of the nominated co-ordinator).

- under no circumstance must any attempt be made to open the item, as it is generally this action that will cause the device to activate
- the suspect item must not be immersed in water as this may cause it to activate
- suspect items must not be placed in confined spaces such as filing cabinets or cupboards as this will only increase the blast effect if it detonates. Where possible the item must be placed in an area where the gases produced by an explosion can be vented, for example near an open window (but not near a window where people are passing by and may be injured by the blast).
- suspect items must not be carried or transported through congested areas and this could expose others to unnecessary hazards.

25.6 Managing Post Incident Issues

NSW Health Policy Directive *Incident Management Policy* provides a framework for managing post-incident issues such as incident reporting, and incident investigation.

NSW Health Policy Directive NSW Health Policy *Rehabilitation, Recovery and Return to Work* provides policy and guidelines for the management of workplace injuries.

25.7 Resources

- NSW Health Security resource webpage
- Australian National Security website
- ASIO outreach resources
- AS4083 Planning for Emergencies in Health Care Facilities
- Bombs: Defusing the Threat (Australian Bomb Data Centre)
- Improvised Explosive Device IED Guidelines for crowded places (Australia New Zealand Counter-Terrorism Committee (ANZCTC))
- Procedures for Reporting Security Incidents (Department of Premier and Cabinet Circular c2007-44)

26. Violence

Policy

NSW Health Agencies are required to ensure, in consultation with workers and other duty holders, that all reasonably foreseeable risks associated with violence are identified, assessed, eliminated where reasonably practicable or, where they cannot be eliminated, effectively minimised and that the process is appropriately documented.

NSW Health Agencies must also identify any workplace where there is a risk of workers undertaking isolated working and complete a risk assessment and implement control measures to manage the risks identified.

Note: Attention is drawn to the Public Health System Nurses' and Midwives (State) Award 2021 regarding obligation for minimum staffing requirements for smaller facilities (see Clause 53, Section III).

NSW Health Agencies must have in place a process for communicating the risks presented by a patient or their family/visitors to workers. NSW Health Agencies must ensure that the process is appropriately documented.

For the purposes of this Chapter, violence is defined as any incident in which an individual is abused, threatened or assaulted and includes verbal, physical or psychological abuse, threats or other intimidating behaviours, intentional physical attacks, aggravated assault, threats or assault with a weapon and sexual assault.

Refer to NSW Health policies on *Prevention and management of bullying in NSW Health* and *Prevention and management of unacceptable behaviours in NSW Health – JMO module* for guidance on the management of worker behaviour.

Standards

NSW Health is committed to eliminating to all forms of violence in the health workplace. To achieve this NSW Health Agencies must ensure that all risks of violence are identified, assessed and controls put in place to eliminate or minimise the risk.

Where violent incidents do occur (or where there are near misses) the response must be prompt, appropriate and consistently managed to prevent their occurrence, escalation and to minimise their impact on workers, patients and visitors.

In Australia everyone shares a fundamental right to basic health care. However, workers also have a right to safety in the workplace and to be treated with respect. These rights must be managed to ensure the safety of everyone is the priority.

To assist with achieving this balance the following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

The standards in this chapter are broken up into four main sections.

- Protocols for **preventing and reducing the risk of violence** – what to do when the potential for violence is identified (26.1)
- **Responding to violent behaviour** – what to do during an incident (26.2)
- **Managing post incident issues** – what to do after an incident occurs (26.3)
- **Managing the risk of violence when working from home** (26.4)

26.1 Protocols for preventing and reducing the risk of violence

26.1.1 Safety and security awareness

NSW Health Agencies must have arrangements in place to support, instruct, and supervise workers to:

- comply with all established work practices and security procedures including those related to personal duress alarms, and clothing and grab risks
- use processes for sharing security and other relevant risks about patients with the multidisciplinary team and other workers (eg cleaners/food services as relevant) during handover, in the safety huddle or via any other means. More information about safety huddles is found in the NSW Health *Work Health and Safety: Better Practice Procedures*
- prevent long hair being untied or wear clothing, jewellery or other accessories that can be used against them or grabbed in an attack eg dangling jewellery or clothing, scissors where they can be seen, lanyards or pouches containing sharps

- use all duress alarms and communication devices to summon assistance
- understand and undertake their role in the event of an accident to assist their colleagues
- report workplace hazards, incidents and near misses. Workers must be encouraged and supported to report all incidents, and these must be assessed to identify whether there is opportunity to take action to prevent a recurrence of the incident
- participate in appropriate training in the prevention and management of violence and duress response (including use of alarms, drills/desktop exercises).

26.1.2 Communicating with patients (and carers) awaiting care

Ensuring appropriate ongoing communication with those waiting for care is important as a strategy in reducing the potential for escalating behaviour. As a minimum, patients and carers in all areas must be advised of changed waiting times or delays in appointment times, including where wait times have increased due to high volume.

In **Emergency Departments** (and in other areas where relevant) NSW Health Agencies must ensure a process is in place for communicating with and monitoring waiting patients. Communication strategies at a minimum must involve:

- informing patients/carers at the time of triage what to do if their condition changes or they become concerned while awaiting care
- if they are not allowed to eat or drink
- suitable alternatives to the ED
- the behavioural responsibilities of patients and visitors.

Further standards are set out in NSW Health policy *Emergency Department Patients Awaiting Care.*

26.1.3 Clinical protocols to prevent and manage violence

Ensure clinical protocols are in place that:

- follow the requirements of NSW Health policy *Recognition and management of patients who are deteriorating*
- provide for first assessment of patients on admission, assessment and transfer of patients particularly that includes indicators of potential for acute severe behavioural disturbances (ASBD see 26.1.5 below)
- identify the risk of violence arising from a clinical condition and provide adequate and appropriate clinical management, eg early diagnosis and treatment of delirium, identification and treatment of drug, alcohol or tobacco dependency
- share any identified risks and information with the multidisciplinary team (including security staff). This may be in handover, safety huddles or by any other means
- incorporate ongoing risk assessment, and management of behavioural issues of patients
- facilitate early identification, diagnosis and treatment of deteriorating behaviour. Patients/clients can experience a deterioration in their mental state for a range of reasons and in all healthcare settings. This is frequently preceded by early warning signs and effective response improves the potential to prevent an adverse outcome. This can include a change in their perception, cognitive function or mood which negatively affects their function as they would typically choose
- ensure appropriate clinical handover of the patient:
  - to other clinical workers – receiving or transferring patient
  - non clinical workers who will be interacting with patient
  - on transfer to other clinical areas
  - on transfer to other services (including short term transfers).
- record all incidents involving a patient's behaviour in the medical record (including file flagging for aggression, see 26.3.5) and in the incident management system ims+
- seek and assess any relevant safety and risk related information from services transferring a patient (eg paramedics, NSW Police, nursing or disability care homes, non–government organisations (NGOs), Corrective Services, GPs, private hospitals)
- provide information to services receiving a transferred patient (including short term transfers eg to radiology for a test)
- communicate and assess any relevant risk information from services transferring between NSW Health facilities (ie intra and inter facility transfers)
- advise security staff and/or the Code Black Response Team when a patient who is known or flagged to pose an aggression risk is admitted/attending appointments
- require clinical workers to notify security staff and/or the Code Black Response Team when they become aware that a patient who may present a behavioural challenge is on route to the hospital emergency department or mental health assessment unit. This allows for preparation and communication between the multidisciplinary team (including security) regarding management strategies
- reduce the use of seclusion and restraint where safe to do so
- allow specialist advice to be accessed after hours
- reduce delays in mental health assessments
- allow for greater utilisation of the clinical initiatives nurse and accredited persons under the *Mental Health Act* who can enact or lift a schedule
- develop procedures for limiting the number of patient support people/visitors in treatment areas
- implement and utilise a patient alert system (file flagging), see 26.3.5 below

- develop communication strategies for ensuring that patients and visitors are aware of their behavioural responsibilities and the consequences of not meeting those responsibilities, eg prominent signage, patient and visitor information brochures
- communicate risks relating to patients to the multidisciplinary care team (including security and other non–clinical workers who may interact with the patient), on an ongoing basis, and during shift changeover / safety huddles and when issues arise. Practices must also take account of the need to communicate risks to workers rotating into the work area who may not have immediate knowledge of any patient related risks (eg visiting workers to the ED or ward)
- consideration of increased observation and if security staff and/or the Code Black Response Team is required to support clinical workers undertaking these observations (see Chapter 14 Role of security staff 26.3.3 *Providing ongoing care to patients who have been aggressive*, below)
- review of the physical location (is the room the most appropriate) and removal of objects that can be used as weapons. This includes local practices that involve the collection of all cutlery (metal and plastic) and sharps (including scissors) used in the treatment area immediately after use, or put in a safe area, out of sight, if it is not to be immediately removed from the workplace.

Ensure that violent incidents are reported, documented and analysed (including Code Black response and its outcomes) from clinical, security and WHS perspectives

Ensure recommendations from incident investigations and post incident debriefings are implemented to prevent reoccurrence.

Ensure there is a well designed, appropriately staffed, secure therapeutic environment which is compatible with clinical care objectives and worker safety. Chapter 15 Designing out Security Risk in the clinical environment provides guidance on the design of the clinical area to reduce violence hazards/risks.

Ensure a process for escalating issues to local protocol committees with Agencies eg NSW Police, as required under the Memorandum of Understanding.

26.1.4 Responding to needs of people with disability during hospitalisation

Ensure protocols are in place that:

- provide for workers communication with the carer, family, guardian, and / or disability support workers, about ways to provide safe and personalised care for people whose disability could result in significant risk of harm to themselves, the carer or hospital workers eg due to fear, anxiety, absconding, challenging behaviours, difficulties with communication
- require the development of a plan for disability support while in hospital as part of pre–admission planning for a person with a disability
- allow for the presence of a person known to the patient where the patient has a known intellectual disability. This may reduce stress, reduce the risk of escalating challenging behaviours and improve overall health and safety outcomes for the health service and the person with disability alike
- apply to identifying and reducing risk related to non–planned admissions for a person with disability through the Emergency Department or through direct admission.

26.1.5 Managing patients who may have or may develop Acute Severe Behavioural Disturbance (ASBD)

Appropriate protocols must be developed and documented, following a risk assessment, that recognise, respond to and manage a deterioration in a person's mental state. These protocols must be implemented during admission, clinical assessment, ongoing management and transfer of patients from admission to discharge.

These protocols must include:

- identifying and responding to the deteriorating behaviour of a patient. This includes escalation of observed changes to a senior colleague, consideration of the causes of the deterioration, and possible referral to specialist mental health services
- triage determination that must take account of observed ASBD or the potential for ASBD to develop. See the NSW Health policy *Triage of Patients in NSW Emergency Departments* and the *Emergency Triage Education Kit*
- development of and documenting of an appropriate patient management plan to address the noted behaviour. The plan must include actions to address any WHS issues to minimise risk to the patient, workers and others from ASBD. The plan must be reviewed when changes are identified and communicated to the team. The patient management plan must be identified and highlighted in the patient's notes, through eMR alerts and other local arrangements for communicating patient related risk, including safety huddles.

Safe physical areas for the assessment and management of patients with ASBD must be identified eg Safe Assessment Rooms in ED (NSW Health guideline *Safe Assessment Rooms*) and identified bedrooms in wards (see Chapter 15 Designing out Security Risk in the clinical environment for further standards).

26.1.6 Patients with particular security needs

In some circumstances, patients who seek treatment or are admitted to a NSW Health Agency are considered 'at risk'.

These patients may include those who:

- present with issues related to domestic, family and sexual violence and child protection and wellbeing concerns
- are children under the care of Department of Communities and Justice (DCJ)
- are in custody (see Chapter 6 Security arrangemnents for patients in custody)
- are confused or cognitively impaired
- require their identity to be suppressed
- have a high public profile.

Where an individual identifies themselves or is identified by another party to have a particular security need, NSW Health Agencies must undertake a risk assessment to identify and address any issues relating to security for that patient and workers.

Where the Police or paramedics bring a patient who has been detained under the *NSW Mental Health Act* or the Mental Health (Forensic Provisions) Act into a NSW Health Agency it must be established if a thorough search has already occurred. This search must be documented by the receiving NSW Health Agency. NSW Health Agency workers, including security staff, may request that an initial or another search of the patient is performed by the Police or paramedic, and a record of the search must be kept.

In developing protocols for these patients to address the identified risk consideration must be given to:

- the reason for the presentation (e. domestic violence, sexual assault)
- whether the individual is a child or an adult
- whether the patient is mentally competent to make decisions
- the legal status of the patient – scheduled, sectioned arrested, detained, AVO etc.
- whether the patient's identity must be suppressed eg for enquiries or on the journey board
- what nonclinical information about the patient is available to workers providing care
- how information regarding risk will be provided to the workers (including non–clinical workers)
- the advice of local police or other agencies (where applicable)
- the safest location for treatment to be provided eg busy or quiet, near security personnel etc
- where the patient is situated in the ward (away from doors, in own room etc)
- any special arrangements to be in place for summoning the Code Black Response Team eg advanced notice of risk on the arrival of the patient, specific information to be included in the briefing, the muster points etc
- briefing security staff and/or Code Black Response Team and other relevant workers regarding any special procedures
- the placement of security staff in the ward to identify individual's seeking entry to the patient and to summon assistance.

In relation to the general security of children and paediatric safe beds, reference must be made to NSW Health Policies on *Children and Adolescent Safety and Security in Acute Health Facilities* and *Child Wellbeing and Child Protection Policies and Procedures for NSW Health.*

Reference must also be made to NSW Health Guideline *Sexual Safety of Mental Health Consumers Guidelines*.

For security issues related to **newborns**, NSW Health Agencies must consider the following additional standards:

- removing signage that identifies the nursery
- taking footprints of each newborn
- taking a clear, high–quality, head and shoulder, colour photograph of the newborn
- installing electronic alarms and bracelets to prevent unauthorised removal of infants
- maintaining a full written description of the newborn, that must be kept with the footprint and photograph and entered as part of the newborn's medical record
- ensuring all hospital personnel (including senior management) wear conspicuous ID cards in the nursery and other newborn areas
- using a distinctive code or second ID card for those authorised to handle newborns
- ensuring that anyone transporting the newborn outside the mother's room wears the appropriate identification
- ensuring that the newborns are always supervised by either the mother or health care personnel
- ensuring the identification of the person taking the newborn home from the hospital is sighted and the child's band is matched with that of the parent
- ensuring newborns are taken to mother one at a time rather than in a group
- marking newborn T–shirts or gowns at the throat and the newborn's blankets in all four corners with the hospital name and logo
- instructing presenting parents (where possible) to request all intending visitors and relatives to present first to the Nurses' Station before visiting
- instructing hospital personnel to ask visitors the name of the patient they are visiting
- ensuring that the mother's or the newborn's name is not visible to visitors eg on the journey board at the nurses station or on care boards in rooms
- placement of camera surveillance at all entrances/exits to the Unit.

Health care facilities must encourage the parent/s to actively participate in the newborn and infant security program, which is best achieved through admissions orientation and awareness programs.

26.1.7 Providing secure worker living quarters

NSW Health Agencies have obligations to ensure safety when providing living quarters for workers (temporary or long–term) and must ensure:

- the design and location of the accommodation is safe including:
  - controlled access to staff accommodation by key or card control access system
  - surrounds, parking areas and paths around the living quarters are well lit and that, as far as possible, there is good line of sight with no areas where a person could hide (eg overgrown bushes)
  - windows, doors and locks can be properly secured while still allowing for adequate ventilation.
- there are procedures that instruct staff how to summon assistance in the event of an incident at the accommodation (eg call 000)
- there are procedures setting out responsibilities for maintenance and repairs.

26.1.8 Providing suitable staffing

NSW Health Agencies must ensure:

- staffing levels and skill mix are suitable to provide clinical care and meet any Award or policy requirements, particularly during peak activity cycles
- staff levels and skill mix allow the early recognition of potential for violence, to deter violence (including when providing increased patient observation) and to participate in the planned response in Code Black situations.

See below for isolated working requirements.

26.1.9 Isolated working

The *NSW Work Health and Safety Regulation* defines 'isolated work' as work that is isolated from the assistance of other people because of the location, time or nature of the work being done.

In NSW Health Agencies examples of isolated working include:

- a unit located in a separate building
- a unit separated from other other areas not occupied 24/7
- a one worker in a location separated from other workers
- a community or hospital–in–the–home workers alone with patients (see Chapter 16 Working in the community).

For remote and isolated facilities refer to Chapter 17 Security in rural health services.

The main hazards that have the potential to increase the risk related to remote or isolated work are:

- exposure to violence
- psychological injuries or mental health arising from the isolation and
- poor access to assistance in the event of an incident.

NSW Health Agencies must as far as practicable must take steps to eliminate isolated working. However, where that cannot be achieved, NSW Health Agencies must manage the risks associated with remote or isolated work. When assessing and managing the risks, consideration must be given to:

- the length of time the person may be working alone
- the time of day when a person may be working alone
- a communication plan with workers
- the location of the work, including proximity to other workers
- access to facilities (eg first aid, toilets, water, eating facilities, personal storage)
- the nature of the work (eg interacts with the public/ patients)
- the skills and capabilities of the worker including any medical considerations
- the physical design of the workplace.

When implementing controls to manage isolated working consideration must be given to:

- rostering so that workers don't work in isolation
- buddy systems
- workplace layout and design
- movement records
- training, information and instruction
- first aid in the workplace
- communication systems. Communication systems need to be provided to allow a worker to call for help in the event of an emergency at any time

A NSW Health Agency must provide a system of work that ensures effective communication with the worker. This can be achieved by ways such as:

- monitoring your workers regularly, by phone calls or periodic visits
- having a check–in process whereby workers are required to contact 'home base' at a nominated time
- having an emergency response plan when workers fail to report in at an agreed time/s.

See the following for more detail on managing the risks associated with isolated working:

- Chapter 16 Working in the community in this manual
- 26.4 below – Managing the risk of violence when working from home
- *SafeWork NSW guidance on remote or isolated work*
- *SafeWork Australia guidance on remote and isolated work*

26.1.10 Staff must be provided with the appropriate skills to prevent and manage violence

The development of skills in violence prevention and management for relevant workers is an important part of managing risk ie being able to de-escalate a potentially violent situation.

It is therefore critical to ensure that training and education for workers is provided in a timely manner, is up-to-date, completion is monitored and the development of skills continues.

Adequate instruction, supervision and support from supervisors is also important in ongoing skill development and application and transfer of these skills to the workplace.

While training is essential in terms of skills development and building the capacity and confidence of workers to prevent and manage incidents, it is not effective as the only risk control measure in place and must therefore be used in conjunction with other controls such as clinical protocols, facility design, access control and provision of equipment eg duress alarms.

Refer to:

- the NSW Health policy *Violence Prevention and Management Training Framework* for detailed information on standard outcomes for training for workers
- this manual Chapter 7 Education and Training as a Strategy to address security risk
- the Chapters of this manual where specific requirements related to skill development are outlined

26.2 Responding to potential or actual violent behaviour

All workers must be aware that a range of options exists when faced with violent individuals. These responses will depend on several factors including the nature and severity of the event, and the skills, experience and confidence of the workers faced with the incident. This response may include immediately triggering a duress response as defined in Chapter 29 Code Black arrangements of this Manual.

This risk could be identified as early as the first access of a medical record that includes a file flag (see 26.3.5), before an outpatient appointment or when something in an initial patient referral or history taking raises concern. This can allow for actions such as planning in the safety huddle, arranging for increased security presence in the area, attendance of the Code Black Response Team in anticipation of an issue, security discussion/planning with ward staff, and in the right circumstances security staff could even introduce themselves to the patient to build a relationship and rapport.

When confronted with a situation of potential or actual violent behaviour, there are immediate and short-term options available to workers, including:

- stay calm
- listen to the patients/other persons current stated needs and action if possible.
- be aware of the potential for violence, recognise contributing factors/warning signs, initiate early, appropriate action
- where the aggressor is a patient, be aware of the possibility of an underlying clinical condition or trauma history contributing to the violent behaviour and consider the need for assessment by a clinician at the earliest opportunity. Consider, when patients behave or respond in unexpected ways, 'What has happened to this person previously?'
- using verbal de-escalation and distraction techniques (see 26.2.1)
- relocation to a calm / low stimulus environment
- sensory modulation techniques
- increasing the frequency or level of observations
- support and encourage the person to manage their own mental state
- when confronted with violent behaviour it is important to remain calm and assess the level of threat as this will help determine the most appropriate action. However, if a worker feels unsafe at any time, they must call for back up or retreat if appropriate
- seeking support from other workers / call for back up (see 26.2.2)
- requesting further assessment/review by the treating team or a specialist mental health clinician
- issuing a verbal warning – if safe to do so and it won't inflame the situation (see 26.2.1)
- requesting that the aggressor leave
- removing the aggressor from the premises (refer to Chapter 14 Role of security staff)
- retreating
- using evasive self-defence/breakaway techniques
- utilising NSW Health security and/or clinical seclusion and restraint policies as appropriate (see below)
- initiating internal emergency response in line with local protocols (refer to Chapter 29 Code Black arrangements)
- initiating external emergency response in line with local protocols eg external security services, police

More than one strategy may be used as considered necessary. However, if a worker feels unsafe at any time they must retreat, and summon assistance eg the manager or the Code Black Response Team. At all times the key priority is to prevent injury to workers and others.

Workers must be supported in their decision to call for assistance early. If a risk of violence occurring is identified before an incident occurs, action must be taken to minimise the likelihood of the violence occurring.

Chapter 29 Code Black arrangements of this Manual provides more information on calling for assistance if faced with an armed hold-up or other personal threat situation. If faced with an armed hold-up situation the priorities are:

- safety of self and
- safety of others.

26.2.1Verbal de-escalation / distraction and warning

When confronted with deteriorating or escalating behaviour, de-escalation may be sufficient to manage the situation. However, de-escalation may not always be possible. Workers must feel that they are able to call for back-up and retreat.

De-escalation techniques must form part of all violence minimisation and management training, along with techniques for identifying conditions and signs of impending violence.

De-escalation techniques consist of a variety of psychosocial techniques aimed at reducing violent and/or disruptive behaviour. They are intended to reduce or eliminate the risk of violence during the escalation phase, through the use of verbal and non-verbal communication skills.

In the face of verbally abusive behaviour, it may be appropriate to set limits on the behaviour. If a worker feels unable to do this or that it is not appropriate to the situation or it will further inflame the situation, back up must be sought.

If a verbal warning is warranted and will not escalate the situation, this must be done in a calm, respectful, 'informative' manner, possibly drawing the individual's attention to the conditions of entry (if these include prohibitions on violence) or patient information brochures outlining patient and visitor behavioural responsibilities. A template for conditions of entry can be found at this link.

26.2.2 Calling for Back-up

If the individual fails to respond to verbal warnings or the situation escalates, workers must seek back-up and / or retreat if necessary. As noted earlier, workers must call for back up any time they feel unsafe.

Depending on the level of perceived threat, imminence or actuality of violence, effect of the behaviour on others, availability of support and local protocols, this may include any / all of the following:

- calling on a more senior worker or clinician to step in
- withdrawing to a safer location
- initiating a duress / Code Black call
- calling police.

All workers must have access to appropriate emergency assistance in the event of threats or actual violence. All work areas must have a clearly documented and practised Code Black response. Facilities must have arrangements in place that consider the possibility of multiple incidents occurring at the same time.

Chapter 29 Code Black arrangements of this *Security Manual* provides specific standards on Code Black response arrangements.

Understanding the role of Security staff

Security staff fulfil a role that has a strong emphasis on assisting with the early identification, prevention and management of incidents. This includes working with and supporting clinical workers as part of a multidisciplinary team.

It is not the role of NSW Health security staff to:

- prevent patients from leaving the facility where there is no lawful authority to retain them (ie they are not involuntary patients under the *Mental Health Act* or there is not a guardianship order in place)
- arrest people suspected of engaging in criminal activity
- search individuals without consent (except in the limited circumstances outlined in Chapter 14 Role of security staff)
- manage high risk incidents involving weapons or hostage situations
- lead patient restraint
- observe a patient who needs clinical observation alone without clinical workers being present.

Chapter 14 of this Manual sets out in further detail the role NSW Health security staff can (and cannot) be expected to undertake while working in NSW Health Agencies.

26.2.3 Evasive / breakaway techniques

No worker should knowingly place themselves or others at unnecessary risk. However, effectively exercised evasive / breakaway technique may provide workers with a controlled physical response when retreat is temporarily blocked, all other non-physical strategies have failed and the worker is under the threat of or suffering an actual attack.

The purpose of evasive techniques in these circumstances is to assist workers to separate or breakaway from an aggressor in a safe manner that does not involve restraint. When properly used, it may minimise the risk of injury and minimise potential trauma for the worker and others.

NSW Health Agencies may determine, via risk assessment, that evasive / breakaway technique training is necessary for a group of workers at high risk of violence.

Evasive / breakaway techniques training must complement other risk control strategies (refer NSW Health policy *Violence Prevention and Management Training Framework for NSW Health Organisations*).

26.2.4 Using seclusion and restraint

NSW Health standards on the use of physical restraint and sedation are set out in the following NSW Health policy documents:

- *Seclusion and Restraint in NSW Health Settings*
- *Management of Patients with Acute Severe Behavioural Disturbance in Emergency Departments*
- Chapter 14 Role of security staff

Seclusion and restraint must only be considered when other preventative strategies have failed or are assessed in the circumstances as not being appropriate.

Use of mechanical restraint

NSW Health Agencies must determine whether mechanical restraints will be used, in what circumstances, who can direct their use, and standardise the type of mechanical restraints used as far as practicable.

This will help ensure workers have experience in correct use. In any event, the equipment must be reviewed and approved for use by the relevant NSW Health Agency clinical governance committee(s) and specific procedures must guide their use. Workers required to use mechanical restraints must be provided with specific training and refresher training in the procedures for restraint, including the use of the equipment.

Appropriate mechanical restraints must:

- be adjustable to reflect the physical frailty of the patient
- be fit for purpose eg manufacturer instructions identify they are fit for use with combative/aggressive patients
- allow the patient to be placed in a sitting or lying position
- have a wide cuff, to prevent tightening and reduced circulation
- have no sharp edges, and not be made from material that is sharp or abrasive
- be made of a material that is easy to clean
- be easy to apply, ie when the patient is moving
- be difficult for the patient to remove
- be able to be secured to furniture ie a bed or chair. It is appropriate to pre–prepare a bed with restraints.

26.3 Managing Post Incident Issues:

26.3.1 Support for workers and others

Every action must be taken to prevent incidents from occurring but where they do occur NSW Health Agencies must support workers and others who have been impacted by the incident.

Workers involved in or witnessing violent incidents must be offered immediate care including emotional support and access to medical assessment/treatment as required.

Workers must be offered access to EAP services. Post incident debriefing must occur to identify ways to improve practice, provide support for workers and support their welfare. Debriefing does not replace individual counselling or intensive psychological support but can assist identifying individuals who need further assistance. Workers must not be forced into participating if they do not want to. See Chapter 29 Code Black arrangements for more detail.

Debriefing does not replace post incident investigations undertaken to identify unmanaged or new risks and contributing factors. NSW Health Policy Directive *Incident Management* provides a framework for managing post–incident issues such as incident reporting, dealing with media, incident investigation and supporting those who were involved in the incident.

Support is detailed in Chapter 30 Effective Incident Management and includes detail on:

- allowing workers to attend the police station during work hours
- providing a support person when making statements to the police
- supporting workers experiencing violence
- support for workers or others who have witnessed an incident

NSW Health Policy Directive for *Rehabilitation, Recovery and Return to Work* provides policy and guidelines for the management of workplace injuries.

26.3.2 Consideration of whether charges should be requested against the perpetrators of aggression

NSW Health Agencies must report all physical assaults and serious threats of assault to the Police, and an event number obtained by the person reporting it. In doing so, the person reporting must provide police with the necessary information to enable an assessment of whether charges will be laid. See Chapter 30 Effective Incident Management for further standards relating to supporting staff who have been assaulted and whether NSW Health Agencies or workers pursue action to seek charges.

26.3.3 Providing ongoing care to patients who have been aggressive while retaining worker safety

Violent behaviour may be a one–off incident or reflect a patten of behaviour. In both cases, following an incident, an individual patient management plan must be developed (or reviewed where one is in place) which includes options such as:

- consideration of who should provide care to the person and the safest way to do so. This could include that the affected worker/s do not continue to provide care to the person and/or all future interactions with the patient do not occur with only one worker present
- negotiating a collaborative patient aggression management plan (where possible in consultation with the patient and/or their carer), setting behavioural requirements and outcomes for failure to comply with these requirements (See 26.3.4 below)
- reviewing the physical location of the patient (including appropriateness and location of the room, removal of items/limiting access to items that can be used as weapons) refer to Chapter 15 Designing out Security Risk in the clinical environment
- reviewing / considering (if not already in place) the actions outlined in Part 26.1 (above)
- where a patient's behaviour is deteriorating providing increased observation. This must be by a clinician with appropriate experience and skill to manage any clinical issues
- considering the need for increased security presence to support clinicians who are managing aggression from a deteriorating patient (refer to Chapter 14 Role of security staff) which sets out the following:
  - security staff alone must not be used to observe patients where there is a clinical/mental health condition that requires clinical observations by a health professional, where the patient is in seclusion or where the patient is in a Safe Assessment Room (SAR). At no time must security staff supervise a patient requiring increased supervision or individual patient specialling without a nurse or midwife present
  - security staff are not trained (nor do they have a duty) to recognise patients whose physical or mental health condition could deteriorate. It would be appropriate for security to provide increased security presence to continually observe the behaviour of a patient to anticipate and prevent absconding or to assist with managing aggression, however this must occur under the direction of the clinician
- issuing written notices (see 26.3.6). These provide a formal process of notifying people that their behaviour is not acceptable and that restrictions may be/have been placed on them for them to continue to receive care.
- patient alerts (see 26.3.5) in conjunction with a supportive patient management plan (see 26.3.4)
- supporting workers to take out an AVO where they feel personally threatened, including implementing systems to maintain their safety (see Chapter 30 *and* 26.3.7).

In determining appropriate long–term actions, these factors must be considered:

- frequency, nature and severity of the behaviour
- circumstances surrounding the behaviour, such as the existence of a medical condition
- extent of exposure of workers, visitors and others to the relevant behaviour
- level of threat or risk the behaviour presents to others
- an individual's ability to comprehend the issues associated with their behaviour and capacity to modify their behaviour
- previous attempts made by workers to discuss concerns with the individual.

26.3.4 Patient management plans

Up to date Patient Management Plans must be developed for anyone who has been aggressive or has the potential to be aggressive to allow the safe and appropriate management of the presenting patient. If the patient does behave aggressively, this must be documented and flagged (see 26.3.5) in the medical record. The patient management plan must consider maintaining worker safety.

Where possible the plan should be developed in consultation with the patient and/or their carer.

Strategies to eliminate or manage known early warning signs or triggers for patients which may involve identifying staff members who are a good fit and/or have developed rapport with the patient should be considered.

26.3.5 Patient alert systems

Patient alert systems, or 'file flagging', can be used for a variety of purposes, including identification of patients and/or their relatives who present a risk to the health and safety of workers and other patients.

Relevant workers must receive clear information on the use of the patient alert system operating in their NSW Health Agency, including during induction.

Note anti–discrimination law does not specifically prohibit file flagging. Obligations under Work Health & Safety legislation support processes to identify individual patients and clients with a propensity to violence where such identification is undertaken to protect workers and other patients as part of the risk management process.

Under the *Privacy and Personal Information Protection Act (PPIPA),* disclosure of personal information is permissible provided it is necessary 'to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates, or another person'. Any patient alert system therefore needs to incorporate these criteria.

Under Section 15 of *PPIPA*, NSW Health organisations have an obligation to ensure information used is 'relevant, accurate, up to date, complete and not misleading'. An active flag must not remain on a file once the risk is no longer current. Health Agencies must have a process to review and remove flags as appropriate.

26.3.6 Written notices

It may be appropriate to issue a written notice to a patient or visitor. These are usually issued in response to repeated violent or aggressive behaviour but may also be issued for a single incident single of violence where there is potential for ongoing violence or where the incident is considered serious. They must be used where a verbal discussion with the patient or visitor has failed to resolve the situation, or a verbal discussion has not been considered appropriate given the risk an individual poses.

There are a variety of written notices that may be used depending on what is necessary under the circumstances to keep workers safe. The types of notices listed in the table below and templates for notices can be found at this link. Note that templates can be altered as needed to suit the needs of the issuing NSW Health Agency.

In choosing to issue a written notice, the NSW Health Agency must consider:

- the frequency, nature and severity of the behaviour
- extent of exposure of workers, visitors and others to the relevant behaviour
- level of threat or risk the behaviour presents to others
- previous attempts made by workers to discuss concerns with the individual
- alternative response options that could be more appropriate to the situation, such as:
  - verbal de-escalation
  - issuing a verbal warning that the behaviour must cease
  - requesting that the individual leave
  - using patient alerts together with patient aggression management plans developed by the multidisciplinary team
  - applying for an Apprehended Personal Violence Order where there is personal ongoing threat to workers
  - reporting the matter to the Police.

NSW Health Agencies must develop local procedures that outline:

- when notices should be used
- who can approve and issue the different notices (generally, the power for approving and issuing a notice will sit with the Chief Executive, who may delegate that power to other staff)
- how a notice will be given
- the process for removing individuals from the premises when required
- what happens when a notice is breached.

Any decision to serve a notice on a patient must be made in consultation with the multidisciplinary care team (including clinical and security staff).

Type of Notice	Impact of Notice	Can be issued to
Written warning	Notifies the recipient that violent behaviour is unacceptable and describes the consequences if this behaviour continues.	Patients and non-patients
Conditional Restricted Access Notice	Restricts access by the recipient to certain times and/or locations and sets other conditions the recipient must follow when attending the facility to help limit risk to workers.	Patients and non-patients
Conditional Treatment Agreement*	An agreement negotiated in consultation with the patient, carer and other relevant stakeholders that sets out requirements for the patient's behaviour.	Patients/carers
Conditional Treatment Notice*	Lists conditions placed upon the recipient's treatment that are necessary for workers to provide health care safely.	Patients/carers
Notice of Inability to Treat^	Restricts the recipient from receiving treatment from the facility outside of emergencies.	Patients/carers
Barring/Exclusion Notice	Prohibits the recipient from entering facility premises unless emergency treatment is necessary.	Patients and non-patients

*** Conditional treatment agreements and conditional treatment notices**

In some circumstances it may be necessary to establish conditions to be able to safety provide healthcare to a patient.

A **conditional treatment agreement** should be negotiated with the patient and, where relevant, their carer to agree the parameters and requirements for treatment to continue. Negotiation with the patient/carer will help ensure compliance with the required measures.

A **conditional treatment notice** is where an agreement has not been reached but for reasons of safety the Health Agency is placing conditions for the person to receive treatment.

Such circumstances may include where a patient has a history of repeatedly:

- presenting for treatment then behaving in a violent or disruptive way
- being accompanied by groups of friends / relatives who significantly disrupt the treating environment
- being accompanied by persons with a history of violent or inappropriate behaviour towards workers or others
- regularly threatening, attempting or perpetrating violence against workers or other patients, including via phone or email.

Depending on the circumstances, the following conditions may be considered when drafting a conditional treatment agreement or notice:

- clearly articulated behavioural requirements (the patient and those accompanying him / her need to understand what behaviour is required)
- setting out the consequences of the patient's failure to comply with those requirements, for example treatment may need to be provided in a different way or at different times, visitors may not be permitted
- where the treatment will be provided eg at what organisation and at what location within that organisation
- who can accompany the patient eg a friend / relative who is able to exercise a calming influence
- who will not accompany the patient eg a friend / relative who is regularly threatening or violent towards workers or others
- the required condition of the patient and those accompanying the patient, for example not being under the influence of drugs or alcohol.

Not every conditional treatment agreement will include all of the above conditions, and some may be more straightforward. However, the conditional treatment agreement must:

- be developed where possible in consultation with the patient and other relevant stakeholders eg guardian, relatives, treating workers, security etc
- focus on the behaviours, not personal characteristics of the individual
- be regularly reviewed according to an agreed timetable (from both a clinical and practical perspective)
- be reviewed when there are changes in the patient's circumstances eg the person moves to a different residential location, or there is an improvement in the person's condition or behaviour
- emphasise that treatment can only be provided in a safe environment
- see also Drafting Written Notices below.

It is not the objective of patient treatment agreements to result in withdrawal of treatment. Such an outcome should only occur in exceptional circumstances after all other efforts have failed (see *Notice of inability to treat – Determining inability to* treat, below).

Agreements should form part of broader risk control strategies aimed at protecting workers, patients and visitors from violence, while at the same time, as far as possible, allowing for appropriate healthcare to be provided.

Conditional treatment agreements must be communicated to all relevant workers and be flagged (see 26.3.5) in the medical record.

^Notice of inability to treat – Determining Inability to Treat

Despite the options available for managing violent patients, there may be, on rare occasions and usually as a temporary measure, a situation where it is impossible to treat a patient without significant, unacceptable risks to those involved.

Depending on the circumstances surrounding this situation, options may include:

- Deferring treatment where possible (if not life threatening) to a time when the risks are better able to be managed eg when more suitably skilled and experienced workers are available, when the patient is more settled, or when back–up (eg police) can be obtained
- Arranging for treatment to be carried out in a different location, where the risks can be more appropriately managed.

The option not to treat (at a particular time, or under particular conditions or at a particular location) would only arise after all other options have been investigated.

Decisions regarding an inability to treat must only be made following consultation with senior clinicians and notification to senior managers. Decisions on inability to treat must be communicated to all relevant workers.

Drafting written notices

Where it is determined that issuing a written notice is an appropriate action, the correspondence must:

- be drafted in consultation with the relevant level of senior management and clinicians involved in determining and delivering care
- have an informative tone, using clear plain language
- focus on the behaviour, not the personal characteristics of the individual, and clearly articulate the matters and behaviour of concern
- identify the possible effects their behaviour may have on workers and other patients, and that it may impact on the ability of workers to provide effective health care in a safe and therapeutic environment
- identify the implications the behaviour has for the NSW Health organisation eg work health and safety responsibilities, duty of care to other patients
- clearly identify the preferred or expected behaviour
- seek the support of the individual in helping the NSW Health organisation meet its work health and safety and duty of care requirements
- clearly indicate the consequences of failing to behave in an appropriate manner, eg conditional treatment agreement; refusal to permit entry to a facility, provision of service elsewhere and under different circumstances; calling the police
- include a mechanism for having the notice reviewed
- invite a response, where appropriate
- be signed by a senior clinician, unit manager, facility manager or Chief Executive as determined by local procedure.

NSW Health organisations must always keep in mind that as with any correspondence issued, written notices are essentially a public statement of the NSW Health Agencies position and must be drafted accordingly.

See the Managing Violent behaviour using written notices factsheet for further details about the procedures for managing ongoing violent behaviour using written notices.

26.3.7 Managing personal threats against individual workers

Where threats are very specifically made against an individual worker the following must occur:

- all such threats must be immediately reported to the appropriate manager, senior manager and the police
- an initial assessment of the potential seriousness of the threat must be conducted as soon as possible, in consultation with police if necessary, to determine whether any immediate action is necessary to ensure the safety of the affected worker
- depending on the circumstances, immediate action may include (but not be limited to) one or more of the following:
  - seeking police intervention
  - banning the perpetrator (whether it be a patient or visitor) from the site (see the Managing Violent behaviour using written notices factsheet)
  - tightening access control to areas where the affected worker is working
  - maintaining a security presence in the relevant work area
  - ensuring the affected worker does not work alone
  - ensuring the affected worker carries emergency communication equipment on their person including a personal duress alarm with person-down capability (as per Chapter 11 Duress Alarm Systems)
  - relocating the affected worker to a different work area
  - ensuring that the necessary file flagging (see 26.3.5) and communication (regarding risks) with other shifts occurs
  - providing the affected worker (and/or their family members where a threat arises from work) with security on the way to and from work or at home depending on the level of threat.

Once any immediate risk is dealt with, a more detailed risk assessment must be conducted, in consultation with police and other relevant personnel, to determine appropriateness of the immediate response and whether further medium or long term action needs to be taken until the threat subsides.

The following questions will assist in determining potential seriousness of the threat and may require input from NSW Police:

- Is the identity of the perpetrator known?
- Does the perpetrator have a history of violence?
- Is, or has the perpetrator been, a client of the organisation?
- Who was the threat made to (if a third party)?
- Who or what was the threat made against (more than one person ie workers, family members, building etc)?
- How was the threat made (eg verbally in face-to-face situation, by phone, by email, by post, was it witnessed)?
- What, if anything, is the threat in response to?
- What is the nature of the threat and how particularised was it (assault, sexual assault, death threat, did it include reference to weapons, bomb threat etc)?
- How long is the threat likely to pose a risk to the affected workers?
- Does the violence risk extend off site?
- How credible is the threat ie what is the likelihood that the person making the threat will actually carry it out?

- Is it likely that the perpetrator knows, or can access personal details of the affected worker eg full name, therefore increasing likelihood that home address and/or home phone number can be obtained?

Questions that will assist in determining the credibility of the threat include:

- Does the person making the threat have a known history of violence?
- Has the person made past attempts (successful or unsuccessful) to carry out the threat?
- Does the person have the means, access and/or opportunity to carry out the threat?
- Is it known if the person has access to firearms or other weapons?

Sources of information in relation to the above may include the following:

- treating clinicians and other workers providing care to the person making the threats
- family or other associates of the person making the threat
- security staff
- incident reporting, security logs/registers
- police
- external agencies such as Community Services/Child Protection Services/NGOs.

Depending on the findings of the risk assessment, NSW Health Agencies may need to consider a range of risk control options for ensuring the safety of the affected worker.

In addition to any immediate actions taken, other internal risk controls may include any/all of the following:

- providing ongoing support to the affected worker and providing assurance that their safety is of the highest priority
- consulting with the affected worker to determine potential short and long term risk control options
- transferring the care of the person making threats to a different facility/location
- formally advising the person making threats that if they attempt to enter the facility, police will be immediately called
- ongoing controlled access to, and/or security presence in, areas where the affected worker is working
- in consultation with the affected worker, relocating them to a different work area or providing alternate duties until the risk subsides
- having security staff accompany the affected worker to and from their car
- considering leave options, if that is the worker's preferred option
- supporting application for an apprehended personal violence order (APVO), see below for further detail.

Where the risk assessment suggests the affected worker may also be at risk when they are not at work (eg the threat is assessed as credible and the perpetrator knows where they live, shop etc) additional action may be necessary. Such action must be specific to the circumstances, based on advice from police and determined in consultation with the affected worker.

Depending on the seriousness of the threat, such action may include (in consultation with the worker):

- arranging for a security risk assessment of the affected worker's accommodation.
- improving physical security of the accommodation premises.
- providing communication devices and/or personal alarms.
- relocating the affected worker at the NSW Health Agency's cost until the threat subsides.
- varying activities eg where they shop, not always following the same route to regular locations etc

Apprehended Personal Violence Orders

Workers must be advised that, in consultation with the police, they have the option of seeking an Apprehended Violence Order (AVO) against an aggressor where they feel a personal ongoing threat. Chapter 30 Effective Incident Management provides detail on this process.

26.4 Managing the risk of violence when working from a remote location (ie working from home)

Flexible work practices such as working remotely (including from home) may increase a worker's potential exposure to existing family and domestic violence. Periods of emergency including public health measures to reduce the spread of COVID–19, related financial pressures, increased stress and disconnection from support networks can also exacerbate existing violence risk or create new risk for the worker that may lead to violence.

When starting remote working arrangements, the NSW Health Agency must identify and manage the risks. Consulting workers is essential in identifying and managing risks given the NSW Health Agency may have limited knowledge of a worker's home environment.

NSW Health Agencies must have a process that provides an avenue for a workers to discuss any specific or individual concerns they may have with respect to their health and safety when working remotely, or the impact any proposed control measures may have on them.

If the worker has disclosed family and domestic violence, consider developing or adjusting their safety plan for remote working.

What the NSW Health Agency can do to minimise risks at a worker›s remote location (ie their home) will be different to what can be done at the usual workplace.

Even when a worker does not disclose a risk of family or domestic violence, or that they cannot work safely at home, the following measures will assist.

Managers/supervisors must:

- maintain regular communication with workers. Avoid directly asking the worker about the violence as this may unintentionally place the worker at risk of serious harm. It is common for perpetrators of family and domestic violence to monitor the worker’s communication including emails, text messages and phone calls
- agree on a course of action if you are not able to contact the worker for a defined period
- appoint a contact person in the organisation that workers can talk to about any concerns
- provide work phones and laptops
- provide continued access to an EAP or other support programs.

If working remotely is not a safe option for the worker, an alternative work environment must be provided, so far as is reasonably practicable. For example, allowing the worker to work from an alternative location or allowing them to work from the office.

Information disclosed by workers regarding family and domestic violence must be kept private and confidential. Disclosure should be on a need to know basis and only to maintain safety or for mandated reporting requirements.

Workers must be made aware of the family and domestic violence leave that is available to them. See the NSW Health policy *Leave Matters for the NSW Health Service* for additional information.

27. Armed Hold–Up

This Chapter has been combined with Chapter 29 Code Black arrangements.

28. Use of Weapons by NSW Health Security Staff

Policy

Currently issuing of weapons, including batons and handcuffs, for use by NSW Health staff is not to occur in any circumstances.

NSW Health Agencies are required to ensure that all practical violence risk control strategies are identified and implemented as outlined in this Security Manual.

The recent review *Improvements to Security in Hospitals* recommended trials of flexicuffs, control sticks and capsicum foam. The process to support the introduction of weapons trials includes consultation with the NSW Police Force and the completion of a risk assessment, considering all risks including potential risk to patients. Any trial would be subject to evaluation in consultation with the NSW Police Force.

29. Code Black Arrangements

Policy

NSW Health Agencies must have documented arrangements for providing a timely and effective response to all Code Black personal threat situations (armed holdup and every other potentially violent incident). These arrangements must be developed, implemented and regularly tested, in consultation with workers and other duty holders.

NSW Health Agencies are responsible for ensuring that workers who are part of a Code Black Response Team are appropriately trained to undertake that role, in line with the requirements set out in NSW Health Policy Directive *Violence Prevention and Management Training Framework for NSW Heath Organisations.*

Standards

Despite all the controls in place to minimise the likelihood of incidents occurring in NSW Health workplaces, incidents of personal threat to a worker that require an urgent team response in the form of a Code Black response, can still occur. The threat may come from patients, visitors, workers or others in the workplace.

It is important that all workers are aware of how to summon assistance while potentially under personal threat. This need for assistance is referred to as a 'Code Black' and this term must be used to describe a situation where a worker or other person is summoning assistance while faced with actual or potential violent, aggressive, abusive or threatening behaviour (including spitting or a threatened infection transmission actions) and may or may not include the presence of a weapon.

Code Black team members may also be engaged to work proactively to prevent a potential situation escalating into an incident, eg where a person has arrived for care and is known to have severe behavioural disturbance. Health facilities must also have protocols to respond to NSW Ambulance workers who call ahead to the Emergency Department with a "Code 29" request for "security/police required at hospital on arrival".

All workers must feel confident that when signalling a Code Black an effective response will be initiated. Workers must also be assured by their managers and colleagues that it is OK to trigger a Code Black response and seek assistance early. Early recognition of an incident and a resulting effective and appropriate response can minimise the risk of injury to workers, patients and others, and in some circumstances actually prevent the further escalation of a situation.

Workers must be supported in their decisions to take action to signal a Code Black. Acceptance by managers that workers are entitled to call for assistance in Code Black situations is an underpinning principle of the NSW Health's approach to work health and safety as described in the NSW Health Policy *Preventing and Managing Violence in the NSW Health Workplace – A Zero Tolerance Approach*.

Workers in community/outreach or isolated settings (including domestic) away from a health facility must also have access to a way of summoning assistance in the event that they are facing a personal threat or attack. This will vary from the Code Black arrangements in place within a facility. Chapter 16 Working in the community provides standards where workers in the community are confronted with a personal threat or attack. For additional requirements to prevent and manage violence see Chapter 26 Violence.

Separate response arrangements will need to be in place for other emergencies such as fire (Code Red), bomb threat (Code Purple), evacuation (Code Orange), medical emergencies (Code Blue), internal emergencies (Code Yellow) and external emergencies (Code Brown).

29.1 What is the aim of a Code Black response?

The aim of a Code Black response is to:

- summon, as a priority, sufficient numbers of skilled, multidisciplinary workers (this may include police / emergency services) to a developing incident (or an incident in progress) in order to prevent or minimise injury or other harm, contain the incident until external assistance arrives or resolve the incident
- support workers, patients and others in threatening or violent situations

Where required the Code Black team members may provide a planned, pre-emptive response that anticipates a potentially difficult/challenging situation and puts into place the necessary resources in the event the situation evolves.

29.2 Developing a Code Black response plan:

Documented Code Black response plans must exist for all areas in a facility and must be developed, and reviewed, in consultation with workers, HSR/WHS representatives and security staff. Input may be sought from external parties who respond to incidents at the facility, such as local Police.

The response plan must be tested via drills and a record of the drills maintained. The plan must include contingency plans for workers while awaiting the arrival of the Code Black Team.

A standardised response plan must be adopted for a facility (and across the NSW Health Agency), as far as possible, to reduce confusion for workers and the Code Black Response Team. A *NSW Health Model Code Black Plan* is set out at this link.

Where a weapon is being used the code black team role may change to keeping the area clear and evacuating where possible. It is not expected that Code Black teams will manage incidents involving weapons, this is a matter for the police.

The elements to be incorporated into a Code Black response plan are:

- the responsibilities of all workers including the Code Black Response Team members (refer to sections 29.3 and 29.4 below)
- that the response must be as fast as possible, so activating the response and alerting the Code Black Response Team must be as simple and as streamlined as possible
- there is a quick and effective protocol for confirming that the Code Black Response Team's attendance is needed ie eliminate false alarms
- contingencies for the possibility of the simultaneous occurrence of Code Black situations
- there are designated and marked mustering points so individual Code Black Response Team members do not confront an incident individually or create confusion by entering an area via multiple entrances. The mustering provides an opportunity for the Code Black Response Team to be briefed and plan the appropriate response
- workers from the location the incident is occurring in must brief the Code Black Response Team on the incident at the musting point prior to entering the incident location. This verbal briefing must include, as relevant, a summary of the current situation, the patient's legal status (if involved), any known triggers or behaviour, actions taken to manage the behaviour, workers or others at risk, any hazards that may be present etc
- the response, and the options available, must reflect the available resources on each shift and in the local area eg worker numbers mean restraint is not possible so the team will focus on ensuring workers and patients are moved to safety if de-escalation is not successful or Police may not be available 24/7. Options may also include letting the person leave the premises or locking down the premises to prevent someone entering
- the Code Black Response Team must allocate responsibility for who will lead each of the response options eg who will attempt de-escalation, who will direct and participate in any restraint or signal retreat
- when, during the Code Black response, the assistance of the Police will be sought, who in the Code Black Response Team makes that determination and how communication with the Police will occur
- identified escape routes and safe havens for both workers and the Code Black Response Team
- easy access to necessary equipment, such as personal protective equipment (safety glasses, gloves) and mechanical restraint (if available) and/or chemical sedation for patient. These may be held in a Code Black Kit
- any mechanical restraints (if used) are fit for purpose (check manufacturer's instructions). See Chapter 26 Violence for further detail
- arrangements for the Code Black Response Team attendance when there is an identified potential for violence ahead of an incident developing/escalating.

Regular liaison with the local Police about facility Code Black plans or opportunities for Police cooperation must occur. This may be through the memorandum of understanding local area committees.

In remote facilities where there are limited workers Code Black responses may include pre-arranged documented plans to utilise appropriate support from outside the facility. This may include establishing arrangements with local business to share security resources (e.g. security patrols) or utilising local suitably skilled and trained personnel eg State Emergency Services (SES), Rural Fire Service (RFS). In these instances external responders must be provided with training in the local Code Black response plan and be able to quickly access the building, ie have their own codes or keys.

Participation in drills is a requirement for external responders. These drills must be documented.

29.3 Code Black responders

Each shift must have a designated Code Black Response Team and the following must occur:

- the names of the Code Black Response Team members must be identified and documented for every shift. See template for recording Code Black Response Team members at this link. A worker with the responsibility for ensuring this occurs, and to manage any necessary changes during a shift, must be identified for each shift
- those on the Code Black Response Team must be able to immediately cease their duties to respond

- the Code Black Response Team must involve a multidisciplinary team who work together to provide for the safe management of a patient or other individual
- Code Black Response Team roles must be allocated eg who will bring the Code Black kit (if used), who will be briefed by workers in the area of the incident, who will lead the de–escalation, who will signal retreat etc
- the Code Black Response Team must include a delegated clinical leader, regardless of whether the individual involved is a patient
- in the event of restraint needing to occur the clinical team leader will be responsible for ensuring the individual's airway is maintained, and be alert to any indications of positional asphyxiation, injury to hyper flexed joints and ensure the minimal amount of force only is maintained throughout the restraint
- any restraint (where used) must be undertaken by all members of the team ie this is not to be undertaken by security staff alone
- any vacancy (eg due to sick leave) needs to be identified and filled at the start of the shift or during the shift if the person proceeds onto sick leave
- if members of the Code Black Response Team are not available for the whole shift (eg on different shift patterns) this must be identified and replacement workers noted
- provide immediate advice to the appropriate person where there is an inability to perform the role eg illness or injury
- if a member of the Code Black Response Team cannot continue in the team for the whole shift (eg allocated duties that cannot be immediately ceased or is sick/injured) replacement workers must be identified

29.4 Identifying responsibilities for all workers

The Code Black response plan must clearly state the responsibilities of **all workers** to:

- use personal protective equipment, safe havens and escape routes, as provided
- follow any instruction given by the Code Black Response Team during an incident, and provide any relevant information to the team regarding the incident
- document all incidents in ims+, patient notes (if relevant), restraint registers (if applicable)
- participate in any operational review and debriefing of a Code Black incident
- cooperate with changes to procedures and any other preventive measures identified through any risk management or post incident investigation processes
- attend training in violence prevention and management and participate in Code Black drills as necessary.

The Code Black response plan must clearly state the responsibilities of **managers** to:

- support workers to summon assistance early in a developing incident
- ensure workers are given skills to identify early intervention opportunities in order to prevent escalation of the incident or where they need to call for assistance (eg activate a duress alarm or call the internal emergency number 2222 or call NSW Police on 000), to prevent a delayed response to the incident
- ensure workers are given the skills to utilise the protocols for summoning assistance, and trained in the use any equipment, eg duress alarms including a 'hands–on' session with the actual equipment to be used
- ensure the release of workers to attend training, drills and arranging the backfilling of positions as necessary
- ensure that incidents are reported and reviewed/investigated to identify any additional controls needed to prevent recurrence of the incident type, or to identify improvements to the planned response.

The appropriate manager (this may be the facility manager) must ensure adequate numbers of workers are available to respond to Code Black calls and are able to leave their duties to respond when a Code Black incident is occurring.

29.5 Determining how workers will summon assistance

Within a Code Black response, plan communication protocols must be included which:

- determine the communication systems that are fit for purpose and needed to allow a worker to call for help in the event of an emergency at any time. These could include:
  - duress alarms
  - mobile phones
  - internal landline phones
  - satellite communication systems
  - personal security systems or personal duress systems
  - radio communication systems
  - distress beacons such as a personal locator beacon (PLB).
- provide clear instructions for workers on how to seek assistance and use the devices provided
- reinforce that patient call emergency buzzers must not be used, as the response will be for a medical emergency (Code Blue) rather than a Code Black emergency.

See Chapter 11 Duress Alarm Systems and Chapter 16 Working in the community for further requirements.

29.6 Managing Post Incident Issues

Code Black response plans must incorporate the need to record the details of Code Black call and the response provided as well as any legislative reporting requirements (eg security staff involved in restraint). The required reporting of the incident must occur as soon as possible after the event utilising the local processes (ie ims+, security logs (if used), patient notes (if relevant), restraint registers (if applicable) and Code Black review documentation.

Where the incident involved a patient, information must be communicated to the clinical team in charge of the patient's care, if they were not present during the incident. There must be a review of the patients care plan in light of the incident and identification of any preventative strategies to be added/modified to this plan (if clinically indicated) to reduce the possibility of ongoing incidents.

Relevant information regarding the incident, triggers, controls, care plans etc must be shared with other workers, including security staff, at safety huddles and this must be documented.

Post incident investigations and operational debriefs must consider information from all workers involved in the incident. If workers are unable to attend a debrief they must be offered the opportunity of providing written or verbal feedback beforehand.

Risk assessments must be reviewed to determine if there were elements of an incident that indicate the need for additional controls to be implemented.

NSW Health Policy Directive *Incident Management Policy* provides standards for incident types that must be reported to the Ministry of Health and provides a framework for managing post–incident issues such as incident reporting, dealing with media, incident investigation and supporting those who were involved in the incident. The incident may also need to be reported to external agencies such as NSW Police or SafeWork NSW.

NSW Health Policy Directive *Rehabilitation, Recovery and Return to Work* provides policy and guidelines for the management of workplace injuries.

29.7 Training and practice

The Code Black response must be regularly tested via drills and a record of the drills maintained.

Worker	Training	
Code black response team	The Code Black Response Team must receive training together to ensure an understanding of roles, particularly as it relates to restraint.	
	Activity Teams that carry out restraint (includes relevant Mental Health and Emergency Department workers)	**Mandatory Training** – The team are Category 3 workers if they carry out restraint, as set out in the *NSW Health Prevention and Management of Violence Training Framework*, and as such must have completed all required training. **Drills** – The Team must put the Code Black response plan into practice using active scenarios. Drills must practice mustering, handover from workers about the incident, de–escalation, restraint and decision making during an incident.
	Activity Teams that do not carry out restraint (eg in locations where patient restraint would not be carried out such as a community centre)	**Mandatory Training** – The Team are Category 2 workers, in addition they must be trained in any local team response protocols and drills (as above). **Drills** – The Team must put the Code Black response plan into practice using active scenarios. Drills must practice mustering, handover from workers about the incident, de–escalation and decision making during an incident.
Community Code Black Response (remote to a facility)	**Mandatory Training** – The workers are Category 2 workers, in addition they must be trained in any local team response protocols and drills (as above). **Drills** – The Code Black response plan must be practiced using active scenarios. Drills must ensure that devices are able to be used and operational, escalation processes and communication is effective.	
Workers	**Mandatory Training** – Depending on the work and the level of risk may be classified as Category 1 or 2 workers for training (see *NSW Health Prevention and Management of Violence Training Framework*) **Table top exercise or drill** – All workers must be aware of how to raise the alarm, requirements to wear duress when provided, how to operate and where to wear the duress, where to retreat to for safety and any specific local issues eg what to do in an armed hold up for cash handling areas, code black procedures for home visiting/community work.	

30. Effective Incident Management

Policy statement

NSW Health Agencies are required to ensure there is a system in place for notifying/recording and investigating incidents and near misses. There must be a process in place to ensure reports/notifications are provided to *SafeWork NSW* and the NSW Ministry of Health, as required.

NSW Health Agencies must ensure that where /incidents occur, they are managed effectively to minimise the impact on those involved and those witnessing the incident.

Following an incident an investigation must be commenced as soon as possible and be conducted in accordance with NSW Health policies for *Incident Management*, the *Work Health and Safety: Better Practice Procedures* and *Chapter 1 Security Risk Management* of this Security Manual. Feedback must be provided to relevant workers when incidents are investigated.

Workers who are impacted by security incidents must be provided with the necessary immediate and follow-up support. Workers who wish to report incidents to NSW Police must be supported to do so, with this support continuing through any subsequent legal proceedings related to the incident.

The reference to incidents in this chapter includes any incident in which an individual is abused, threatened or assaulted and includes verbal, physical or psychological abuse, threats or other intimidating behaviours, intentional physical attacks, aggravated assault, threats or assault with a weapon and sexual assault.

Standards

The following standards must be implemented unless a documented risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address the identified risk). Any departure from the standards must provide, as far as reasonably practicable, at least the same, or if not, a higher level of control to manage the identified risk.

30.1 Documented incident management arrangements are in place

There must be pre-determined operational procedures in place to deal with the range of incidents that may occur in the workplace.

These procedures set out the actions for workers and managers to ensure the effective management of an incident, including how to activate a timely response to the incident in progress (eg Code Black – personal threat, Code Red – fire, Code Purple – bomb threat etc).

Workers must be given training/instruction and participate as necessary in drills, on the procedures for incidents (including reporting) and their role.

The incident procedures must include allocating of roles responsible for the following elements:

- assessing the developing incident to determine its magnitude, severity and the numbers of people involved and the nature of any physical and psychological trauma to workers, patients and others as well as damage to the facility
- ensuring the immediate safety of those involved, including where the incident is still in progress. Workers must not however place themselves at risk in doing this
- co-ordinating the immediate response, including contacting and briefing external agencies such as police, fire or ambulance
- co-ordinating the communication both during and after the incident.

30.2 Ensure immediate support for people involved in an incident

Arrangements must be in place to ensure workers are supported following an incident as necessary. These arrangements must include:

- immediate first aid (physical and psychological/ emotional) can be provided to those involved in an incident (this includes those directly involved, witnesses or others who may be affected)

- provision of information on accessing the Employee Assistance Program.
- practical assistance such as calling their next of kin, providing a taxi voucher home if unable to drive etc
- supporting the worker if they feel unsafe/apprehensive, including not requiring them to continue to provide care to a patient who has been violent to them
- supporting and encouraging workers to report any incident that resulted in assault to the Police and request action to be taken by the police against the perpetrator
- where reporting an assault to Police involves attendance at a police station, the worker is accompanied by another worker who they agree can appropriately support them, unless they decline this offer. Time taken attending the police station for a work matter must be considered work time
- arrangements are in place to ensure the incident is recorded in the incident management system (ims+) as soon as possible. If the worker is injured and unable to report the incident, the incident must be reported by a witness or their manager, and the injured worker encouraged to report when they can.

At an appropriate time debriefing will occur, see Chapter 29 Code Black arrangements for detail.

30.3 Ensure processes are in place to ensure follow-up support with workers involved in incidents

Workers must be supported by managers and their colleagues following an incident. This may be through just providing an opportunity to talk or looking out for symptoms or after-effects.

Where a manager or other workers recognise symptoms or after-effects of an incident (eg flashbacks, not sleeping, irritable, not acting as they usually do) the affected worker is supported in the workplace and provided information on the Employee Assistance Program (EAP). These symptoms or after-effects may not occur straight away so support and ongoing assistance must be offered at any time after the event.

Support may also need to be provided to other workers, patients and carers who witnessed an incident.

Support must also be provided for workers who are at risk of experiencing vicarious trauma or secondary traumatic stress. This can include use of clinical supervision practices:

- **vicarious trauma** is the experience of trauma symptoms that can result from being repeatedly exposed to other people's trauma and their stories of traumatic events
- **secondary traumatic stress** is the emotional duress that results when an individual hears about the firsthand trauma experiences of another.

Workers must be supported throughout any criminal justice proceedings arising from work related assault against them.

A worker who attends a police station or a court, either as the victim or Health Agency's nominated support person, for proceedings arising out of a work-related assault, will be considered to be on-duty for the time they are completing these actions. The Health Agency must nominate a support person in consultation with the worker, who can appropriately support the worker (unless they do not wish this to occur). Workers have the right to privacy and to seek legal representation. Worker are advised of their right to access Union support related to the matter.

Workers must be advised that, in consultation with the Police, they have the option of seeking an Apprehended Personal Violence Order (APVO) against an aggressor **where they feel a personal ongoing threat**. See below for further detail.

Workers must be provided with information on the injury management and return to work processes consistent with the NSW Health policy *Rehabilitation, Recovery and Return to Work*.

Apprehended Personal Violence Orders

There are different types of Apprehended Violence Orders (AVOs), for workplace violence an Apprehended Personal Violence Order (APVO) may apply. AVOs must be taken out by a person and cannot be taken out by the Health Agency.

Where an APVO is applied for the following will apply:

- where workers wish to seek an APVO they are supported by the Health Agency to do so
- the workplace address can be given for the APVO rather than the worker's personal address (there may be circumstances where a personal address is required to also be included in the APVO)
- where a worker is successful in gaining an APVO in response to work related violence any costs associated with the application for an APVO are to be covered by the Health Agency
- see the APVO factsheet to assist development of a management plan and ongoing arrangements in response to an APVO and example conditions that can be included in an APVO application.

30.4 Incident investigation and review of systems of work

When investigating an incident, the following must occur:

- the investigation is commenced as soon as possible after the incident, so that the NSW Health Agency can find out information when the people involved can remember events and the order in which they happened
- information is collected and recorded such as what happened, where it happened and why it happened, by conducting interviews, reviewing written reports, training records and workplace policies
- causal factors are identified by considering all aspects of the incident such as the environment, work tasks, systems and procedures, responses and people involved
- review the risk control measures to identify if they worked as intended and how they could be improved
- consider privacy and confidentiality when keeping information and records.

This process must be undertaken in consultation with workers and their representatives. Input must be sought from other stakeholders who may have a perspective or expertise relevant to the incident eg security staff or healthcare consumers.

Any conclusions reached must be documented and communicated to all relevant parties, such as HSRs, health and safety committees and affected workers. This documentation must include a summary of the incident, what has been done and what will be done in the future.

In addition to any investigation the NSW Health Agency must undertake a new or review a current risk assessment to identify any further risks and controls required (see Chapter 26 Violence for further standards).

If a matter has been referred to Police, the incident must still be investigated to assess whether risk controls are effective and if the response procedures worked the way they were intended.

It is important to maintain a supportive environment in which workers feel safe to discuss their concerns about violence and aggression, or to report incidents.

For further information refer to:

- SafeWork Australia's guidance material
- NSW Health *Incident Management Policy*
- *Chapter 1 Security Risk Management* of this Security Manual
- NSW Health *Work Health and Safety: Better Practice Procedures*

30.5 Audit process

The framework for incident management is audited in the *NSW Health Work Health and Safety Audit*.

The implementation of the incident management process is audited in the *NSW Health Security Improvement Audit* under Chapter 26 Violence.

NSW
GOVERNMENT