Protecting People and Property

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

June 2013
# Protecting People and Property: NSW Health Policy and Standards for Security Risk Management in NSW Health Agencies.

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter Number</th>
<th>Section Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>SECTION 1 Security Risk Management Framework</td>
</tr>
<tr>
<td>2</td>
<td>Security Risk Management</td>
</tr>
<tr>
<td>3</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>4</td>
<td>Security Risk Management in the Planning Process</td>
</tr>
<tr>
<td>5</td>
<td>Health Facility Design</td>
</tr>
<tr>
<td>6</td>
<td>Health Service Leasing of Property to or from External Parties</td>
</tr>
<tr>
<td>7</td>
<td>Security Arrangements for Patients in Custody</td>
</tr>
<tr>
<td>8</td>
<td>Security Education and Training</td>
</tr>
<tr>
<td>9</td>
<td>On-going Review and Continuous Improvement of Security Risk Management</td>
</tr>
<tr>
<td>9</td>
<td>SECTION 2 Core Security Risk Controls</td>
</tr>
<tr>
<td>10</td>
<td>Access and Egress Control</td>
</tr>
<tr>
<td>11</td>
<td>Key Control</td>
</tr>
<tr>
<td>12</td>
<td>Duress Alarm Systems</td>
</tr>
<tr>
<td>13</td>
<td>Lighting</td>
</tr>
<tr>
<td>14</td>
<td>Workplace Camera Surveillance</td>
</tr>
<tr>
<td>15</td>
<td>Role of Security Staff in NSW Health</td>
</tr>
<tr>
<td>15</td>
<td>SECTION 3 Security Risk Controls in Priority Areas</td>
</tr>
<tr>
<td>16</td>
<td>Security in the Clinical Environment</td>
</tr>
<tr>
<td>17</td>
<td>Security of Staff Working in the Community</td>
</tr>
<tr>
<td>18</td>
<td>Security in Rural and Remote Health Services</td>
</tr>
<tr>
<td>19</td>
<td>Security in Pharmacies</td>
</tr>
<tr>
<td>20</td>
<td>Security in Car Parks</td>
</tr>
<tr>
<td>21</td>
<td>Security of Property</td>
</tr>
<tr>
<td>22</td>
<td>Security of Information</td>
</tr>
<tr>
<td>23</td>
<td>Security of Medical Gases</td>
</tr>
<tr>
<td>23</td>
<td>Security of Radioactive Substances</td>
</tr>
<tr>
<td>SECTION 4 Security Risk Controls in Unplanned Events</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>--</td>
</tr>
<tr>
<td>Fire, Evacuation and other Emergencies</td>
<td>24</td>
</tr>
<tr>
<td>Bomb Threat/Terrorist Threat</td>
<td>25</td>
</tr>
<tr>
<td>Violence</td>
<td>26</td>
</tr>
<tr>
<td>Armed Hold-up</td>
<td>27</td>
</tr>
<tr>
<td>Weapons are not to be Used by NSW Health Security Staff</td>
<td>28</td>
</tr>
<tr>
<td>Code Black Arrangements</td>
<td>29</td>
</tr>
<tr>
<td>Effective Incident Management</td>
<td>30</td>
</tr>
</tbody>
</table>
Introduction

Purpose and Scope of Document:

The purpose of the NSW Health document ‘Protecting People and Property: NSW Health Policy and Guidelines for Security Risk Management in Health Facilities’ (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 on-going risk management.
  - Consultation.
  - Appropriate documentation and record keeping.
  - Regular monitoring and evaluation.

How the Manual is Arranged:

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

<table>
<thead>
<tr>
<th>Section 1</th>
<th>Security Risk Management Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 2</td>
<td>Core Security Risk Controls</td>
</tr>
<tr>
<td>Section 3</td>
<td>Security Risk Controls in Priority Areas</td>
</tr>
<tr>
<td>Section 4</td>
<td>Security Risk Controls in Unplanned Events</td>
</tr>
</tbody>
</table>

As a Manual, is not intended to be read from cover to cover. However, 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.
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 information from unauthorised disclosure, and the protection of property from intentional damage and from theft.

Violence:
Any incident or behaviour in which staff feel abused, are threatened or assaulted in circumstances arising out of, or in the course of, their employment including verbal, physical or psychological abuse, threats or other intimidating behaviours, intentional physical attacks, aggravated assault, threats with an offensive weapon, sexual harassment and sexual assault.

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 Director-General of Health including:
- A Local Health District; or
- 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.

This Manual does not apply to the Ambulance Service of NSW or to the Ministry of Health which have separate standards.

Staff:
For the purposes of this Manual the term ‘staff’ 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
- volunteers
- an apprentice or trainee
- work experience students

Anyone who carries out work for NSW Health Agency is given the legal status of ‘worker’ under s.7 Work Health and Safety Act 2011.

Other duty holder:
An ‘other duty holder’, referred to in section 16 of the 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 Labour Hire Companies, building /service contractors, retail stores, leasors, . Each duty holder must comply with that duty to the standard required by WHS Act, even if another duty holder has the same duty.
1. Security Risk Management

Policy:

NSW Health Agencies are required to ensure that:

- 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.
- Each stage of the risk management process is documented.
- Incidents are reported and investigated.
- Risk control strategies are monitored and regularly evaluated for effectiveness.
- In order to optimise the effectiveness of risk control strategies, a system for collaboration and information sharing between clinical, WHS and security personnel is established (e.g. security committee).
- Consultation with staff and/or nominated WHS representatives and occurs during all stages of risk management.
- Consultation, co-operation and co-ordination with other duty holders occurs, where there is a shared duty.
- Chief Executive and the Board get relevant information on security related risks and how they are being addressed.

Standards:

Overview of security risk management:
Security risk management encompasses the assessment of all aspects of the clinical and non-clinical environment, including consideration of internal and external risks e.g. local crime profile.

NSW Health Agencies need to identify hazards, assess the risks arising from the hazards in their workplaces and develop strategies to eliminate, or where they can not be eliminated, minimise these risks.

This process is referred to as risk management. The NSW Health Policy Directive PD2013_050 Work Health and Safety Better Practice Procedures outlines the risk management process and in what circumstances it should occur.

The security risk management process should be undertaken, in consultation with staff and other stakeholders, by those who have expertise in the areas being assessed. A multidisciplinary team of clinical, non-clinical, WHS and security staff should be convened to undertake the appropriate aspects of the process.

Consultation as an essential part of risk management:
Workplace Health and Safety legislation requires NSW Health Agencies to consult with its staff and/or their representatives.

Consultation is a pivotal activity at all stages of the risk management process. Staff 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 effective controls. During the
security risk management process consultation should also occur with other appropriate stakeholders, such as Police.

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.

**Security hazard identification:**
In order to eliminate or control factors that can affect the security of people and property, a structured process for identifying security hazards that exist in the workplace, and the contributing factors, must be undertaken.

Security hazard identification is the process of identifying all situations, procedures, events or factors in the workplace and during the course of work (including the design of premises, during work related travel or during the procurement of equipment) that could potentially cause injury or illness to staff, 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 should 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.
- Consulting with staff 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.
- Formal workplace inspections and security audits.
- Developing scenarios about what could happen during or as a consequence of a security incident.
- Analysing incidents and breaches.
- Considering all possible contributing risk factors, e.g. staffing and skills, work environment/building design; equipment; training; clinical procedures.

**Security risk assessment:**
Security risk assessment is the process of determining how likely it is that someone could be harmed or property 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.
- Likelihood of injury/illness/loss/damage occurring.
- Number of people/amount of property at risk.
- Existing control strategies.

The process of assessment involves:
- Consulting with staff and their representatives.
- Examining the experience of the workplace or other similar workplaces including a review of incident data and near misses and other information such as prosecution decisions.
- Reviewing relevant guidance material, industry codes of practice, Australian Standards, and NSW Health policies and guidelines.
• Reviewing clinical, WHS and security information relating to incidents.

Risk Managers and Security Managers should be consulted to identify the tools currently used within the NSW Health Agency.

Part of the assessment process is the prioritisation of risks for action. Security hazards assessed as having a high risk factor are required to be eliminated/controlled immediately. However, low priority hazards that can be cheaply and easily fixed should also be done without delay. Actions should be planned and prioritised to improve workplace security.

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

Eliminating the hazard is the most effective way of controlling risk. Where elimination is not possible NSW Health Agencies must take the following measures in the order presented to minimise security risks to the lowest level reasonably practicable:

1. Substituting the hazard, which gives rise to the risk, with a hazard which gives rise to a lesser risk.
2. Isolating the hazard from the person put at risk.
3. Minimising the risk by engineering means.
4. Minimising the risk by administrative means.
5. Using personal protective equipment.

Where a single measure is not sufficient for effectively minimising risk to the lowest level, a combination of the above measures is required.

**Priority workplaces:**
Within the health workforce a number of priority areas exist where the likelihood of security incidents occurring may be increased and these areas must be identified. These areas may include, but are not limited to, emergency departments, maternity units, mental health services, oral health clinics, ICUs and HDUs, community health services, drug and alcohol services, pharmacies and car parks.

It is essential that the hazards identified in these areas are dealt with as a priority and the effectiveness of risk control strategies regularly monitored.

**Monitoring and review:**
To ensure that the outcomes from the security risk management process continue to effectively address security issues, monitoring and evaluation of risk control strategies should be undertaken.

Security risk monitoring and review involves:
• Consulting with staff who are working in that workplace, to assist with identifying if 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 action where they are identified.
• Reviewing existing risk assessments and any measures adopted to control the risk.
• Monitoring implementation and 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.
NSW Health Agencies must review an existing risk assessment and any measures adopted to control the risk, and provide feedback to staff on changes, whenever:

- There is evidence that the risk assessment is no longer valid, 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 staff or other stakeholders at the workplace.

It is also advisable to periodically review risk assessments and control strategies, to ensure they remain relevant and effective.

**Hazard and incident reporting, management and investigation:**

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 should be assessed and strategies to address the risk implemented in a timely way. This action should be communicated to relevant staff.

**Hazard reporting:**
As an essential part of a risk management, all staff should be encouraged to report problems as soon as they notice them using the appropriate local process eg IIMS

Appropriate action to address hazards should be taken immediately.

**Incident reporting:**
All security related incidents should be reported and recorded using the appropriate local format (eg hospital incident form, IIMS database).

Depending on the nature of the incident, it may need to be reported to the NSW Health Agency Chief Executive, the Ministry of Health or external agencies such as the NSW Police or WorkCover NSW (refer to NSW Health Policy Directive PD2014_004 Incident Management Policy).

**Incident management:**
All security related incidents need to be efficiently and effectively managed. Chapters in this Manual provide standards to address a range of security related risks.

**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 should:
- 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 patients and/or their family, be conducted by a multi-disciplinary 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 (e.g., 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.
- 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 staff.

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.

**Injury management:**
The loss or disruption that can result when an incident occurs in the workplace can be multiplied when that incident leads to an injury to staff or a patient/visitor. A comprehensive, effective security program should 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 staff member and the workplace with the implementation of early intervention and early return to work strategies.


**********
2. Responsibilities

The **Ministry of Health** is responsible for:
- Setting the statewide policy framework for security risk management.
- Monitoring policy implementation and effectiveness.

The following responsibilities apply to security risk management within NSW Health Agencies:

**Board members** are responsible for exercising due diligence to ensure the NSW Health Agency meets its obligations under the WHS Act, including by taking reasonable steps to ensure:
- The NSW Health Agency has systems in place to identify, assess and eliminate or control security related risks.
- They get 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 matters and take appropriate action to resolve issues or concerns.

**Chief Executives** are responsible for ensuring:
- The resourcing, development, implementation and maintenance of effective security risk management within their NSW Health Agency, which is based on a structured, on-going risk management process, consultation, appropriate documentation and record keeping and regular monitoring and evaluation.
- That NSW Health security risk management standards are met.
- Staff are consulted in the development and implementation of security procedures and when determining and purchasing equipment.
- Appropriate legislative and Ministry reporting requirements are met, including compliance with the *Security Industry Act 2007* in nominating a suitably qualified and experienced person as a ‘nominated person’ for the purpose of holding the Master License and its associated responsibilities.
- Staff are provided with the necessary skills to prevent and manage security/violence related issues.

**Facility Managers** are responsible for:
- Identifying individuals responsible for security administration within their facility.
- Ensuring the on-going 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.
- Reporting all crimes and suspicious activity to police.
- Ensuring the Chief Executive, Risk Managers, Security Master Licence holders, and where necessary external authorities such as Police and WorkCover, are advised of security related incidents, as required under local 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 staff and their WHS representatives, WHS and security staff, and other duty holders on security matters.
✓ Keeping staff 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 staff.
✓ 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 staff and ensuring training is provided and attendance documented.
✓ Reporting security related incidents as required under local procedures.

Security Officers and Health and Security Assistants are responsible for:
✓ Maintaining current security licence and first aid certificate.
✓ Responding to security related requests and providing appropriate assistance as necessary, in line with relevant policies and procedures.
✓ Identifying and reporting security risks within the facility.
✓ Responding to security related requests, in the clinical environment, under the direction of clinicians.
✓ Providing reports to management on security matters.
✓ Providing security recommendations, consistent with their licensing level, experience and allocated role, to management on matters of security within their facility/service.
✓ Implementing the security directives of management.
✓ Working within the requirements of legislation, NSW Health policy directives and local protocols.
✓ Security audits and inspections, as appropriate.
✓ Maintaining documentation and reporting incidents.
✓ Maintaining security provisions such as key control, ID systems as required.
✓ 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.

All staff 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.
✓ Participating in consultation and training on personal and property security matters.
✓ Not knowingly placing themselves or others at unnecessary risk.

*******

Policy:
NSW Health Agencies are required to ensure that the implications for security are considered and documented in all planning and decision making.

All plans and proposals (including but not limited to construction/refurbishment of premises, changes to equipment, and changes to systems of work such as models of care) must identify and assess security risks and include strategies to eliminate, or where they can’t be eliminated, minimise security risks.

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

Standards:
Planning takes place at all levels of the organisation across all disciplines. When planning and making the resulting decisions that affect staff and/or the place of work eg accommodation, work practices, purchasing equipment, security issues need to be considered.

All planning activities must include consideration of security risk management, including:
- Strategic planning.
- Business planning.
- Service development planning.
- Disaster/emergency planning.
- Project Definition Planning (as part of Facility planning).
- Procurement Processes, including processes for procuring services, premises, equipment, furniture, fixtures and fittings.
- WHS/security improvement and management planning.
- Individual department plans.

Other Resources:
4. Health Facility Design

Policy:
NSW Health Agencies are required to ensure, in consultation with staff 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 and this Manual must be referenced and compliance achieved during all stages of the facility planning, design or refurbishment process. This includes security considerations related to any temporary accommodation or other temporary arrangements, e.g. wards, offices, parking, contractor access.

Workplace safety, risk management and security staff 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 staff and those involved in the planning and building, that all reasonably foreseeable security risks are identified, assessed, eliminated where reasonably practicable or effectively minimised.

Standards:
The Australasian Health Facility Guidelines (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, staff and visitors.
- Eliminate design features that result in unacceptable practices or risks.
- Update guidelines to meet current clinical practices and standards.
- Eliminate duplication between various guidelines.
- Minimise recurrent costs and encourage operational efficiencies.

AusHFGs are not intended to restrict innovation that might improve performance or outcomes.

The AusHFG are available in electronic format at:
www.healthfacilityguidelines.com.au
The following standards must be implemented unless a risk assessment determines another control is more appropriate:

**Crime Prevention through Environmental Design (CPTED)**

Crime Prevention through Environmental 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 Crime Prevention Through Environmental Design (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.
- Relevant staff must be trained to understand and apply the CPTED principles (Refer to the NSW Police website [www.police.nsw.gov.au/community_issues/crime_prevention/safer_by_design](http://www.police.nsw.gov.au/community_issues/crime_prevention/safer_by_design) for information about their training course ‘Safer by design’).

CPTED principles fall into four broad categories: territorial reinforcement, surveillance, space management and access control. They must form part of the complete risk management strategy as they apply in particular to the way that buildings and their surroundings are designed but also have an application in determining the most appropriate lay out of individual work areas.

- **Territorial reinforcement** 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 is 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.

  Eg if ‘staff only’ areas are provided, staff are more likely to pay more attention to the area and note an intruder. Additionally, if these areas are clearly separated from other areas (eg by signposting or locking) it reduces 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).

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

- **Surveillance** draws on the natural surveillance principle where people feel safe in public areas where they can be seen and interact with others. This principle refers to the way in which working areas of buildings have been designed so that priority areas are overseen and watched by other staff going about their normal business. This is different to surveillance using CCTV, which is more fully covered in Chapter 13.

  For example, pathways to car parks can be designed in full view of passers-by and overlooked by offices, wards and walkways.
• **Space management** is linked to territorial reinforcement and also draws on the image principle and refers to the impact produced by a building that appears to be well cared for. The belief is that a run down structure with graffiti may attract criminal activity and offenders.

• **Access control** draws in 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 target.

**Local working environment decisions**
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 ensure that all security related risks are identified, assessed, eliminated or effectively controlled.

**********
5. Leasing of Property to or from External Parties

Policy:
NSW Health Agencies are required to ensure, in consultation with staff, 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:
In some instances, NSW Health Agencies, as part of providing services to the community, are required to lease premises eg located within shopping centres, office blocks, community halls, schools or other premises remote from their community health team base. Alternatively 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 of the abovementioned scenarios any security related risks should be identified, assessed and controlled to ensure the security of staff, patients and clients of the services and the public is maintained. 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 (e.g. security grills, locks, alarms, lighting).

Where NSW Health Agencies intend to lease premises to or 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).

Leasing Premises from External Organisations:
In assessing the requirement for security when leasing premises from external organisations, NSW Health Agencies must consider, as a minimum, the following issues:

- For assessment of property
  - Geographical location eg is it isolated.
  - Crime risk/business security assessment of the locality - police can provide statistics and advice.
- Type of service to be provided from the premises including hours of operation and associated security requirements.
- Security assessment of the property, e.g. locks, alarms, interior and exterior lighting, security doors and screens.
- Availability of safe parking for staff and patients including during and after hours as relevant.
- Also consider geographical location in terms of WHS issues, e.g. driving distances, remoteness, and access to emergency or security services.
- Location relative to major roads and transport routes, e.g. an isolated location may be more attractive to criminals.

For Business Continuity planning
- Will field communication technology work eg reception for mobile phones, remote and hard-wired duress alarms etc.
- Proximity of local police services and/or a duress response team and their hours of operation relative to service operation.
- Number of staff to be working at the premises.
- The parking/public transport arrangements, including its proximity to the premises. Hours of operation in relation to parking location, e.g. will staff be arriving/departing or packing/unpacking vehicles in the dark.
- Security of approaches, eg well lit, line of sight particularly access to parking and building egress, potential hiding places.
- If there are no current security arrangements that can be accessed, providing a service from that location should be reconsidered.

- The hours of operation.
- Any restrictions by the lessor/property owner on changes that can be made eg would the property owner allow the installation of security grilles, CCTV, duress alarms or approved locks.
- The service to be provided from the premises and the likely clientele.
- Security already provided eg within a shopping centre, 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.
- 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.

When Leasing to External Organisations:
In assessing the requirement for security when leasing premises to external organisations, NSW Health Agencies must consider, as a minimum, the following issues:

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.
Location of ATMs
Where Automatic Teller Machines (ATMs) are being installed in NSW Health Agencies consideration should be given to the risks associated with attempted ram raid and explosion style thefts.

An effective control strategy is to eliminate access to the ATM by vehicles, therefore priority should be given to placing the ATM in an area that is not visible from outside the facility such as on a first floor.

Where it is determined that placement on a floor above ground is not practical or would introduce new risks, a risk assessment relating to the alternative placement of the ATM should be conducted to ensure appropriate risk control strategies are put in place. To assist NSW Health Agencies a simple Risk Assessment Tool is provided at Attachment A to this Chapter.

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

Security Arrangements
- The role of health facility security staff and what they will and will not respond to.
- 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.
- If the tenant is a pharmacy, then there need 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.

Duty to 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 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.
Attachment A

Controlling the risk of ram raid style attempted theft of Automatic Teller Machines (ATMs) on NSW Health Agency Premises

The information in this document is provided to assist NSW Health Agencies assess the risk of attempted ram raid style theft on ATMs where an ATM can not be placed on a floor above ground level.

Risk assessment of alternative locations should be undertaken and consider the following issues:

Information Gathering:
- Is there a recent history of criminal activity on or around the health facility?
- Have there been other robbery attempts on ATMs in the local area or nearby suburbs?
- Is the ATM to be located on an external wall?
- Is the ATM to be located inside the premises, but close to the periphery?
- Structural integrity of the walls and traffic/pedestrian flow where it is planned to locate the ATM?
- Would an internal ATM be clearly visible from external areas during the day?
- Would an internal ATM be illuminated during the night so as to increase external visibility?
- Would there be external signs advising of internal ATM locations?
- Would the ATM be potentially accessible to a vehicle?
- What contractual/commercial arrangements are in place with the supplying financial institution?
- What would be the utilisation rate of the ATM?
- How would cash delivery be achieved safely?
- Can the area around the ATM be fitted with bollards?
- Would the installation of bollards interfere with disabled access?
- Is the area under CCTV surveillance?

Determining Risk Reduction Strategies:
- Risk reduction activities will be dependent on the range of individual circumstances relating to the particular ATM, as well as the potential risk vs convenience to staff, patients and others and could include:
  - No external signage indicating there is an ATM inside.
  - Ensuring the ATM is not visible from the exterior of the building.
  - Placing bollards at entrances to prevent unauthorised parking and to prevent people driving through the entrance.
  - Providing safe access for cash delivery including were the cash delivery vehicle would park.
  - Placing ATMs overtly under CCTV surveillance.
- When identifying ATMs that will require risk reduction strategies and when determining potential risk reduction strategies key stakeholders (including unions, relevant financial institution, security manager, structural engineer and police local area command) should be consulted.
- A primary activity when identifying risk control strategies is to ensure that they do not introduce new, unplanned risks.
- Chief Executives (or delegates) should approve all significant risk control strategies before they are implemented.
6. Security Arrangements for Patients in Custody

Policy:
NSW Health Agencies are required to ensure, in consultation with staff, relevant external agencies (ie Corrective Services NSW, Juvenile Justice NSW, Department of Immigration and Citizenship and NSW Police) and other duty holders that:

- All reasonably foreseeable security risks associated with patients in custody are identified and assessed.
- 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 Agencies, are developed and implemented.
- The procedures are appropriately documented and communicated to relevant staff.

The security of patients who are in custody is the responsibility of the agency in whose custody they are held.

Standards:
NSW Health Agencies need to be aware that NSW Police, Corrective Services NSW, Juvenile Justice NSW and the Department of Immigration and Citizenship have operational protocols, regarding the transport and supervision of their inmates/detainees during treatment in a public health facility.

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).

- Develop facility protocols for managing patients who are in the custody of another 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 should provide a clear role delineation between the role of staff of the NSW Health Agency and the external Agency, and must be developed in consultation with the relevant external Agencies.
- Ensure police, corrective services, juvenile justice and immigration management and custodial staff are aware of any relevant health facility protocols to be followed when inmate/detainee patients are in the facility. This may be achieved by providing escorting officers with written information upon their arrival at the facility.
- Ensure escorting officers are advised upon arrival of local evacuation plans and places where a patient in custody can be taken in the event of a fire, blackout or other emergency.
- Ensure the implementation of a system so that the appropriate NSW Health Agency staff (eg the facility manager, security service 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.
• Ensure all inquiries from the public and the media regarding the release of any official information are channelled through to the relevant external Agency.
• Ensure clinical enquiries from Justice Health medical staff in relation to inmate patients of Corrective Services and Juvenile Justice are answered with due regard to the clinical and statutory responsibilities for the patient’s ongoing care.

Corrective Services NSW patients in custody:

The following Corrective Services NSW standards should be reflected in NSW Health Agency procedures:
• The number of Corrective Officers required to guard a patient in custody is to be determined by Corrective Services NSW (CSNSW).
• CSNSW is responsible for ensuring all escorts/hospital supervisions are conducted in accordance with the relevant CSNSW protocols, policies and procedures.
• Patients in custody admitted to a health facility for medical treatment are to be given the same considerations as extended to any other patient. Personal matters pertaining to the patient in custody are to be treated with strict confidentiality by NSW Health staff and Correctional Officers.
• Security needs are to be appropriately instituted by CSNSW to ensure that the patient in custody's medical needs are not compromised. Where there is a conflict between security requirements and the patient’s medical needs, treating clinical staff and the Officer in Charge of the escort need to negotiate an appropriate solution.
• Relieving Correctional Officers are to identify themselves to the nurse in charge. Their identity is to be confirmed with the outgoing Correctional Officer.
• Clinical staff responsible for the patient's care should identify themselves to the attending Officer in Charge of the escort.
• The names and contact telephone numbers of the Correctional Officers in charge of the escort, General Manager/Manager of Security/Correctional Centre are to be given to the health facility administration in case of an emergency or any infringement of facility protocol.
• The nurse in charge is to be informed when the number of Correctional Officers is reduced or increased.
• Correctional Officers are to ensure patients in custody do not engage in offensive or violent behaviour while at the facility.
• Correctional Officers are not to utilise nursing or other NSW health Agency staff, including security staff, to supervise a patient in custody at any time.
• Correctional Officers will carry firearms in accordance with CSNSW policies and procedures.
• A patient's in custody's medical care is the responsibility of the facility's medical and nursing staff.
• Patients in custody are not to be left unsupervised or unescorted at any time.
• Female Correctional Officers are to supervise female patients in custody who are outpatients or inpatients for any obstetric and/or gynaecological matter.
• Correctional Officers are to determine their meal arrangements based on risk assessment (e.g., one at a time when there are two Correctional Officers on duty). If the Correctional Officers are not required to be with the patient in custody, and are on a break, they should have access to NSW Health staff amenities.
• Access to the patients in custody is to be controlled at all times—allowing as few entry and exit points as practicable. The Officer in Charge of the Escort in consultation with the nurse in charge is to negotiate the best and most secure area to hold the patient in custody.
• Approval from the Officer in Charge of the Escort (delegated from the General Manager of the Correctional Centre) is to be given before a patient in custody can receive visitors.
• Correctional Officers are responsible for screening visitors and enforcing any restrictions.
• Approval from the Officer in Charge of the Escort (delegated from the General Manager of the Correctional Centre) is required for visits from legal, welfare and/or religious persons.
• Patients in custody may be allowed to make one telephone call to an approved number on admission to hospital. An escorting officer will make the call for the patient in custody.
• Patients in custody may have access to television hire at their own cost, with the approval of the Officer in Charge of the Escort (delegated from the General Manager of the Correctional Centre).
• Visitors may be permitted to arrange television hire for the patient in custody by signing the contract and paying the fee.
• Gifts intended for the patient in custody will not be accepted from visitors.
• Correctional Officers have the right to refuse or terminate visits. Visitors who have visiting restrictions will be denied visits. In the event that a visitor to a patient in custody refuses to leave the hospital room, the hospital security manager is to be contacted.
• Complaints by NSW Health staff concerning a breach of protocol can be made to the nurse in charge who will then refer the complaint to the General Manager of the Correctional Centre.
• Patients in custody may also complain to the relevant bodies on issues related to their care and treatment by NSW Health Agency staff.
• A delegate of the General Manager of the Correctional Centre may visit the hospital while the patient in custody is being guarded to review security arrangements and review daily documentation.

Juvenile detainee patients:
The following Juvenile Justice NSW standards must be reflected in NSW Health Agency procedures:
• All detainee patients from Juvenile Justice are to be escorted by Youth Officers. The Centre Manager of a Juvenile Justice Centre can determine the number of Youth Officers required.
• The detainee patient should, wherever possible, remain in the vehicle until called, if there is a wait on arrival to an appointment.
• No detainee patient is to be left under the supervision of any person other than officer/s of Juvenile Justice NSW (the number of officers to be consistent with the detainee’s criminal history and risk level).
• A detainee patient is not to make telephone calls without direct approval of the patient's Juvenile Justice Centre.
• Detainee 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 staff.
• Security needs are to be appropriately instituted to ensure detainee patients’ medical needs and the safety of staff, other patients and visitors are not compromised.
• Relieving Youth Officers are to identify themselves to the nurse in charge. Their identity is to be confirmed with the out going Youth Officer. NSW Health Agency
staff responsible for the detainee patient’s care should identify themselves to the attending Youth Officer/s.

- The name and contact telephone number of the Youth Officer’s supervisor is to be given to the health facility administration in case of an emergency or any infringement of facility protocol.
- NSW Health Agency staff are to be informed when the number of Youth Officers is reduced or increased.
- Youth Officers are to ensure that the inmate does not engage in offensive or violent behaviour while at the facility.
- Youth Officers are not to rely on NSW Health staff including nursing staff or security staff to supervise a detainee patient regardless of reason or length of time.
- Clinical staff are to be advised before handcuffs are removed if the detainee patient has a history of violence or escape. The handcuffing of a detainee patient is a decision best made by the centre manager of the juvenile justice centre in which the detainee patient is normally held.
- Detainee patient medical care is to be left to the facility’s medical and nursing staff.
- Detainee patients must be supervised or escorted at all times by a Youth 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 reversed barrier nursed.

Note: In the abovementioned circumstances Youth 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, Youth Officers will not leave an exit unsupervised unless the detainee’s condition would prevent escape.

- Female Youth Officers are to supervise female detainees patients who are outpatient or in-patient for any obstetric and/or gynaecological matter. Male Youth Officers can only attend if female Youth Officers are unavailable.
- Youth Officers are to eat their meals in the detainee patient’s room, one at a time when there are two officers on duty. If Youth Officers are not required to be with the detainee, and are on a break, they should have access to the same amenities as NSW Health Agency staff.
- Access to detainee patients is to be controlled at all times - allowing as few entry and exit points as practicable.
- Approval from the Centre Manager of the Juvenile Justice Centre needs to be given before a detainee patient can receive visitors. Youth 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 Youth Officers.
- Detainee patients are to have access to television hire, at their own cost, with the approval of the Centre Manager of the Juvenile Justice Centre.
- Gifts intended for the detainee 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. Youth Officers have the right to refuse or terminate visits.
- Complaints by NSW Health Agency staff concerning a breach of protocol can be made to the nurse in charge. Detainee patients can also complain to the Patient Advocate (if the facility has one) on issues related to their care and treatment by NSW Health Agency staff.
Patients in the custody of Police:

Introduction:
Where a person has been arrested, detained or taken into Police custody, and requires assessment or hospitalisation, treatment or mandatory testing, the Police role is to provide personnel to guard the person at a security level that is appropriate to the prisoner and the circumstances.

Each Local Area Command (LAC) has Standing Operating Procedures (SOPs) for the hospitals in their area and these will guide the Police response. Some LACs provide Police on rotating shifts so that not all Police undertaking guard duty for the duration of the admission will be from the same LAC, nor necessarily from the LAC responsible for the arrest.

Arresting Police:
It is the responsibility of the LAC to which the arresting Police are attached to provide the initial guards and possibly the subsequent shift.

NSW Health Agency staff must be advised of any potential risks relating to the admission or hospital stay, including the risk of violence.

Bedside Courts:
As soon as practicable after Police refuse bail for a person admitted to hospital, arrangements will be made by a senior Police Officer at the arresting LAC to attend the hospital with a local court magistrate or clerk of the court, to convene a ‘bedside court’ to determine bail.

Once bail has been granted or an agreement entered into, it will no longer be necessary for Police to be in attendance at the hospital.

Persons Refused Bail:
If the prisoner is bail refused or cannot meet the bail conditions, the Police guard will remain until the prisoner is transferred into the custody of CSNSW.

Police Guard:
The Police will:
• Have at least two Police Officers (not probationary police officers) performing guard duty at all times
• Ensure approval is obtained from the police officer in charge of the investigation or a Senior Officer/Duty Officer prior to any visitor and/or legal representative speaking to or visiting a prisoner
• Not allow visitors physical contact with the prisoner
• Keep the prisoner in full view at all times
• Patients are not to receive gifts. Not accept gifts on behalf of the patient
• Protect staff from the risk of violence
• Be in full uniform (unless in permanent plain clothes) with full appointments and
• Ensure all local guard duty standard operating procedures are adhered to.

Any questions relating to visitors or the manner of the guard should be directed to the Officer in Charge of the matter or the LAC Custody Manager. Questioning of the prisoner should only occur with the consent of the Director of Medical Services or treating clinician. Police questions relating to medical treatment will be directed to the senior nursing or medical staff. Police will not perform nursing duties of any kind.
Police on guard do not have the discretion to release or leave the prisoner or change the guard arrangements without prior approval from the Officer in Charge except in exceptional circumstances.

Medical procedures that take the prisoner from the ward such as surgery or birth must be first approved by the officer in charge of the matter and Police will remain on guard at exits to the procedure room.

Spontaneous requests from hospital staff to remove the prisoner from view of the guard will be refused until the circumstances are outlined and approval is obtained. In an emergency situation it may not be possible for the officer in charge to approve removing a prisoner from the ward for a medical procedure. In these circumstances police officers will ensure that the prisoner is within their line of site at all times.

Normal considerations for consent to treatment apply to guarded prisoners with some exceptions including for example:

- Blood sampling in cases related to the provision of the Traffic Act
- Medical examinations and blood sampling for evidence under the Crimes Act
- Medical examinations under the Children and Young Persons (Care and Protection) Act
- Court orders made under the Crimes (Forensic Procedures) Act.

In cases where a prisoner is treated at the hospital and not admitted, they will be returned to the Police Station in Police custody.

**Restraints:**
Prisoners who are requiring restraints such as handcuffs should be so detained in a manner that does not interfere with the provision of medical treatment. Removal of restraints to allow for treatment is at the guarding Police Officer's discretion and will only occur when two Police Officers are present.

**Supervision:**
Police Supervisors (may visit the hospital while the prisoner is being guarded). Relevant daily documentation, such as a daily guard record sheet, should be completed by the attending Police.

Any changes to the guarding arrangements should be documented, approved by a supervisor and communicated to the Director of Medical Services and person in charge of facility (e.g. General Manager or Executive Director). In cases involving current inmate patients of the Corrective Services NSW, or Court cells etc, local protocols and SOPs will apply.

**Mental health patients in the custody of Police:**
The Memorandum of Understanding between NSW Police and NSW Health, and the associated flowcharts, outline relevant security considerations in relation to people who may have a mental illness and who are in the custody of the police.

**Firearms/taser security:**
NSW Health Guideline GL2013_002 provides guidance for the security of firearms in health facilities and vehicles and should be read in conjunction with the Memorandum of Understanding between NSW Police and NSW Health.

The Commissioner of Police has given authority for Police Officers to remove and place a firearm in a hospital or health facility safe only in the following circumstances:
• The Police Officer believes that this is the safest course of action and
• The safe conforms with the type that has been approved by the Commissioner. For this purpose the minimum standard has been approved as a single locking unit of a type that is used in non-24 hour Police premises. It is to be a locked steel safe that cannot be easily penetrated and be bolted to the structure of the premises. No other person must have access to a key while the firearm is stored therein.

In summary the decision to remove a firearm is to be made by the individual Police Officer at the time, taking into account all the facts presented by the particular circumstances and in accordance with the NSW Police Force Handbook.

**Forensic patients arriving from a mental health facility:**
In some circumstances forensic patients, not being held in Correctional Centres, are admitted to hospital or require medical attention in a health care facility removed from their mental health facility.

In these instances a risk assessment of the patient will be undertaken by the staff at the mental health facility prior to transporting the patient to a health care 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.

Information on the risk assessment and any particular security requirements will be provided to the health care facility by the centre they are coming from. Where it is determined that there is a risk that the patient may engage in violence or attempt to abscond, a mental health care staff member, or other appropriate persons, should accompany the individual during the course of their treatment.

**********
7. Security Education and Training

Policy:
NSW Health Agencies are required to ensure that:
- All staff are provided with appropriate security related education and training, including violence prevention and management training.
- Education and training are appropriate to the role of the staff member, targeted to the level and type of security risk that may be encountered in the course of their work, and consistent with NSW Health Policy PD2012_008 Prevention and Management of Violence Training Framework.
- Training for staff in high risk areas and security personnel must be provided prior to commencement of as soon as possible after commencement of duties. Other staff must receive training as soon as possible after commencing duties.
- Details of security related education and training conducted within the NSW Health Agency are documented and maintained.
- Training is provided on an ongoing basis, including regular drills, in order to update and maintain skills.

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

The following standards must be implemented unless a risk assessment determines another control is more appropriate (a risk assessment may also identify additional local controls necessary to address the identified risk).

Identifying security related education and training needs for all staff:
- Conduct training needs analysis, as part of an on-going security program, 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.

- When identifying and assessing security related training needs ensure the following elements are considered:
  - Duties being undertaken.
  - 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 staff and response personnel (e.g. duress teams, security staff and police).
  - Experience in the position.
  - Previous training.
  - 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).
• Determine the most effective method of delivery considering the needs of the target audience and the subject matter e.g. restraint techniques must include a practical element.
• Education and training activities should 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 qualifications and experience.
• Records of who attended training, the nature of the training (topics covered) and when, must be kept.

In determining appropriate education and training content, the required competencies outlined in PD2012_008 Prevention and Management of Violence Training Framework and PD2012_035 Aggression Seclusion and Restraint: Preventing, Minimising and Managing Disturbed Behaviour in Mental Health Facilities, as a minimum must be referenced.

When should security related education and training be provided?
• Relevant security education and training must be provided:
  - At induction or prior to commencing duties, where possible.
  - On arrival at a new work area (e.g. ward induction).
  - During the course of employment /engagement (on-going refresher training).
  - When there are changes to work practices or procedures.
  - When new activities are introduced to the work area.
  - When incident investigations identify new hazards and/or new controls are introduced.

PD2012_008 Violence Prevention and Management Training Framework for the NSW Public Health System
• This document provides the minimum standards for training delivered to staff, and must be reflected in local training and education strategies.

Specialised training:
• The NSW Health Agency must identify and implement any specialised and ongoing training needs for:
  - Supervisors and managers.
  - Security staff.
  - WHS/Risk management practitioners.
  - First Aid Officers.
  - Fire Wardens.
  - Return to Work Co-ordinators.
  - Health and Safety Representatives.
  - Duress response staff.

Duress Responders
• Staff identified as duress responders to a clinical or corporate/security incident, in accordance with Chapter 29 of this document, must be provided with specific training to enable them to undertake this role effectively, including:
  - The process for duress response.
  - Assessing a scene.
  - Verbal de-escalation.
  - Negotiation skills.
- Evasive self-defence, physical restraint techniques, use of mechanical and other restraints where appropriate and approved for use, and associated legal implications.

Evaluation of security related education and training activities:

- 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:
  - Staff 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.
- Training and education should be reviewed at least every three years or if:
  - The outcomes of an incident indicate that review may be required
  - If requested by the Health and Safety Committee, Health and Safety Representative or other relevant person
  - There are changes to premises, equipment, systems of work, laws, or policies that impact on the training required.
8. On-going review and continuous improvement of security risk management

Policy:
As part of a process of on-going review, NSW Health Agencies are required to evaluate all aspects of security risk management and ensure that evaluation outcomes are used in the on-going risk assessment actions.

As a minimum, NSW Health Agencies are required to:
- Undertake an annual internal security survey to assess compliance with the requirements of this Manual, and the recommendations arising from any previous security risk assessments (the annual survey must be carried out by a team that includes a person with a security license and extensive health care security experience, a WHS representative, a clinical nurse, and a representative from management).
- Undergo an external security survey every five years utilising the same tool as used for the annual security audits* in order to provide a valid point of comparison. External audits can be undertaken by suitably skilled security personnel from other NSW Health Agencies.
- Ensure that the results and recommendations of the annual and external surveys are provided to the NSW Health Agency risk manager and the facility/service manager.
- Ensure that the results and recommendations of the annual and external surveys are provided to the Chief Executive and the Board as the organisation’s officers and primary duty holders under WHS legislation.
- Ensure that a security improvement plan, for both the internal and external audits, is developed from the findings and recommendations of the survey and implemented. The improvement plan must include actions and time frames for implementation, and be signed off by the service manager and the HSC/HSR.

*This includes any tool determined by the Ministry of Health to be mandatory from time to time.

Standards:
The following standards must be implemented:

Measuring and evaluating performance as part of continuous improvement:
- NSW Health Agencies must measure existing security risk management performance against a set of pre-determined indicators, evaluate progress and feed the outcomes of this process back into on-going 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:**
A number of sources of information can be used to develop performance indicators and these may include:
- Hazard and incident reports.
- Duress response records.
- WHS committee meeting minutes.
- Results of security audits, surveys and inspections.
- Workers compensation data.
- Workplace grievance records and staff turnover in priority areas.

When using existing information sources to develop performance indicators, consideration should 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.

Security related performance indicators may include:
- Percentage of staff trained.
- Percentage of staff trained within 4 weeks of commencing work.
- Timeliness of audits.
- On-time completion/implementation of the security improvement plan.
- Compliance with security polices, e.g. wearing of duress alarms.
- Timeliness of repairs/maintenance/ replacement of security equipment (e.g. alarms, locks, cameras).

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.

************
9. **Access and Egress Control**

**Policy:**
NSW Health Agencies are required to ensure, in consultation with staff 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 can not be eliminated, effectively minimised.

NSW Health Agencies are required to 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.

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:


**Standards:**
In general effective access and egress controls are in place to provide a secure work environment and involves:

- Appropriate 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 e.g. door alarms.
- Providing safe access and egress, especially after hours and during emergencies.
- Controlling access to vulnerable areas and securing vulnerable patients.
- Clear wayfinding.
- Instituting access/ identification systems that allow members of the organisation to be identified and allocates access limited by the requirements of the position held by a staff member.
- Applying the principles of Crime Prevention Through Environmental Design (CPTED) as outlined in Chapter 4, to assist in managing risks associated with access control.

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):

- In assessing the most appropriate access and egress controls, NSW Health Agencies must consider, as a minimum, the following issues:
  - 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 access to staff only and treatment areas can be regulated and controlled.
- The need to secure vulnerable patients.
- The need to provide for rapid escape routes and access to safe havens for staff eg in the event of a violent incident.
- The need to prevent unauthorised access or, in the case of some patients (e.g. children, patients scheduled under the Mental Health Act), unauthorised egress.

Doors:
- Perimeter/external access doors must be locked and access restricted to the minimum necessary points in the building (especially at night).
- Perimeter/external access doors must meet the following building design standards and any additional standards set out in this Manual or the Australian 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 choked 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 staff 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.
- After hours public and staff entry points must be fitted with video/CCTV intercom systems to allow screening of members of the public presenting at the door, to allow staff 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 staff 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. Staff must be cautious in allowing entry in to 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.
- Glazing in doors and panels beside doors must be resistant to breakage and not shatter on impact, i.e. the glazing must resist being breached.
• 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 site of the door.
• 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 the potential 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 decals (refer to Chapter 29 for more information on Code Black arrangements).

Windows:
• Perimeter windows must minimise the opportunity for entry to, or exit from, a window by the use of 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).

Wayfinding:
• All signage must conform with the requirements set out in GL2014_018 Wayfinding for Health Facilities, and assist staff, 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.

Name Badges:
• Security staff and Health and Security Assistants must have their full licence displayed at all times while on duty in line as required by section 36 of the Security Industry Act 1997.
• For other staff, full names, worn at chest height, are the default position for NSW Health and this is influenced by a number of factors including:
  - The right of a patient to be able to identify a staff member.
  - 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.
• Staff in emergency departments and mental health units and drug and alcohol units, are only required to display first names and family name initial and the name badge can be issued with this information only. In any other area, a decision to not display both first and last names on name badges must be based on a
documented risk assessment. Care must be taken to ensure that patients and others are always able to identify individual staff members.

- 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 staff can be individually identified within the work environment.
- With the exception of emergency department and mental health staff, all decisions not to display surnames must be based on a documented risk assessment, relevant to the department and approved by the facility manager.

Identity/Access Systems:

**Determining access for staff:**

- The level of access to be granted to a staff member 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 may be required to attend.
- Identity/access cards must only be issued where a new staff member’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 drivers licence.
- Arrangements for determining access must be in place to support the required access by staff 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.
- Level of access for a staff member 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 staff member 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.
- Staff 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. This must be done sensitively and only for as long as required for the purpose of taking the photo. 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 (Refer to M2012_01 Policy on Identity and Full Face Coverings for NSW Public Sector Agencies).

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

Administration of an Identity/Access System:

- 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 staff 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 (i.e., 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. Staff should 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 staff 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.
- 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 staff 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 staff to advise, out of business hours, of lost or stolen cards.

Determining access for others

- Each facility must have a documented procedure for determining, approving and recording the level of access of a non-staff members to ‘staff only’ areas. This procedure must include the following features:
  - Access must be limited to the role they are to perform or the purpose of their attendance at the facility.
  - A record of access to staff only areas within a facility must be kept and must include an indication of when the individual is expected to exit the facility i.e. expected meeting duration.
10. Key Control

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

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

‘Keys’ as used in this Chapter refers to metal keys, electronic keys, swipe, electronic access cards and key pad codes.

Standards:
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);

Electronic locks, and associated swipe cards, have significant security advantages with ‘keys’ that can be reprogrammed and can also be remotely ‘deleted’ if lost.

Managing Keys:
- The authority to hold and control the issue of keys must be determined and documented (Refer to Chapter 9 for standards on appropriate access control).
- Movement of keys must be controlled using:
  - **Key Authority Records.** All personnel authorised to draw and return keys should have their name printed and their specimen signature recorded. This may be done via a secure electronic log.
  - **Key and Security Logs.** Where all keys issued are recorded. Completed logs should be reconciled and retained for a period of not less than twelve months from the date of the last entry and should identify keys issued on a daily or temporary basis.
- 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.
- Ensure that the person identified as responsible for facility key control, must:
  - Conduct a stocktake, at least annually, and record results.
  - Report any unaccounted keys to the appropriate supervisor.
  - 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 afterhours.
- Ensure staff are advised that keys should not be worn around the neck, as this is a possible strangulation risk or could be used by a violent person to draw the staff member closer.
- Ensure keys are not left lying around in view.
• Authority to draw keys is kept up to date by deleting from key authority cards the names of staff who:
  - Have ceased their engagement. Confirmation that the return of keys has occurred must be included and documented in the termination clearance process.
  - No longer require access to the area to which the key gives access.
• Ensure keys not on issue are stored in a locked container which should be located out of sight of unauthorised persons.
• Ensure, at the time of installation of locks, that the keys are given to the person identified as responsible for facility key control, who will ensure:
  - 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.
• Ensure all keys for the same lock or entry are individually numbered to indicate the lock or entry they fit and the actual key number for that lock or entry.
• Ensure the loss, or suspected loss or compromise of a key is reported to the facility key control officer, include mechanisms for staff members to report losses where they occur out of hours.
• Take immediate action to replace compromised locks or entries.
• Staff are not permitted to cut keys to their offices or other work environments. Cutting of additional or replacement keys must only be:
  - Authorised by a nominated officer delegated by the facility manager.
  - Cut by an authorised locksmith who is contracted by the facility. Note: cutting of security keys must only be done by a person licensed 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.
• Destroy keys that are no longer required. Details of the destruction should be entered on the appropriate key control card/system.
• Ensure key cutting codes and key blanks used by NSW Health Agencies that have their own key cutting/duplication capability are protected at all times. If a NSW Health Agency site has a key cutting machine and they have master blanks or restricted blanks, then they are required to comply with the NSW Security Industries Act and have a Master Licence.
• Ensure codes used to control code locks are only available to those with a legitimate reason for access, including paramedics and police, where necessary, and remind staff they are not to disclose individual alarm or door codes to other staff, family members or others (patients and visitors).
• Digilocks or coded doors need to have master key override hardware.
• Change key pad access codes with more than one user every six months or sooner if circumstances change or dictate 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.
• Communicate changes to codes to all relevant staff in a timely way.

**********
11. Duress Alarm Systems

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

A review of all alarm systems must occur, appropriate to the level of risk, as part of the on-going risk management process.

Staff members 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.

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

All staff who are required to work within an emergency department must be provided with a mobile duress alarm. The mobile duress alarm must be worn at all times while working in the emergency department.

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.

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):

- In assessing the requirement for alarms, NSW Health Agencies must consider, as a minimum, the following issues:
  - Size, layout and location of the facility/service.
  - Potential for violence against staff, patients or others within and in the grounds of the facility.
  - The type of work being carried out by staff, the work practices in place and whether staff 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 staff members are working in isolation.
  - Whether the staff members are involved in cash handling.
  - Goods and equipment stored in the area.
  - Security of pharmaceuticals.
  - Level of external security risks.
  - Level of internal security risks.
  - The potential for exits to be left open by staff, patients or visitors.
  - The security needs of ‘at risk’ patients such as wandering elderly patients in wards, or children at risk of unauthorised removal from the facility.
- Potential for use of emergency exits (e.g. 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.
- Potential for assault of persons (e.g. staff or visitors) in the 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 duress alarms.

- In assessing the requirement for alarms and particularly duress alarms, NSW Health Agencies must consult with staff and other duty holders, where they exist, working in relevant areas such as:
  - Mental health services.
  - Emergency departments.
  - Pharmacy and other drug storage areas.
  - Women’s health and maternity units.
  - Paediatric Units.
  - Youth health units.
  - Sexual assault units.
  - Cash handling and storage areas.
  - Isolated facilities/units.
  - Car parks and grounds.
  - Vehicles (e.g. ambulances).
  - Alcohol and other drugs services including methadone units
  - ICUs and HDUs.
  - Aged care wards/dementia units/brain injury units/rehabilitation units
  - Community services.
  - Theatre recovery.

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

- Duress alarm systems used for community health staff require GPS capability.

- Alarm system features and configuration must be appropriate to address the identified risks.

- When tendering for 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.
  - Benchmark criteria are included to ensure the system operates correctly under a range of conditions with minimal false activation.
  - Training of staff 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 duress alarm system is expected to have sufficient redundancy and be of high availability to achieve 100% continuous operation. Downtime procedures must be in place, including uninterrupted power supply (UPS) for a period suitable for the risk, for instances where the system does shutdown.

**Duress Alarms:**

**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.
- Mobile duress alarms worn by staff within the NSW Health Agency.
- Mobile duress alarms worn by staff who regularly work outside the NSW Health Agency, i.e. community health staff.

Note that irrespective of a risk assessment, all staff required to work in an Emergency Department must have (and wear) a mobile duress alarm while on duty.

- Fixed alarms may be used in well defined areas where:
  - The person works from a static position (e.g. where staff are behind a screen such as a pharmacy distribution window or behind a counter).
  - The alarm can be discretely activated without the staff member leaving their normal working position.
  - As a back-up system to a mobile duress alarm system.
- Fixed alarms may not be appropriate for areas accessible to patients and the public (e.g. corridors), as tampering with alarms may occur.
- Mobile duress alarms are used where the staff member is moving around in the course of their work and where there is a risk of being confronted by aggressive behaviour. Mobile duress alarms must be worn attached to a strong and stable part of the wearer’s clothing (e.g. clipped to a trouser pocket or waistband). They must not be worn around the neck. It must be noted that some types of alarms cannot be covered by clothing as they rely on infra-red frequencies for communication. If this is the case the design of the uniform and how the staff member will wear the alarm must be considered.
- Mobile duress alarms for use within a facility and the immediate area must comply with all relevant Australian and regulatory requirements.
- The alarm system solution should consider the operation practices of the entire campus to ensure it is operationally sound, efficient and seamless.

Features specific to Mobile Duress Alarms
Mobile duress systems have a unique identifier that is transmitted when an alarm is raised. The quantity of alarm devices must be sufficient to cater for the largest shift plus allowances for visitors to the unit, units being charged and spare units.

All mobile duress alarm units must have the following physical features:
- Provide activation that can be initiated by the wearer and activated where the user is not moving or is falling down. These must not be able to be disabled by individual staff members.
- 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.
- A ratio between unit cost and life expectancy of the device before failure is to be such that it makes the device cost effective.
- Be able to be affixed to clothing, and not be worn around the neck. Where the alarm will be affixed to clothing also influences the type of communication systems, e.g. some types of signals cannot be transmitted through clothing should staff affix the alarm on a waist band under clothing.
- Include a “warning indication” if the user is out of range, communications or battery failure.
- Provide accurate information on the location of the activated alarm to within five (5) metres inside health care facility and to within ten (10) metres outside of
health care facility so that the person can be found without delay on commencing a search in the area.

- In high risk areas room-by-room location finding accuracy should be provided.

Features of both Mobile and Fixed Duress Alarms
- Be able to interface with other local communication and security systems (e.g. paging systems and CCTV 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 (e.g. 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 (e.g. staff leave or join, without needing to install a new range or design of equipment).
- Be capable of transmitting a duress signal within five (5) seconds of activation with a reliability factor of no less than 98% for both indoor and outdoor situations.
- Be guaranteed by the supplier of the duress system (i.e. all equipment and systems will be supported for a period of no less than five (5) years from the date of service and the supplier needs to provide “urgent and routine” servicing and replacement of all parts during that period).
- Be user friendly and simple to use.

Mobile 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 within ten (10) seconds from activation in the form of a unique tone, identification of the activating alarms, time stamp and text/visualisation of the location.
- Alert other staff in the work area/facility that a colleague requires assistance, to ensure that assistance is activated and to ensure that another staff member does not accidentally walk in on a duress situation thus putting themselves at risk

Mobile 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.

Testing
- Mobile 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 staff member is recognised by the system. Where manual testing has to occur, NSW Health Agencies should seek the advice of the supplier to set up a suitable testing protocol.
• Mobile duress systems must be self-testing and notify of any malfunction. If a fault is detected it must notify appropriate staff immediately via an independent system. 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. A specific testing regime must be documented eg testing occurs at least every 30 days.

• Testing records must be maintained and any faults reported and fixed as a priority. Staff 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.

Training and information

• Suppliers of any alarm system must, as part of any contract, provide training in an easy to understand manner for staff 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, e.g. low battery, impending person down alert.

• Arrangements must be made by the NSW Health Agency to ensure new staff are provided with instruction on the operation of the equipment.

A duress alarm is only the means of signalling that someone needs assistance. The response to that alarm is the important part of the incident management process (Refer to Chapter 29 of this Manual).

*******
12. Lighting

Policy:
NSW Health Agencies are required to ensure, in consultation with staff 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.

External lighting must be sufficient to eliminate dark areas, must allow facial recognition and must facilitate the correct functioning of CCTV cameras.

Standards:
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):

- External lighting systems use lighting appropriate to the area to be lit, such as LED floodlighting.
- External security lighting must be housed in vandal resistant containers and mounted to restrict tampering (e.g., 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 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.
- There must be a process for reporting malfunctioning lights.
- Malfunctioning lights must be replaced immediately.
- Security lights must be automatically activated and deactivated at pre-set times (times need to be seasonally adjusted) or at pre-set light levels.
- Security lights must be connected to an electrical circuit separate to that of the main facility and be connected to uninterruptible power supply (UPS).
- Some internal lighting must remain on during the night, after that workplace has been closed for the day and some internal lighting should be available via movement sensors after the workplace has been closed for the day.
- Lighting must be located and designed to ensure maximum benefit and coverage. Lights must be bright enough and provide sufficient light to ensure a safe entry to and safe exit from the workplace (including paths), allow facial recognition, and support the usefulness of any CCTV installed.
- Prior to installation of CCTV cameras, light levels at different times of day must be considered to ensure that CCTV camera provides a clear image at all times.
- Prior to installing or making changes to lighting, ensure that there will not be any adverse impact on CCTV camera performance.
- There must be appropriate lighting in car parks. Where the facility does not have dedicated on-site parking, consultation on street lighting should occur with local councils.
- Lighting must avoid the creation of dark spots and be sufficiently bright to deter crime 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), AS4485.1 and AS/NZS2890 as applicable.
- Areas requiring special lighting eg entrance foyers, emergency departments, staff entry and exit points, pharmacies and car parks must be identified and appropriate lighting installed.
- Exterior lighting must be connected to an uninterruptible power supply (UPS).
13. Workplace Camera Surveillance

Policy:
NSW Health Agencies are required, in consultation with staff, 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 CCTV 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 does not cover circumstances where the intended purpose of the camera surveillance is to provide surveillance of staff or patients.

NSW Health Agencies are required to ensure, in consultation with staff 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, used as part of a security risk management program.
- **Covert** camera surveillance, used to capture suspected unlawful activity.

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.

The following standards apply to overt camera surveillance and 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) and only where the standard does not reflect a legislative requirement.

Determining the need to introduce/add to overt camera surveillance /CCTV:
Regardless of the reasons for the installation, having a clearly displayed camera in an area can create an expectation from staff and others that a duress 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...
The primary purpose of the CCTV, and what they should do in the event of a threat, is clearly communicated to staff.

As camera surveillance is considered to be a risk control strategy that is toward the lower end of the hierarchy of risk controls, eg an administrative control, NSW Health Agencies must ensure that, as far as practicable, all other appropriate risk control strategies higher up the hierarchy are put in place to control security risks.

The decision to utilize CCTV, and the purpose for which it will be used as part of the security risk management program, must be determined through a risk assessment. 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.
- Cost of properly maintaining and supporting the CCTV, 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 staff 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.

Informed by the risk assessment the primary purpose/s of the camera surveillance must be established, documented and clearly communicated to staff eg crime deterrence and protection of assets, recording of evidence only, verifying identity of persons presenting at doors as part of the facility access controls, to provide a live feed into poorly visualised areas or spaces such as car parks and driveways or to actively identify incidents that are escalating so a response can be activated. 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.

As a minimum in Emergency Departments, regardless of the purpose of the camera surveillance, live feed should be available at staff stations ie all ED CCTV should feed into a monitor regardless of whether the footage requires continuous monitoring (eg main public access entry doors).

Where existing CCTV infrastructure has not been adequately assessed and implemented in line with the above standards, a documented risk assessment must be undertaken.
Notification Requirements

- Where CCTV is being installed, following a risk assessment, as a security measure, there must be agreement with staff (or a body representing a substantial number of staff at the particular workplace, eg a union) about the purpose of video surveillance and how it will be carried out. This requirement is set out in Section 14 of the Workplace Surveillance Act 2005.
- The CCTV must be used in accordance with that agreement and not for any other purpose. Staff must be advised of the presence of CCTV ie signs notifying people that they may be under surveillance.
- 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 CCTV.
- Video footage capturing staff at work must not be used for disciplinary/misconduct or performance matters unless the notification requirements set out in Section 10 of the Workplace Surveillance Act have occurred.

Monitoring and storage of camera surveillance images

- All CCTV images must be stored for a minimum of 21 days. Even where the CCTV images are continuously monitored, or based on a risk assessment, only monitored on an adhoc basis, these images must be recorded and stored for a minimum of 21 days, so that evidence is available in the event of an incident.
- Where CCTV is 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.
- However, where the continuous monitoring of CCTV in higher risk areas is not assessed as necessary the following alternative controls, as a minimum, must be implemented:
  - A fixed duress alarm or another mechanism for summoning assistance is installed within the vicinity of the CCTV (except where in a public corridor) and
  - A duress response is mobilised where the fixed duress alarm is activated and
  - Signage advising staff of the need to activate a duress alarm in the event of an incident is displayed in the vicinity of the CCTV and
  - Review of the effectiveness of the above strategies is undertaken, appropriate to the level of risk, to ensure risk and liability are being appropriately managed in a way that maintains the security of staff and others.
- Within an Emergency Department, CCTV not requiring continuous monitoring must be connected to monitors installed at staff stations to allow visibility into the area covered by the CCTV.
- Where practicable, CCTV should be connected to the duress alarm system. This would allow CCTV 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 and make an informed decision as to what type of response is required.
- CCTV must have the capacity to record and provide live feed in colour.

Placement of CCTV units

Where following a security risk assessment camera surveillance is required in a particular location, the risk assessment must also consider the effective placement of the CCTVs within this location.
The following applies when determining the placement of CCTV:
- Expert advice on the type and location of cameras must be sought. This could be provided by internal security staff or by external parties. Any placement of CCTV in a clinical area should be determined via a risk assessment involving relevant clinicians.
- Placement should focus on areas where there is a higher likelihood for incidents to occur and where the CCTV will have value as a deterrence.
- The location of CCTV must not encroach on patient privacy and confidentiality (i.e. no view of clinical procedures or physical examinations). CCTV must not be placed in any change room, toilet facility or shower or other bathing facility.
- Where CCTV is located within a seclusion room, for the purposes of ensuring safety of access, images must not be visible beyond staff supporting patients in the room.
- 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.
- Placement must eliminate concealment opportunities. Where the CCTV is being used as an access control strategy and 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, a second camera or a change of lens needs to be considered.
- Landscaping, including line of sight, type and growth rate of trees and vegetation must be assessed and the risk eliminated.
- Pedestrian and vehicular thoroughfares, including analysis of the amount of pedestrian and vehicular access throughout each day must occur.
- 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.
- The potential for the direction of the sun, including sunrise and sunset to cause ‘blooming’ 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 staff undertaking the maintenance.
- Possibility of accompanying lighting intruding upon the surrounding area
- Access to 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 down load images and security of the hard drive so it can not be tampered with eg unplugging.

Placement of monitors with consideration to right to privacy, confidentiality considerations – to include placement of main monitor in a position so as to discourage inappropriate viewing or monitoring of staff, patients and visitors.
- As far as is possible, CCTV must be placed at a position that allows for full facial recognition.
• Review of the placement of CCTV must occur to ensure it remains appropriately placed, and continues to be pointed in the necessary direction.
• A maintenance log must be kept.

**Use and disclosure of CCTV records**

The *Workplace Surveillance Act 2005* 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 (e.g. 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.

Only where the notification requirements set out in Section 10 of the *Workplace Surveillance Act 2005* have occurred can video footage be used for disciplinary/misconduct or performance matters.

While NSW Health Agencies are not obliged by law to provide surveillance records without a warrant, Section 316 of the *Crimes Act 1900* 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 should assess requests for surveillance records, in the absence of a warrant, on a case by case basis. In deciding whether to provide surveillance records, in situations other than those covered by Section 316 of the *Crimes Act 1900*, NSW Health Agencies need to balance this need with the obligations in the *Health Records and Information Privacy Act 2002* regarding confidentiality of patients and the often sensitive nature of health information.

Factors that must be considered prior to disclosing surveillance records without a warrant include:
- The seriousness of the alleged offence.
- The degree of evidence available that suggests the surveillance record contains information that will assist with law enforcement.
- How well sign posted the camera surveillance is, i.e. will staff and visitors to the area have a reasonable expectation that they will be captured in surveillance records?
- Any local arrangements with staff representatives, as the surveillance records may also include footage of staff.

- The CCTV footage must not be publicly available and monitors displaying CCTV images must not be viewable by the public.
- NSW Health Agencies must implement clear protocols for determining, in each instance, whether such 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. Procedures must be in place that require the logging of when, where and why stored footage was accessed.
- Password protection of recorded footage is required. Downloading access must be restricted to those staff who have been identified within the NSW Health Agency as having the authority to have this access. All CCTV 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 CCTV records downloaded and utilised. These Authorities can be found at:


Covert camera surveillance:
- The approval of the Secretary of NSW Health must be sought prior to the application 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 Workplace Surveillance Act 2005 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/violence occurring, the size of the facility, the services being provided and the local 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 at Appendix 1 to this Chapter.

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

Standards:

1. Licence Requirements

All security staff, including health and security assistants, must have a current 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, i.e. annual verification that a security staff member continues to hold a valid security licence.

Security staff undertaking security audits within NSW Health are not required to possess a Class 2A Security Consultant licence.

2. Determining the appropriate level of security staffing:

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

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 with managing this risk and the time required for security staff to undertake their other duties, and then
determine the level of security staffing and the rostering required to address these issues.

Determining the current and potential risk of violence and aggression must take into consideration the following:

- The type of services being delivered at the facility and the identified risk of aggression or violent incidents occurring (e.g., emergency departments, alcohol and other drug/mental health units or community services working with domestic violence victims 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 (e.g., large festivals or events);
- The number of all staff on duty at any one time and their experience and skill levels;
- 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;
- 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, e.g., 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 (e.g., patient risk assessment processes, access control measures).

It is critical that managers and staff, including security and clinical staff, decide on and document, through the development of local procedures, the way security staff will undertake the role in that NSW Health Agency, to the extent set out in this Chapter, and how violence-related incidents will be managed.

To assist with differentiating the roles of security staff, paramedics, and the police, where individuals are transported to NSW Health Agencies or between NSW Health facilities, reference should be made to the Mental Health Emergency Response Memorandums of Understanding between the NSW Ministry of Health, the Ambulance Service of NSW and NSW Police Force, and other relevant NSW Health Policy Directives, found at: www.health.nsw.gov.au/policies/index.html

The required level of security staffing may be achieved through employment of security staff or health and security assistants, the creation and utilisation of casual pools of security staff or the engagement of contractors or on-call patrols, or a combination of these arrangements.

Where a NSW Health Agency utilises contract security staff, it must ensure that specific risk arising from this arrangement (i.e., ensuring competence, 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.) and 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 *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 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 other workers at the conclusion of the engagement as part of the continuous improvement process.

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

### 3. Background

- 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 staff, to assist with managing patients, provide assistance to visitors, and assist with protecting staff and securing the assets of the facility.

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

- NSW Health Agencies must ensure that security staff understand their role clearly, including the boundaries between their role and that of the Police. 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 staff, must contact the Police if there is suspected criminal activity or concerns about public safety in or around a NSW Health Agency.
• Security staff must not place themselves at unnecessary risk in carrying out their duties. In practice, there may be times when the duty of care to patients or others may require intervention but **at no time** should the duty of care override a staff member’s right to safety.

• Security staff, including contractors, must be provided with suitable induction information and training consistent with the requirements outlined in PD2012_008 *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.

• Appropriate and on-going supervision of security staff, including contractors, must occur. This will ensure that support can be provided to security staff, training issues can be identified and standards reinforced.

• 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.

Attached to this Chapter (at Appendix 14.1) is a summary of information on the scope of duties that may be undertaken by security staff in NSW Health Agency. However, following are some key areas of this role that require further explanation.

### 4. Physically (Manually) Restraining Patients and Others

• Prior to the use of physical restraint, all other prevention strategies must be attempted including:
  - early identification of escalating behaviour; and
  - 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.

• 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 violence risk assessments, as part of a multidisciplinary team approach to the care of patients.

#### 4.1 Using physical restraint on a medical practitioner’s directive (non-capacity patients)

• Except in certain specified emergency situations, as outlined in the section below, a decision to use physical restraint on a patient, who is **not** being cared for under the Mental Health Act 2007 **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 damage 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 Guardianship Act 1987 and this patient is referred to as a non-capacity patient in this Chapter.

4.2 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 Mental Health Act 2007.

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

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

• The physical restraint of a patient must occur at and 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
  - Clinical staff are unable to issue instructions (e.g. they are injured or incapacitated).

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

• At all times, all staff 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, i.e. 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.

• 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 Security Industry legislation and the NSW Health Incident Management Policy.
• Security staff are responsible for ensuring that their actions involve only the use of reasonable force.

• Local procedures on the use of physical restraint must be developed and must address:
  - When physical restraint will be used;
  - How it will be applied safely, including risk associated with prone restraint techniques;
  - The need for a multidisciplinary team approach to restraint;
  - Protocols for managing the person during the physical restraint episode;
  - The respective roles and responsibilities of staff, including which clinician will take the lead role during the restraint;
  - Escalation procedure which identifies the staff member responsible for making the decision to escalate; and
  - Requirements for post incident investigations and operational debriefings to consider information provided by all staff involved in the incident.

• 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 staff 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.


4.4 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.
• At all times, all staff 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 i.e. 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.

• Where security staff are involved in using physical restraint on a person this must be recorded after the incident.

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

• Local procedures on the use of physical restraint must be developed and must address:
  - When physical restraint will be used.
  - How it will be applied safely, including the risks involved in prone restraint.
  - The need for a multidisciplinary team approach to restraint.
  - Protocols for managing the person during the physical restraint episode.
  - The respective roles and responsibilities of staff, including which clinician will take the lead role during the restraint.
  - Escalation procedure which identifies the staff member responsible for making the decision to escalate; and
  - Requirements for post incident investigations and operational debriefings to consider information provided by all staff involved in the incident.

• 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 staff 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 person’s 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.

5. Using mechanical restraint on patients

• Mechanical restraints must only be used on patients as a last resort. 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.

- The following NSW Health Policy Directives provide further standards relating to the use of mechanical restraints, including obligations and documentation requirements:
  - PD2015_004 Principles for the Safe Management of Disturbed and/or Aggressive Behaviour and the Use of Restraint and
  - PD2012_035 Aggression Seclusion and Restraint: Preventing, Minimising and Managing Disturbed Behaviour in Mental Health Facilities
  - GL2015_007 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. This will assist in ensuring staff have experience in its correct use. In any event, the equipment used must be reviewed and approved for use by the relevant NSW Health Agencies clinical governance committee(s) and specific procedures must guide their use. Staff must be provided with specific training and refresher training in the procedures for use of the equipment.

- Features of appropriate mechanical restraints include:
  - 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.


- Wherever possible staff should take evasive action to escape from a violent situation, including removing themselves, other staff, 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 Crimes Act, Section 52 of the 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 his or herself, 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.

- Local procedures must include provisions and instruction that the following will need to occur where force by a staff member, including restraint has been used:
  - A procedural debriefing involving all the staff involved in the incident must be carried out as soon as practicable following the incident;
  - Requirements for post incident investigations and operational debriefings to consider information provided by all staff involved in the incident
  - The incident must be reported and managed in accordance with the relevant NSW Health policies; and

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

- Section 100 of the Guardianship Act 1987 (NSW), 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 damage 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.

- The 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 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 damage to the patient.

8. 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 Law Enforcement (Powers and Responsibilities) Act 2002 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 staff 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).

9. Detaining Patients under the Mental Health Act 2007

- Division 2 of Part 2 of the Mental Health Act 2007 (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 staff (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.
10. **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 the section 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 should 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 Mental Health Act, a patient must not be prevented from leaving a NSW Health Agency by security staff.
   - Where a patient needs clinical observation (e.g., specialising) it is not appropriate for security alone to be doing this. Security staff are not trained (nor do they have a duty) to recognise patients whose physical or mental health condition is deteriorating. It would be appropriate for security to observe a patient if the purpose of the observation is to prevent absconding or to assist with managing aggression, however this would also need to occur under the direction of the clinician.
   - 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, Juvenile Justice, Immigration or Police patients in their custody must not be retrieved by security staff. This is the role of the relevant Agency.

11. **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 staff or others and eliminate or minimise these risks as far as is practicable.

12. **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 (referred to also as Code Black teams, Emergency Response team or Clinical Aggression Response teams), to assist staff and others who are at risk. Chapter 29 of this Manual provides standards for the identification, training and implementation of Code Black teams.

13. Searching Patients and Visitors and their property

• To ensure the security of staff, 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 is undertaken with respect 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 and requires the consent of the individual.

• Security staff must not attempt to search a person without their consent, except in the limited circumstances outlined in the section 13 below titled ‘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 Inclosed Lands Protection Act 1901 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. These conditions may include the following:
  - Prohibited weapons, illegal drugs or alcohol are not to be brought into the facility.
  - The NSW Health Agency reserves the right to search persons if there is a reasonable suspicion that a person has brought such weapons or drugs into the facility (note: searching in these circumstances still requires the consent of the person).
  - A person who refuses to be searched when requested will be asked to leave the premises or the Police may be called.

• Where, after a risk assessment, a NSW Health Agency determines the need for procedures to deal with searching for weapons and other dangerous objects 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 about:
  - How to maintain personal safety.
  - What to do where there is a suspicion that an individual is carrying a concealed weapon.
  - When and how searches may be conducted.
  - How to ensure consent.
  - Issues to be considered before conducting a search such as whether Police involvement may be more appropriate.

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

• 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 staff anything they want to bring into a clinical area.

14. Searching mental health patients
• The situation is somewhat different in relation to mental health patients under the Mental Health Act 2007.

• 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 can conduct a frisk/pat down search of a mental health patient. 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 such a search must be conducted by more than one person, who should both be of the same gender as the patient.

• Where the Police or paramedics bring a patient who has been detained under the Mental Health Act into a NSW Health Agency it must be established if a thorough search has already occurred. NSW Health Agency staff, including security staff, may request that an initial or another search of the patient is performed by the Police or paramedic.

• Any staff, 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.

15. Accompanying patients being treated under the Mental Health Act and who are being transported between 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 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 Mental Health Act 2007 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 escape.

• The following NSW Health documents provide further standards relating to the transport of patients:
  - Memorandum of Understanding: Mental Health Emergency Response (July 2007)
  - Mental Health for Emergency Departments: A Reference Guide
  - GL2015_007 Management of Patients with Acute Severe Behavioural Disturbance in Emergency Departments.

16. 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 should 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 staff member may exercise judgement and action to escort a person, under the powers provided by the Inclosed Lands Protection Act 1901.

• A Chief Executive, through an instrument of authority/delegation, can authorise individual NSW Health staff members to exercise judgement and action to escort individuals from NSW Health premises.

• 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 staff must have undertaken:
  - De-escalation and restraint techniques training; and
  - 3 day program Security in a Health Environment (if they are a security staff member).
• The authorised staff member can not be directed to take this action if the authorised staff member does not deem the situation safe or necessary.

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

17. Retention and Restoration of Weapons or Implements
• On occasion people may present to a NSW Health Agency carrying weapons or implements 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 weapons or implements, and the discovery of the weapon may only arise once the person has been admitted as a patient.

• Weapons and implements 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 staff, patients or others.

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

• When developing these procedures, the following risk control strategies must be considered:
  - People who hand over custody of a weapon or implement to NSW Health Agency staff must, where practicable, be given a receipt for their property.
  - All weapons and implements must be placed in a plastic bag, to protect any forensic evidence, in case it is later found that the weapon or implement has been used in a crime. Staff handling weapons and implements must wear gloves.
  - Where there are any concerns that the weapon or implement may fall into the category of a prohibited weapon, as defined by the Prohibited Weapons Act 1998, or carrying the weapon is against the law (e.g. 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 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 section below on Storage and Disposal of Weapons).

- Under section 79 of the Firearms Act 1996 (NSW), 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 Weapons Prohibition Act and Section 79 of the Firearms Act 1996, provide protection from civil or criminal liability, including breach of confidentiality when a clinician discloses information to the NSW police. Security staff must inform clinical staff 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.

18. 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 *Evidence Act 1995*.

- 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 GL2013_002 Firearms Security.

  - 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 staff member 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.
Appendix 14.1

Scope of Duties
Security Staff (including Health and Security Assistants):

1. The role security staff undertake in NSW Health Agencies can include:
   - Responding to security alarms and fire alarms.
   - Securing a physical area in a NSW Health facility to protect staff, patients or visitors, in response to a real or immediate threat.
   - Escorting staff to vehicles.
   - Maintaining order in crowded areas such as emergency departments, methadone clinics and at helipads.
   - Assisting with emergency evacuations.
   - Participating as a team member in a response to a ‘Code Black’ alarm.
   - Providing customer services including information and advice to visitors.
   - Internal and external patrolling, to ensure security is maintained and to provide a visible presence.
   - Maintaining parking control.
   - Reporting security related incidents.
   - Providing input into security issues and audits.
   - Receiving, receipting and recording lost items of value and weapons, and reporting to police as appropriate.
   - Monitoring CCTV.
   - Maintaining key control processes.
   - Operating access control systems, including locking/unlocking buildings or rooms.
   - Operating or managing staff identification processes where necessary.

2. Additionally, the role security staff undertake in a NSW Health Agency can include, as an option of last resort:
   - Restraining physically (that is, holding the person temporarily), by a reasonable amount of force, a patient or visitor who has assaulted the security staff, other staff, another patient or another visitor and who is (in the reasonable opinion of the security staff in attendance) likely to continue to assault and where the security staff believe the restraint is necessary to defend themselves or another, and report to Police as appropriate.
   - Restraining physically (that is, holding the person temporarily), by a reasonable amount of force, a patient or visitor who (in the reasonable opinion of the security staff in attendance) is threatening to imminently assault the security staff, other staff, another patient or a visitor, and where the security staff believe the restraint is necessary to defend themselves or another, and report to Police as appropriate.
   - Restraining physically (that is, holding the person temporarily), by a reasonable amount of force, a patient or visitor who has destroyed or damaged significant property of the NSW Health Agency and who is (in the reasonable opinion of the security staff in attendance) likely to continue to destroy or damage the property, and where the security staff believe the restraint is necessary, and report to Police as appropriate.
   - Restraining physically (that is, holding the person temporarily), by a reasonable amount of force, a patient or visitor who is (in the reasonable opinion of the security
staff in attendance) threatening to imminently destroy or damage significant property of the NSW Health Agency, and where the security staff believe the restraint is necessary, and report to Police as appropriate.

- Restraining physically (that is, holding the person temporarily), by a reasonable amount of force, a patient after a medical practitioner has informed the security staff in attendance that the patient is incapable (either temporarily or permanently) of giving consent and the medical practitioner directs that the patient be restrained for the purposes of the medical practitioner carrying out urgent and necessary medical treatment to save the life of the patient or to prevent serious damage to the patient (referred to in this document as a non-capacity patient).

Security staff may also assist other staff in carrying out these additional tasks.

For force to be reasonable, the actions must be a reasonable response in the circumstance and there must be some reasonable proportion between the circumstances involved and the response to it.

The role security staff undertake in NSW Health Agencies, in relation to involuntary mental health patients, is set out in Section 4 of this Appendix.

3. Activities outside of the scope of duties

It is NOT the role of NSW Health security staff to:

- Arrest people suspected of engaging in criminal activity, or at the direction of another person.
- Detain (ie stop from leaving) or forcibly retrieve individuals except in circumstances involving an involuntary mental health patient or a non-capacity patient.
- Restrain a patient so as to assist in the provision of medical treatment, except in circumstances involving an involuntary mental health patient or a non-capacity patient.
- Detain (ie stop from leaving) a child who is the subject of an Assumption of Care Order, where the parents or carer attempt to remove that child.
- Search individuals without their consent except in circumstances relating to involuntary mental health patients (refer to clause 4)
- Remove individuals from NSW Health premises, except in the limited circumstances set out in Section 16 of this Chapter.
- Manage high risk incidents such as those involving prohibited weapons or hostage situations.

Security staff, like other NSW Health staff, must contact the Police if there is suspected criminal activity on or around a NSW Health premises.
4. Role in relation to involuntary patients covered by the *Mental Health Act 2007*

In responding to incidents relating to involuntary patients detained under the Mental Health Act 2007, security staff are required to follow the direction of a registered health professional in the management of disturbed or violent behaviour.

Security staff may provide assistance, in relation to involuntary patients, in accordance with NSW Health policies, to:

- Restrain a patient (including applying mechanical restraint).
- Prevent a patient from leaving a facility in unauthorised circumstances.
- Retrieve a patient who attempts to leave the facility in unauthorised circumstances. If the patient has left NSW Health property the Police must be called.
- Accompany non sedated mental health patients when they are being transferred between facilities, where the patient has been assessed by the treating registered health practitioner to be co-operative, a low risk to safety and does not require active monitoring or medical care during the transfer.
- Frisk/pat down search a patient.

Policy:
NSW Health Agencies are required to ensure, in consultation with staff and other duty holders, that all reasonably foreseeable security risks associated with the Emergency Department (ED) environment are identified, assessed, eliminated where reasonably practicable, or where they can not be eliminated, effectively minimised.

NSW Health Agencies must have in place a process for staff to communicate to colleagues the risks presented by a patient.

NSW Health Agencies must ensure that the process is appropriately documented.

NSW Health Agencies must ensure that they comply, as far as practicable, with the Australasian Health Facility Guidelines, 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.

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).

NSW Health Agencies must develop procedures, in consultation with staff and other duty holders, to effectively manage security risks in ED. Procedures and physical design/layout must reflect the specific risks identified for that ED environment. Clinical protocols must be developed, to identify the risk of and manage potential or actual violence arising from a patient’s medical or mental health condition.

Main public entry access doors and use of CCTV
- Main public entry access doors must be able to be locked/unlocked remotely, that includes from a location that is within the line of site of the door.
- Main public entry access doors must be fitted with CCTV, particularly for after hours access or for circumstances where the doors are remotely locked (refer to Chapter 9 and Chapter 13 of this Manual).
- The CCTV must provide a clear picture at all times of the day and night. Both CCTV placement and the monitor size must allow visual surveillance of the area around the access doors. Monitors must be located near remote door latching/unlatching points and linked to digital/video door phone/communication device.
• The ED risk assessment must consider the use of CCTV and the purpose for that CCTV (refer to Chapter on Camera Surveillance)
• As a minimum, waiting rooms must have CCTV which both records and provides a live view into the waiting rooms. CCTV placement in waiting rooms must eliminate opportunities for the concealment of individuals to prevent unauthorised access to treatment areas eg tailgating.
• CCTV and monitors must be of sufficient quality to allow a clear visual image on individuals at all times of day and night.
• As a minimum in Emergency Departments, regardless of the purpose of the camera surveillance, live feed must be available at staff stations ie all ED CCTV should feed into a monitor regardless of whether the footage requires continuous monitoring (eg main public access entry doors).
• Placement of CCTV and monitors must take privacy issues into account. Signage notifying of CCTV must be displayed in line with the requirements set out in the Workplace Surveillance Act 2005

**Protecting People and Property: NSW Health Policy and Standards for Security Risk Management in NSW Health Agencies.**

**Waiting areas – Physical design**

Waiting areas must:

• Be comfortable, decorated in muted colours and be free of unnecessary clutter.
• Have a clear path to commonly used amenities (eg phones, water and vending machines, toilets etc).
• Have adequate lighting, seating, ventilation and temperature control
• Have signage that clearly directs patients and carers to the reception area, triage and the waiting area. Refer to:
• Be fitted with furnishings that cannot be moved and/or used to cause injury eg linked rows of seating.
• Have controlled access to clinical areas eg doors are locked and access controlled from reception/triage or other treatment areas.

**Communicating with patients (and carers) awaiting care**

Ensuring appropriate on-going communication with those waiting for care is important as a strategy in reducing the potential for escalating behaviour.

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 and
• Regular advice on changed waiting times including where wait times increase due to high volume.

Further standards are set out in the *NSW Health policy for Emergency Patients Awaiting Care.*

**Triage areas, interview rooms, write-up areas and staff stations**

• Ensure that the design does not create entrapment or concealment points. These spaces should have the following characteristics:
- An appropriate barrier where there is a requirement for protection from violence, security of property or records, or privacy of clinical discussions.
- Two exit points.
- Layout should prevent the position of the patient and furniture/equipment from blocking staff members access to an exit route.
- Speed of access/egress.

The rooms must have two doors with the room layout being such that the patient cannot obstruct or intercept staff access to an escape route or safe area. If doors need to be locked, then doors should be on swipe card locks so as to facilitate rapid exit.

- Must include duress alarms – fixed and/or mobile alarms, as appropriate. Fixed duress alarms must be positioned to allow easy access by staff.
- Must include safety glass in any windows with integrated blinds so staff can be seen while retaining client privacy.
- Must not be in isolated areas, but close to and in view of other staff ie 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.
- The Australasian Health Facility Guidelines must be referenced for any additional or new standards.

**Treatment rooms – Physical design**

Every room, eg write-up areas, family rooms and examination/consultation/procedures rooms, must have the following characteristics:

- Two exit points and be free from entrapment risks with the room layout being such that the patient cannot obstruct or intercept staff access to an escape route or safe area. If doors need to be locked, then doors must be on swipe card locks so as to facilitate rapid exit.
- Layout that allows the clinician to face the patient at all times, including positioning the desk, computer and telephone so that the clinician does not turn their back to the patient to use the computer or other equipment. Consideration should be given to computers on wheels.
- Fixed duress alarms (to supplement mobile duress alarms not as an alternative to individual mobile duress alarms).
- Be free of equipment laying in view and unsecured that may be used to cause injury.
- Windows and glass doors are constructed to be resistant to physical force ie used lamination, shatterproof film of security screens.
- Include dimensions that reflect NSW Health standards.
- Not be used for a purpose other than what it is designated for, including adding having multiple patients in a room designed for one patient.

**Open clinical treatment areas – physical design**

Treatment areas (other than rooms) must have the following characteristics:

- Ensure layout does not create entrapment or concealment risks. There must be line of sight from staff stations into all areas of the open plan clinical areas.
- Layout that allows the clinician to face the patient at all times, including positioning the desk, computer and telephone so that the clinician does not turn their back to the patient to use the computer or other equipment. Consideration should be given to computers on wheels.
- Separation between adult and paediatric beds and amenities (refer to *NSW Health policy on Children and Adolescents: Safety and Security in Acute Health Settings*).
- A separate safe area for the assessment and management of patients with acute severe behavioural disturbances (refer to *NSW Health policy on Safe Assessment Rooms and NSW Health guidelines on the Management of Patients with Acute Severe Behavioural Disturbance (ASBD) in Emergency Departments*).
- Lockable storage for equipment. Local practices must involve the collection of all cutlery (metal and plastic) and sharps used in the treatment area immediately after use, or put in a safe area if it is not to be immediately removed from the workplace.

**Staff only areas**
Staff-only areas such as meal rooms, tutorial rooms, offices and staff toilet and locker rooms must have the following characteristic:
- Have signage to clearly identify these areas as staff only areas.
- Be access controlled to ensure they are secured from patient access areas.
- Be fitted with fixed duress alarms.

**Clinical areas for safe assessment of patients with Acute Severe Behavioural Disturbance (ASBD)**
Dedicated clinical areas in an ED (eg safe assessment rooms) must be available to provide a safe area for the assessment and management of patients in the ED with ASBD.

Clinical practices consistent with NSW Health policy must be in place to manage patients with ASBD (refer to NSW Health policy on Safe Assessment Rooms and NSW Health guidelines on the Management of Patients with Acute Severe Behavioural Disturbance (ASBD) in Emergency Departments).

These clinical spaces must be designed in consultation with staff, including mental health staff.

Refer to Health Infrastructure *Guideline for the design of Safe Assessment Rooms/Areas.*

**Managing Patients who may have or may develop ASBD**
Appropriate protocols must be implemented for admission, assessment ongoing management and transfer of patients aimed at:
- Triage assignment that takes account of observed ASBD or the potential for ASBD to develop
- Identifying the deteriorating behaviour of a patient.
- Assessing any relevant risk information from services transferring or transporting patients into the ED
- The provision of information to services receiving a patient from ED.
- Recording all incidents involving a patient’s behaviour in the medical record (eg file flagging) and in the incident management system and the development of and documenting of an appropriate patient management plan to address the noted behaviour.
- Communication of risks relating to patients to colleagues, on an on-going basis, and during shift changeover safety huddles. Practices must also take account of the need to communicate risks to staff rotating into the ED who may not have immediate knowledge of any patient related risks.
- Establishing local protocol committees with Agencies eg NSW Police, as required under the Memorandum of Understanding.

**Clinical protocols to prevent and manage violence**
- Ensure clinical protocols are in place that:
  - 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).
- Identify the risk of violence arising from a clinical condition and provide adequate and appropriate clinical management, e.g. early diagnosis and treatment of delirium, identification and treatment of drug, alcohol or tobacco dependency.
- Incorporate on-going risk assessment, and management of behavioural issues of patients.
- Provide for communicating with and monitoring waiting patients and waiting family members eg information on delays in procedures and timing.
- Seek and assess any relevant risk information from services transferring a patient (e.g. nursing homes, NGOs, Corrective Services, GPs, private hospitals)
- Provide information to services receiving the transferred patient.

- Report, document and analyse violent incidents (including duress response and its outcomes) from clinical, security and WHS perspectives.
- Conduct operational debriefings after an incident to ensure protocols were followed, equipment worked properly and that these were adequate to manage the event.
- Establish a well designed, appropriately staffed, secure therapeutic environment which is compatible with clinical care objectives.
- Develop procedures for limiting the number of patient support people/visitors in treatment areas.
- Implement a patient alert system (For further information refer to the NSW Health Policy Zero Tolerance Approach: Responding to Violence in the NSW Health Workplace).
- Develop communication strategies for ensuring that patients and visitors are aware of their behavioural responsibilities and the consequences of not meeting those responsibilities.

Security staff (refer to chapter 14 for further more detailed standards)
- Security staff fulfil a role that has a strong emphasis on assisting with the early identification, prevention and management of incidents.
- 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).
  - Manage high risk incidents such as those involving weapons or hostage situations.

Chapter 14 of this Manual sets out in further detail the role NSW Health security staff can (and cannot) be expected to undertake in clinical areas in all NSW Health Agencies.

Using Physical restraint

NSW Health standards on the use of physical restraint are set out in the following documents:

- Policy Directive PD2015_004 Principles for the Safe Management of Disturbed and/or Aggressive Behaviour and the Use of Restraint and NSW Health
- Policy Directive PD2012_035 Aggression Seclusion and Restraint: Preventing, Minimising and Managing Disturbed Behaviour in Mental Health Facilities
Other references:
Australasian College for Emergency Medicine Design Guideline that can be found at: 
15. Security in the Clinical Environment: Part B Other Clinical Areas

Policy:
NSW Health Agencies are required to ensure, in consultation with staff 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 cannot be eliminated, effectively minimised.

NSW Health Agencies must have in place a process for staff to communicate to colleagues the risks presented by a patient.

NSW Health Agencies must ensure that the process is appropriately documented.

NSW Health Agencies must ensure that they comply, as far as practicable, with the Australasian Health Facility Guidelines, especially Parts B and C, which deal with security features in specific clinical environments.

Note: For issues relating to staff working in community settings refer to Chapter 16 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).

NSW Health Agencies must develop procedures, in consultation with staff and other duty holders, to effectively manage security risks in every clinical area (for emergency departments refer to Part A of this Chapter). Procedures and physical design/layout must reflect the specific risks identified for the clinical environment. Clinical protocols must be developed, to identify the risk of and manage potential or actual violence arising from a patient's medical or mental health condition.

All clinical environments (for EDs refer to Part A of this Chapter)

Physical design of key clinical areas (refer to Chapter 4 for further standards)

Desks, counters and screens:
- The design of desks, counters and screens must be determined by:
  - Their purpose.
  - The identified risk of violence.
  - The required security of records and information held in the area.
• The confidentiality of the discussions that take place.
• The requirement for a staff member to be able to face a patient at all times.
• The equipment being used.
• Whether the desk is always staffed.
• The availability of escape routes.
• Access to mobile and fixed duress alarms to summon assistance.

Interview rooms, write-up areas, staff stations and examination/consultation areas:
• Ensure that the design does not create entrapment or concealment points. These spaces should have the following characteristics:
  - An appropriate barrier where there is a requirement for protection from violence, security of property or records, or privacy of clinical discussions.
  - Two exit points.
  - Layout must prevent the position of the patient and furniture/equipment from blocking staff members access to an exit route.
  - Speed of access/egress.
• The rooms must have two doors with the room layout being such that the patient cannot obstruct or intercept staff access to an escape route or safe area. If doors need to be locked, then doors should be on swipe card locks so as to facilitate rapid exit.
• Layout that allows the clinician to face the patient at all times, including positioning the desk, computer and telephone so that the clinician does not turn their back to the patient to use the computer or other equipment. Consideration should be given to computers on wheels.
• Must include duress alarms – fixed and/or mobile alarms, as appropriate. Fixed duress alarms must be positioned to allow easy access by staff.
• Must include safety glass in any windows with integrated blinds so staff can be seen while retaining client privacy.
• Must not be in isolated areas, but close to and in view of other staff ie 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.
• The Australasian Health Facility Guidelines must be referenced for any additional or new standards.
• Waiting areas and common spaces, particularly in mental health units, must be sufficiently sized to give people ‘space’ and avoid the stress of overcrowding and be monitored by CCTV.

Meal rooms, offices and toilets
• Staff-only areas such as meal rooms, tutorial rooms, offices and staff toilet and locker rooms must be secure and separate from patient/public access areas.
• Staff while in these areas must be able to summon assistance in the event of a threat arising from unauthorised access to these areas.
• Staff only areas must be clearly signposted.

Access and egress control (Refer to Chapter 9 further standards)
• Clinical areas and staff only areas must be appropriately signposted and secured to ensure ease of access and 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 (e.g. ICU, MHU, Maternity and Paediatric Units), internal access points such as unit entrances, waiting areas, car parks, and potentially high risk areas, e.g. where cash or pharmaceuticals are handled.
• Intercoms at entrances (internal and external)
• Access control to the facility and units (e.g. ICUs, paediatric units, geriatric units)
• Consider how cameras are positioned, e.g. 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.

**Duress alarms (refer to Chapter 11 for further standards)**
• Staff must be provided with appropriate duress alarms as determined by documented risk assessment and consultation. See Chapter 11 for further standards.
• Where personal duress alarms are provided, staff must wear them in accordance with local procedures. Staff must wear mobile duress alarms where they are required to answer public access doors after hours eg maternity units.

**Clinical protocols to prevent and manage violence—**
• Ensure clinical protocols are in place that:
  • 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).
  • Identify the risk of violence arising from a clinical condition and provide adequate and appropriate clinical management, e.g. early diagnosis and treatment of delirium, identification and treatment of drug, alcohol or tobacco dependency.
  • Incorporate on-going risk assessment, and management of behavioural issues of patients.
  • Provide for communicating with and monitoring waiting patients and waiting family members eg information on delays in procedures and timing.
  • Seek and assess any relevant risk information from services transferring a patient (e.g. nursing homes, NGOs, Corrective Services, GPs, private hospitals)
  • Provide information to services receiving the transferred patient.
• Report, document and analyse violent incidents (including duress response and its outcomes) from clinical, security and WHS perspectives.
• Conduct operational debriefings after an incident to ensure protocols were followed, equipment worked properly and that these were adequate to manage the event.
• Establish a well designed, appropriately staffed, secure therapeutic environment which is compatible with clinical care objectives.
• Develop procedures for limiting the number of patient support people/visitors in treatment areas.
• Implement a patient alert system (For further information refer to the NSW Health Policy *Zero Tolerance Approach: Responding to Violence in the NSW Health Workplace*).
• Develop communication strategies for ensuring that patients and visitors are aware of their behavioural responsibilities and the consequences of not meeting those responsibilities, e.g. prominent signage, patient and visitor information brochures.

**Responding to Needs of People with Disability during Hospitalisation**
• Developing a plan for disability support while in hospital should be part of pre-admission planning for a person with a disability

• Staff must communicate with the carer, family, guardian, and / or disability support staff, 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 staff eg.
due to fear, anxiety, absconding, challenging behaviours, difficulties with communication.

- Where the patient has a known intellectual disability, the presence of a known person 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.

- Non-planned admissions for a person with disability through the Emergency Department or through direct admission must have a Transfer of Care Risk Assessment completed on the inpatient ward within the first 24 hours of admission.

**Managing Patients who may have or may develop Acute Severe Behavioural Disturbance (ASBD)**

Appropriate protocols must be implemented for assessment and ongoing management of patients aimed at:

- Identifying the deteriorating behaviour of a patient.
- The provision of information to services receiving a patient from ED or from another service.
- Recording all incidents involving a patient’s behaviour in the medical record (e.g., file flagging) and in the incident management system and the development of and documenting of an appropriate patient management plan to address the noted behaviour.
- Communication to colleagues the risks relating to patients, on an on-going basis, and during shift changeover safety huddles. Practices must also take account of the need to communicate risks to staff rotating into the clinical area who may not have immediate knowledge of any patient related risks.
- Establishing local protocol committees with Agencies (e.g., NSW Police, as required under the Memorandum of Understanding).

**Role of Security staff (refer to chapter 14 for further more detailed standards)**

- Security staff fulfil a role that has a strong emphasis on assisting with the early identification, prevention and management of incidents.
- 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 (i.e., 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).
  - Manage high risk incidents such as those involving weapons or hostage situations.

Chapter 14 of this Manual sets out in further detail the role NSW Health security staff can (and cannot) be expected to undertake in clinical areas in all NSW Health Agencies.

**Using Physical restraint**

NSW Health standards on the use of physical restraint are set out in the following documents:

- Policy Directive PD2015_004 *Principles for the Safe Management of Disturbed and/or Aggressive Behaviour and the Use of Restraint* and NSW Health
• Policy Directive PD2012_035 Aggression Seclusion and Restraint: Preventing, Minimising and Managing Disturbed Behaviour in Mental Health Facilities

**Staffing issues**
• Ensure sufficient staffing levels and skill mix to provide prompt clinical care, particularly during peak activity cycles to reduce the risk of violence from patients and visitors.
• Ensure adequate staff levels and skill mix to allow the early recognition of potential for violence, to deter violence and to provide for a response in duress situations.
• Ensure staffing levels, at all times, allow for an adequate duress response to be provided.
• Ensure staffing is arranged so that no individual staff member works alone, in isolation.

**Education and training (refer to chapter 7 for further standards)**
• Ensure the training and education for staff is provided in a timely manner, up-to-date, monitored and ongoing.
• Refer to the NSW Health policy Violence Prevention and Management Training Framework for detailed information on standard outcomes for training for staff.

**Safety and security awareness**
Unit Managers must ensure staff:
• Comply with all established work practices and security procedures including the need to wear mobile duress alarms at all times while on duty, where they have been deemed as necessary.
• Report workplace hazards and incidents. Staff 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 re-occurrence of the incident.
• Participate in appropriate training in the prevention and management of violence and duress response.
• Assist others if it is safe to do so.
• Behave appropriately towards patients and other staff and provide patients and their family members with adequate information.
• Do not wear clothing, jewellery or other accessories that can be used against them or grabbed in an attack eg dangling jewellery or clothing, lanyards, pouches containing scissors or untied long hair.
• Are provided with instruction on where to affix personal duress alarms to ensure easy access in an incident, full functioning of the unit, prevent patients removing them and also prevent false alarms by accidental triggering.

**Patients with particular security needs**
In some circumstances patients who may be considered to be ‘at risk’ seek treatment or are admitted to a NSW Health Agency.

• Such patients may include:
  - Victims of sexual assault.
  - Victims of domestic violence.
  - Patients with a high public profile.
  - Children at risk (e.g. FACS).
  - Patients withdrawing from drugs or alcohol.
  - Patients with mental illness.
  - Patients in custody.
- Patients who are confused or cognitively impaired.
- Patients with developmental disability.

- 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 staff.

- In controlling security risks consideration must be given to:
  - The reason for the presentation (e.g. domestic violence, sexual assault).
  - Whether the individual is a child or an adult.
  - Whether the patient is mentally competent to make decisions.
  - The advice of local police or other agencies (where applicable).
  - The unit in which the individual is to be treated (busy or quiet, near security personnel etc).
  - Where the patient is situated in the ward (away from doors, in own room etc).
  - Special arrangements for duress calls.
  - Briefing security and other relevant staff regarding any special procedures.
  - Placing security staff in the ward (as opposed to a mobile response model).


- Reference should also be made to NSW Health Guideline Sexual Safety of Mental Health Consumers Guidelines.

- For security issues related to newborns, NSW Health Agencies may consider the following additional strategies:
  - Removing signage that identifies the nursery (as supported by AS4485.2).
  - 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 should 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.
  - Placement of CCTV at all entrances/exits to the Unit.
Health care facilities should encourage the parent/s to actively participate in the newborn and infant security program, which is best achieved through admissions orientation and awareness programs.
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 staff working in the community must have access to appropriate field equipment and effective communication devices.

Staff must not carry out home 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.

Standards:
Working in the community usually encompasses 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.

Staff working in the community may face a particular set of risks associated with working in environments that are not within NSW Health Agency premises.

Staff working in the community can work alone or in isolation, away from access to rapid support from other staff or even emergency services such as police. This makes them more vulnerable to the risk of violence.

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);

- NSW Health Agencies must have in place procedures, developed in consultation with relevant staff, to assure, as far as possible, security when working in the community. These procedures must be communicated and must cover:
  - Conducting patient risk assessments and appropriate care plan.
  - Obtaining relevant client information from the referring clinician/service.
  - Conducting violence risk assessment prior to each visit and implementing appropriate management measures.
  - Staff training requirements.
  - A means of tracking staff to ensure safe return and follow up if they don't return including procedures for responding to duress alarms or triggered emergency beacons.
  - Appropriate on-going support for staff in the event of an incident.
  - Arrangements for developing and maintaining good communication and cooperation with local police and other local services.
- Identifying relevant local crime demographics ie relevant to risk of robberies, damage/vandalism of vehicles, risk of assault in the vicinity of the client’s home.

- Staff must have access to good quality information regarding contacts and locations, so they can do their job effectively and safely. It is also important that patients and other clients have information about the purpose of visits, so they know what to expect.

- Staff must be provided with adequate equipment, and training in its correct use, including vehicles, communication devices with reception in the areas to be visited (may require satellite phone or two devices such as radio and telephone to provide coverage), remote duress alarm or personal locator beacon as appropriate to the locality, reflective jacket/vest, torch.

- The provision of an effective communication device for community nurses and midwives is a requirement of the Public Health Nurses’ and Midwives’ (State) Award 2011 clause 22 which states:

An employee who is required to visit clients away from a secure working environment shall, during the performance of such duties, be provided with a suitable and effective communication device. The provision of this equipment is intended to improve service delivery, together with enhancing the safety and wellbeing of the employee.

Failure to provide an effective communication device may therefore a breach of the Award.

Working in the Community (away from base)

Preparing for Community Visits

- Ensure adequate equipment is provided including a vehicle suited to the terrain and equipment carried, effective communication device, remote duress alarm (where possible), emergency supplies including torch, blanket, water, and where terrain and/or remoteness indicate, a second spare tyre and/or tyre inflation pump

- Ensure adequate information is provided to staff prior to a community visit, including:
  - As much information as possible about the patient/client/business (particularly prior to the first visit) including any history of violent behaviour or sexual harassment
  - Relevant information about other members of the household, likely visitors and attitude of neighbours or dogs or other dangerous animals
  - Information about the geographical location of the premises (eg is it in a high crime area, geographically isolated, have reduced accessibility to/availability of police)
  - Specific information about the premises (is there security access, stairs, external lighting, hiding places, are the premises modern, in good repair, is phone connected etc) or any other known dangers or concerns from other staff
  - Relevant information from other resources (eg point of referral, inpatient facilities, relevant patient/client records, other staff, local GPs and local police)

- Develop a system where other staff who may have provided a service or inspected the premises in the past are consulted and these issues are documented (eg inpatient medical records). Under the Privacy and Personal Information Protection Act 1998 (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’.

- Implement a system for file flagging/alerts to highlight a history of violent behaviour or other risks. Any patient alert system needs to incorporate the requirements of the PPIPA, as outlined above. For further information on file flagging refer to NSW

- Advise staff to speak to the patient/client by phone prior to appointments, particularly first appointments, to confirm the appointment and clarify the purpose of the visit, as this can also provide insights, including establishing if there are likely to be any visitors.
- Arrange for patients or clients to be seen at clinics where other staff are present, rather than at home if there is a potential for, or history of, violence.
- Arrange for another staff member or police to be present during the visit if there is a potential for, or history of, violence or the situation is unknown.
- Provide appropriate communication devices, remote duress alarms, vehicle security and tracking devices including training in their use, and procedures for response to triggered alarms/beacons or non-return of staff member.
- Provide maps, directories and 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.
- Provide training (eg in related policies and procedures, back to base communication, use and maintenance of security equipment provided, verbal de-escalation and defusion, evasive self-defence, negotiation and conflict resolution).
- Provide a driver or taxi, if appropriate, to areas where cars may be vandalised or staff have to go through unsafe areas to make a visit and ensuring that a return fare is booked for when the visit is finalised so the staff member can leave the area safely.
- Provide staff working in the evening and at night with an appropriate torch (such as a halogen mag light) and spot lights on the side of vehicles.
- Where there is a risk of violence and other risk control strategies have failed to control the risks or resolve the issues, arrange for senior management to write to the household indicating that visits will not be made to that address and that alternative arrangements will need to be made (refer to NSW Health Policy Directive PD2015_001 Zero Tolerance to Violence for further standards).
- Implement procedures for transfer of relevant clinical and risk information on a client when the client changes services.
- Develop and implement incident reporting procedures.
- Provide appropriate support for staff in the event of an incident.
- Implement response plans or procedures for addressing and responding to security incidents during home visits, or when agreed reporting to base protocols with the community health staff member are not maintained.
- Implement procedures for after hours/weekend security. Where available, consider contractual arrangements with third party security service providers.
- Health service 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.

Prior to Leaving Base:
- Establish a system where prior to commencing community based activities, the staff member 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 staff member does not know these in advance they should be communicated to base as they occur) and
  - The proposed route and map references
  - Mobile phone number of the staff member
- Make and model and registration number of the vehicle.
- The system must include procedures for checking return of staff and procedures to follow in the event of the staff member’s failure to return or call in.
- Tracking sheets must be kept safe and confidential and not left sitting where they can be viewed, accessed or removed by unauthorised persons.
- Ensure the staff member has access to patient information and records, including risk assessments, prior to the visit.

**During Community Visits**
- Provide staff with well maintained vehicles and communication devices.
- Ensure staff are made aware of the general security precautions attached (Appendix 16.1) to this Chapter.

**At the Conclusion of Community Visits:**
- Ensure local procedures are 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).
- Provide appropriate support to a staff member who cancels or ends a visit as a result of a perceived or real threat.

**After Hours Visits in the Community:**
- NSW Health Agency staff, who are required to visit clients in the community outside normal business hours, including in an emergency situation, can be particularly vulnerable. Generally speaking no client should be registered with the after hours community service prior to being visited and assessed by staff during business hours, unless all of the following conditions are met:
  - Two staff members attend and / or security and / or police are present.
  - Staff carry a mobile phone/effective communication device.
  - A monitoring system is in place to identify that staff have returned to base or proceeded home.
  - Reliable information has been received that provides details on 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 staff, should be satisfied that the visit can be undertaken safely. In assessing whether a visit can occur safely the manager should seek and be advised of the full clinical diagnosis by the treating Medical Officer including the risk of violent behaviour and any other relevant information.
- Where staff arrive at a site and identify a potential risk such as the person is intoxicated or suffering withdrawal, there are signs of agitation, disorientation or aggressiveness, there are unexpected visitors or visitor’s behaviour is implicitly or explicitly threatening, or illicit activities are underway, staff should withdraw to a safe place and notify management and, where appropriate, the police are to be called.
- If necessary, arrangements can be made for the person to be seen in an emergency department or police station or alternative safe venue.
- Staff are to withdraw until the arrival of police. Staff must not put themselves at risk.
Clients and/or carers should be given instructions to ensure that the house is illuminated and easily identified, access gates are unlocked and animals have been restrained when they are expecting the service.

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 two staff members are rostered on simultaneously.
- Ensure 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).
- Ensure staff carry a mobile telephone and remote alarm or emergency radio beacon in the event of an incident while travelling.
- Ensure emergency and evacuation procedures are developed and communicated to staff (including pre programming emergency numbers into phones, if possible).
- Ensure all major emergency telephone numbers are prominently displayed and an effective contact network is established within the local community prior to the staff working at the site.
- Ensure that doors are locked when clinics are not in session and that the doors are locked when staff are working alone out of clinic hours.
- Establish a system for people seeking entry to identify themselves without staff having to open the door (eg installation of a video intercom system).
- Ensure that all door and window locks are in good working order and maintenance problems are responded to and resolved promptly.
- Ensure that blinds are placed on windows and staff close blinds after hours to reduce the likelihood of break-ins.
- Ensure the visibility of computers, equipment etc is limited by placing them away from windows and doors.
- Establish a system where staff complete a movement sheet which establishes arrival and departure times, routes taken and any foreseeable difficulties with travel to and from the clinic.
- Establish a system where a staff member leaving an isolated workplace advises another staff member of destination, purpose and anticipated return. This will include procedures for what to do in the event of an incident or if the staff member does not check in by the advised time.
- Display signage (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.
- Prominently display signage about non-tolerance of violence.
- Provide written information to patients about appropriate behaviour and their responsibilities. This should form part of their service contract.
- Ensure the facility has a procedure that has been tried and tested to deal with a “failure to notify or return”. This procedure is to include a finalisation process that ensures the failure to return or notify has been safely accounted for. Nominate a person to be responsible for this task for each shift.
- Ensure a duress response is planned, tested regularly and activated when the staff member requires it.
- Ensure that there are escape routes from the consultation room, i.e. two exits.
• Ensure that room layout is such that the staff member cannot be trapped and so that they do not sit with their back to the patient while accessing computers, telephones and other equipment.

• Ensure all fire safety standards are met and that any fire extinguishers, hose reels, etc are appropriate and regularly inspected.

• Ensure staff 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.

When Confronted with Violent or Potentially Violent Behaviour
Under no circumstances should any staff working in the community knowingly place themselves or another person at risk.

• If a client, carer or member of a household or site being visited makes physical or verbal threats, or their behaviour escalates or appears to be atypical, staff should retreat and/or seek further assistance.

• Where the staff member is unable to retreat as their exit is blocked and all other non-physical strategies have failed, evasive techniques may be necessary. Evasive techniques involve manoeuvres designed to free the individual to enable them to retreat.

• In such circumstances staff should always use their telephone/radio/duress alarm to call for assistance. The emergency phone number for mobile phone services is 112.

• Staff should not hesitate to request police assistance. They should contact police on 000 or 112 (which can be used across all mobile phone networks) rather than ringing a local police station, and they should explain to the police the urgency of the issue so that an appropriate response can be formulated.

• When contacting police to arrange a police escort, the relevant police station should be contacted directly, or if unsure about the relevant police station, contact the Police Assistance Line on 131 444 (this is a 24 hour service).

• If potentially violent animals are not restrained the visit should not proceed until the animal is restrained.

• It is most important that all security incidents are reported as per local reporting protocols as soon as possible after the event, and, if relevant, be documented on the client's file.

Field Communication Technology
Staff working in the community must have access to effective communication devices (more than one device may need to be provided).

• The devices should be selected to give as complete communication coverage in the event of an emergency as possible.

• Suitable devices can include mobile telephones, satellite telephones, two-way radios, long-range duress alarms, GPS duress beacons and tracking devices that can provide the location of the person.

When providing communication devices the following elements must be addressed in local procedures and in training of staff:

• Field testing of equipment prior to purchase to determine any limitations.

• How to communicate with designated support systems (eg base, other staff, police).

• How to use/activate communication equipment correctly (including refresher training and drills in using emergency equipment).

• Advise the police that staff are using emergency communication technology and the types of technology being used.

• The limitations of the equipment.
• Testing, maintaining and operating communication systems.
• Effective and efficient methods of communicating problems.
• Initiating a duress alarm.
• Responding to duress alarms where this is a designated part of the staff member’s role.

**********
Appendix 16.1

General Security Precautions when Working in the Community

Staff working in the community must:
✓ Complete a risk assessment of the client and the client's home prior to any visit.
✓ Attend a client with a second staff member, or the police, where there is a risk of violence, or the risk is unknown.
✓ Make an excuse not to enter the premises if the person answering the door gives cause for concern eg if they are drunk, if the patient is not in, or if a potentially dangerous relative is present.
✓ Be familiar with the vehicle they have been allocated and should ensure the vehicle has sufficient fuel to complete the journey.
✓ Know, to the best of their ability, the area, region and streets they work in. They should try and identify the address without having to continuously refer to an electronically aligned navigation system or hard copy map since risks can arise from sitting on the side of the road to read a map, or a staff member trying to read a “SatNav” while driving an unfamiliar road.
✓ Carry emergency supplies such as a torch, water, tyre pump, and GPS emergency beacon, particularly in rural or remote areas.
✓ Terminate the home visit if there is an obvious increase in numbers of people when the clinician presents, or if there is any other overt or implied threat. The pre attendance risk assessment should show who inhabits the premises on a regular basis.
✓ Show identity badges.
✓ Follow the occupant when entering the premises.
✓ Not search for clients by unnecessarily knocking on doors.
✓ Ensure any correspondence for a client is pushed firmly under the door or placed in their letterbox.
✓ Determine whether the client is at home prior to entering the premises if an unfamiliar person opens the door.
✓ Immediately leave if firearms or other weapons are seen (the presence of weapons should be noted in the client's file and communicated to police and management). Staff should not return to these premises until the matter is resolved.
✓ Ensure animals are restrained.
✓ Remain aware of the environment and potential escape routes in case problems arise.
✓ Position self when providing treatment so that the patient or others do not block quick access to exit routes.
✓ Lock their vehicle while driving through areas identified as potentially dangerous.
✓ Con sec all bags, drugs and equipment when first entering the car so that nothing is visible while travelling, and staff are not seen to be hiding them as they park or prior to leaving the car for the visit.
✓ On reaching the intended home visit – only take what is necessary for the visit/treatment. Staff working in the community should only carry personal items necessary for the home visit. Consider a second wallet with drivers licence, Health Service Identification, and sufficient money to cater for a meal. Mobile phones should be kept on the person out of view and laptops kept completely out of view.
✓ Remove navigation systems, personal music storage devices, sunglasses, non-uniform clothes of high end value are all regarded as opportune theft items. Mobile phones and portable navigation systems offer the owner storage for personal information such as home addresses however if stolen this information is available to a thief provides access to the staff member’s home address and daily routine.
✓ Drive to the nearest police, fire or petrol station, other populated place, or a pre-determined ‘safe’ venue if they suspect they are being followed.
✓ Park in a well lit area as close to the patient’s home as possible.
✓ Park in a way to allow rapid exit – facing the intended direction of travel if possible.
✓ Not remain in the parked car for a prolonged period either before or after making the visit and keep doors locked.
✓ Avoid walking in deserted places, or taking short cuts through secluded alleys or vacant lots.
✓ Walk in the centre of footpaths away from buildings.
✓ Observe windows, alcoves and doorways for loiterers, and be aware of any partly open doors where a person could be concealed.
✓ Walk around, rather than through groups of people.
✓ Avoid entering areas of unrest, or where there appears to be trouble in the neighbourhood.
✓ Check lighting and stairwells when entering a building where no lift is available.
✓ Look before entering a lift and not enter if concerned.
✓ Stay near to the door and control panel in lifts and be observant of other passengers.
✓ Cross the street and walk in the opposite direction or into an open business if there is suspicion of being followed by a car.
17. Security in Rural and Remote Health Services

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

Where staff accommodation is provided it must be included in the facility risk management process.

Standards
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):

- Ensure security risk assessments consider the impact of:
  - Reduced access to police and emergency services.
  - Delayed response times for emergency services and other referral agencies.
  - Complications and time delays associated with organising transport of victims or perpetrators out of the community.
  - Small populations, close community ties and lack of anonymity.
  - Conflict between reporting requirements and community sensitivities.
  - Communication difficulties (e.g. no mobile phone coverage etc).
  - Co-location of residence and clinic.
  - Individual working in isolation from colleagues and support systems.
  - Road standards and driving times including risks from wildlife and farm animals on the roads.
  - Climate and associated hazards, e.g. fire, flood, snow.
  - Emergency supplies including to ensure safety during vehicle breakdown or accident (e.g. warm clothing for cold climates, water, EPIRB).
  - Hard-wired and portable routine and emergency communication devices.

- Risk assessments must consider:
  - Access to security advice and support persons.
  - Training of staff in violence prevention and management.
  - Security of buildings.
  - Relationships with other agencies such as Police, SES, Ambulance Service.
  - Routine and breakdown maintenance of security devices.
  - Issues associated with working alone in isolation from colleagues and support personnel.

- Remote health services can work in partnership with other community organisations and businesses to explore opportunities to combine resources (e.g. security patrols).
Field Communication Technology:
Staff in rural and remote health services need to have access to functional communication devices. More than one device may be needed to ensure full coverage. The devices should give as complete a communication coverage as possible, in the event of an emergency. Suitable devices can include mobile telephones, satellite telephones, two-way radios, long range duress alarms and GPS duress beacons that can provide the location of the person.

GPS duress beacons, in particular, should be considered for rural and remote staff due to their ability to assist in locating a staff member who has had an accident, a mechanical breakdown or is experiencing some other misfortune or injury.

When providing communication devices the following elements should be addressed in local procedures and in training of staff:
- Communicating with designated support systems (eg base, other staff, emergency services, other local agencies as required )
- Detection and response to failure to return to base or call in (staff working in the community and sole operator clinics)
- The limitations of the equipment
- Testing, maintaining and operating communication systems
- Effective and efficient methods of communicating problems
- Initiating duress alarms and
- Responding to duress alarms and failure to return to base.

**********
18. Security in Pharmacies

Policy:
NSW Health Agencies are required to ensure, in consultation with staff and other duty holders, that all reasonably foreseeable security risks associated with pharmacy areas are identified, assessed, eliminated where reasonably practicable or, where they cannot 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 must be constructed in accordance with the standards set out in the Australasian Health Care Facility Guidelines as amended from time to time.

Standards:
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):

- Carry out a risk assessment that includes consideration of:
  - 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 and availability of access to the roof.
  - Security of staff including duress alarms and duress response and CCTV.
  - Ability to control and identify persons accessing pharmacy, e.g. by visual identification or card 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 shatterproof glazing while being designed to provide for communication. Install intruder alarms to pharmacies and drug safes. Intruder alarms should include detection of breaches to doors and windows including glass breakage detection.

- Extend 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 laminated glass.

- Incorporate shatterproof security glass windows into the design of the front of the pharmacy to enable staff to carry out transfer operations with safety, while maintaining communication with staff and patients. The framework must be securely anchored and anchor points concealed. It should not be possible to climb in between the window frame and the top of the wall/roof.

- Design a two door entry approach (i.e. one door for the public and hospital staff to enter to access front glass transaction windows and a separate door for the entry of pharmacy staff to the pharmacy).

- Ensure external lighting, CCTV and duress alarms and security arrangements, and access and egress arrangements are provided and are appropriate to staff in pharmacy areas and other staff accessing pharmacy after hours.
- 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 additional 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 to be alarmed – it should report to an audible alarm as well as the portable communication/duress equipment carried by security and staff members.
- Ensure drugs are locked away in a cupboard that is out of the line of vision of patients and the general public
- Ensure a procedure is in place for the safe transportation of drugs to wards and other clinical areas.
- 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. While Chapter 16 deals with staff working in the community it includes standards, in relation to the need to have systems to track whereabouts, relevant to staff transporting pharmaceuticals to other facilities and should therefore be incorporated into local procedures.
- Install an intruder alarm system that meets Australian Standard AS 2201 and incorporates a duress alarm/s to enable staff to activate the alarm in the event of an emergency
- Restrict access to the pharmacy to authorised staff 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
- Ensure, where the risk assessment warrants it, that mobile staff have personal duress alarms.
19. Security in Car Parks

Policy:
NSW Health Agencies are required to ensure, in consultation with staff and other duty holders, that:

- Car parks are designed and located for maximum security for staff, patients and visitors as far as practicable.
- All reasonably foreseeable security risks associated with car parking are identified, assessed, where reasonably practicable eliminated or, where they cannot be eliminated, effectively minimised.
- The process is appropriately documented.
- Effective car park security procedures are implemented, including appropriate lighting levels, access control, CCTV surveillance, signage and after-hours access.
- Designated car spaces are allocated for afternoon and night shift staff, where reasonably practicable.
- 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.

Standards:
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):

- Afternoon and night shift staff are, where reasonably practicable, 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, ensure entry to designated staff parking areas in dual purpose car parks is controlled by gates in the afternoon and night (eg boom gate could be left up in the morning and put down about 1-2 hours before afternoon shift commences so they are operated by pass cards). Exit boom gates should operate automatically (eg after a certain time a card is needed to enter, but exit can occur any time).
- Ensure vehicle entry to car parks is by automated gates or doors, via camera and intercom, or by passing through an entry/exit gate staffed by security personnel.
- Ensure security personnel undertake high profile patrolling in car parks associated with the facility.
- Ensure security personnel undertake random audits on vehicles in a car park (eg door unlocked, window down, valuables exposed etc) and secure the vehicle if possible.
- Display signs in car parks reinforcing theft awareness.
- Display signs that advise that regular patrols are undertaken and CCTV monitoring is in place.
- Provide security escorts for staff at the conclusion of afternoon and night shifts. This would include designating a mustering spot for staff to assemble.
- Ensure landscaping is done in a way to provide good line of sight.
- Ensure all car parks have:
- Good lighting (refer to AS 1158.3.1, AS4485.1.5.2 Security for Healthcare Facilities 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 on line of sight.
- Flexibility to close some entrances and exits during low traffic periods.
- Approved locks on exits intended for emergency exit only.
- Frequent patrols by security personnel.
- CCTV surveillance.
- Duress alarm points.
- Routine maintenance of lighting and other systems.

- Restrict the parking of delivery vehicles to a parking dock.
- Ensure facility vehicles are parked in a secure overnight car park with good lighting and regular security patrols. A fenced compound or lock-up garage is preferable.
- Ensure all facility vehicle keys are held by the designated custodian when the vehicle is not in use, and taken by the driver when the vehicle is required.
- Provide security for bicycles and motorcyles (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).
- 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.
- Advise staff to:
  - Use security escort services or travel in groups to the car park when working at night.
  - Meet at designated mustering spots.
  - Park in designated afternoon/night shift parking areas. If this is not possible, park in well lit areas close to the facility and/or moving the vehicle closer during break.
  - Report any suspicious activity.
  - Not confront any potential assailants or persons seen attempting to break into a vehicle.
  - Not leave valuable or attractive items on view in the vehicle, including small amounts of change.
  - Not load valuable or attractive items into the vehicle in public areas, if the vehicle is to remain parked.
  - Not leave important papers, driver's licence or registration papers in vehicles.
  - Avoid parking in isolated or dark places and try to park under a street light or in a well lit area. Consider if there will be sufficient light when returning to vehicles after shifts.
  - Activate/use any alarms or other protection devices where they are fitted to the vehicle or car park.
  - Close all windows, lock all doors and take the keys when leaving the vehicle.
  - Carry keys in hands when approaching vehicle as this will avoid having to stand and search for keys on arrival at vehicle. Carry any access cards in hand when leaving the car and approaching doorways to allow quick access to the facility.
  - Do not unlock central locking systems or alarm systems until you are close to the vehicle.
  - Check for persons who may be loitering or hiding before unlocking the car

********
20. Security of Property

Policy:
NSW Health Agencies are required to ensure, in consultation with staff and other duty holders, that all potential for theft and wilful damage is identified, assessed, eliminated where reasonably practicable or, where it cannot 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:
Every case of theft and wilful damage needs to be reported to the police. If the theft involves a staff member, no arrangements should be entered into to accept settlement eg resignation on condition that the NSW Health Agency refrains from instituting legal proceedings.

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):

- Keep assets and property registers up-to-date, providing full descriptions of each item, including serial numbers.
- Keep a separate register of donated items, equipment of historical value, antique furniture or other items of historical, heritage or cultural significance.
- Keep a register of property theft and wilful damage to assist with identifying problem areas or patterns of behaviour.
- Investigate all theft.
- Identify all assets with a unique physical marking, such as bar code, micro dot systems, digital photography, nano marking, invisible marking pens or chemical identification. This includes items of historical, heritage or cultural significance which should be invisibly coded.
- Store attractive portable items (calculator, cameras, tape recorders etc) separately in a locked area. Only designated staff should have access.
- Enforce an effective key control program (for more information refer to Chapter 10 of this Manual).
- Utilise CCTV monitoring of identified high risk areas.
- Install alarm systems (refer to Chapter 11 of this Manual for more information).
- Ensure effective perimeter and internal access control (refer to Chapter 9 of this Manual for more information).
- Ensure CPTED principles are applied when designing/refurbishing facilities (refer to Chapter 4 of this Manual for more information).
- Reduce risk of theft by ensuring that obsolete equipment with no historical value is written off and disposed of correctly and promptly.
- Where items of historical, heritage or cultural significance are displayed, and where practicable, ensure that display cabinets are secure with shatterproof glass, secure locks and, where risk assessment indicates a need, alarms that respond to any breach of locks or glazing. The cabinets should be under camera surveillance and located in high traffic areas to reduce opportunities for unobserved theft.
Install security screens in areas that are not continually staffed, e.g. reception areas, so that valuables such as telephones and computers are secure.

**Specific Areas for Attention:**

**Engineering/Maintenance:**
- Ensure controlled access to areas where tools or equipment are stored.
- Brand or stencil all tools or equipment to show ownership.
- Keep a written record of tools or equipment on loan from one section to another.
- Ensure staff understand their responsibility for the equipment allocated to them.
- Ensure that vehicles are parked away from storage areas to reduce opportunities to steal items.
- Conduct regular checks of inventory.

**Transport:**
- Ensure petrol pumps are only operated by authorised staff. The petrol pumps should be locked when not in use.
- Regularly auditing petrol pump use and reporting unauthorised use.
- Only purchase vehicles with a locked petrol cap cover and inbuilt security devices (e.g. data dot technology, ignition locks).
- Regularly monitor vehicle running petrol sheets purchase details and comparing them to distance travelled.
- Where practicable ensure that vehicles are securely garaged or parked in compounds. Garages and compounds should be subject to security inspections on a regular basis.
- Ensure that all property transported in vehicles (e.g laptops) is 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.

**Laundry:**
- Ensure deliveries are met and signed for.
- Check delivery weights (quantities) against delivery dockets. A signed copy in the Linen Supply Area should be used to check against amounts and quantities charged for.
- Check account delivery amounts and quantities against Linen Service records for correctness.
- Ensure linen is not left on open trolleys in areas where it can be pilfered unobserved, e.g. loading docks, infrequently used corridors or corners, unsecure bays. Where practicable, linen should be stored in a lockable room or linen bay.
- Limit access to linen stock rooms in wards and facility areas, and ensure that these have minimum stock levels.
- Ensure that vehicles are parked in areas away from the linen supply area.
- Conduct spot checks of linen levels held against stock records.
- Undertake spot checks of facility areas which have been allocated linen to look for:
  - Excess stock, above the agreed imprest levels.
  - Shortage of stock.
• Ensure that soiled linen bags are not 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 should be placed in strategic areas where they are visible.
• Ensure babies are not discharged in NSW Health Agency clothing or blankets.

Catering:
• Regularly reviewing 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 should be immediately moved to secure storage areas.
• Ensure that fridges and store areas are locked at all times and only opened to take supplies necessary for the meal that is to be cooked. Ideally the store should then be locked. Consider installing time delay alarms to alert when a door is not secured or is opened without authority.
• Ensure that lockers are provided for staff 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 should not be of such a size that they pose a manual handling risk to staff.
• Do not allow utensils or equipment to be borrowed by kitchen staff. The facility name should be stencilled or marked on portable items (eg 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. Persons are not allowed in the kitchen area unless accompanied by a senior kitchen staff.
• Ensure that all stores and fridges are locked when maintenance work is being carried out.
• 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.
• Check the return of cutlery, plates and food trays from wards against what was issued. Food equipment should 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.

Stores:
• Ensure staff 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 should be immediately located in a secure area.

Ensure that goods to be delivered to facility areas are receipted/signed for with copies of signed paperwork kept with facility and stores area.

Check altered requisitions for accuracy before acceptance. Internal requisitions that have been altered should not be acceptable under any circumstances.

Where possible, ensure that goods are ordered and issued as complete packages, ensuring broken packages stand out.

Conduct physical checks to look for broken packages or seals, and to ensure that bottom 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 should not be so large as to create a manual handling risk to staff.

Ensure that vehicles are parked in an area away from the store.

Restrict entry/exit to the store to only one door which is able to be observed by supply/stores staff.

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.

Lock away items such as batteries.

Ensure that stocks held in areas are securely stored and not easily accessible to patients and unauthorised staff. 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.

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 should only be made available to authorised persons (Refer to Chapter 21 for additional information).

Ensure laptop computers are password protected and securely stored when offices are left unattended.

Store office consumables in a lockable area and nominating one member of the administrative staff to issue stationery requirements.

Mail Deliveries:

Ensure receptacles for mail are clearly labelled and cannot be accessed or opened by unauthorised persons.

Ensure deliveries of mail are made in a restricted, defined area with appropriate access control.

Ensure staff pigeon holes are in secure areas accessible only by staff.
- Keep registered mail/couriered packages separate from other incoming mail and establishing procedures for receiving and promptly securing registered mail/couriered packages.
- 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.
- Limit the access to the mail areas or use a sign-in access card system.
- Keep the area for receiving incoming/outgoing mail separate from other operational/public areas including using a counter to separate the mail area from other working areas.
- Ensure all work areas are visible to supervisors.
- Ensure emergency procedures as per Chapter 25 are in place

**Cash Handling:**

- Ensure cash handling, receipting and banking practices are consistent with the document entitled ‘Accounting Manual for Public Health Organisations’.
- Ensure emergency procedures as per Chapter 27 are in place.

**Patients’ Property:**

- Information given to patients before admission should advise that:
  - Large sums of money, items of significant value, monetary or otherwise, should 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, 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 should be placed in an envelope with the patients' identifying details (e.g. MRN), a receipt provided to the patient with the details of the items, signed by the staff member in the presence of the patient or another staff member 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, and any 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 ICAC.
- Property held in safekeeping must be checked against the original list on discharge of the patient.

**Note:** Where money is placed into the Patients’ Trust Account the details should be entered into the Patients’ Valuables Register.

- 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 patients’ 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 cloakroom should be used to store the clothing and must be kept locked.
• Routine ward level checking of food trays and linen, for patient property such as hearing aids/dentures should occur.


**Staff Property:**
• Discourage staff from bringing large sums of money, personal documents or belongings into the workplace.
• Ensure that staff are provided with a lockable storage area (eg individual locker or cupboard) for safe keeping of their property.
• Ensure car parks have good lighting and camera surveillance to deter theft and vandalism.
• Signpost areas such as locker rooms and cafeterias to warn staff to keep their valuables secure.

************
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 cannot be eliminated, effectively minimised.

NSW Health Agencies are required to ensure that the risk management process is undertaken in consultation with staff 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.

*’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.

Standards:
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):

- 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 should be 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 staff 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.
- IT technical staff must ensure correct configuration of 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.
• 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.

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 Privacy Manual for Health Information (March 2015) provides guidance material to assist NSW Health Agencies to comply with the security requirements established in the Health Records and Information Privacy Act 2002.

Security of Equipment:
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, locked in the boot of cars and
• Equipment is only left in cars where absolutely necessary.
• Computer system servers must be located in secure, climate controlled locations off public corridors.
• All records are removed from equipment prior to disposals.

Labelling Information:
• Sensitive official information must be protected from unauthorised access.
• NSW Health Agencies must use ‘labels’ to mark such information, whether it be in electronic, paper or other format.

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

There are three levels of labelling. These are, in ascending order of sensitivity:
• X -IN-CONFIDENCE (where X may be ‘CABINET, COMMERCIAL, CLIENT, PERSONNEL or some other term selected by the NSW Health Agencies as appropriate to their needs)
• PROTECTED
• HIGHLY PROTECTED

The absence of a sensitivity label means that official information continues to be handled in accordance with existing NSW Health Agency practices, including compliance with the Government Information (Public Access) Act 2009.

The Department of Premier & Cabinet Circular 2002/69 (Guide to Labelling Sensitive Information) provides standards for the preparation, handling, removal, auditing, copying, storage, disposal and transmission of sensitive information and should be utilised by NSW Health Agencies when developing local procedures.

Disposal of information
• NSW Health Agencies should therefore refer to the General Disposal Authority (GDA 17) Public health services: Patient/Client Records, issued by State Records NSW in determining how long to retain clinical and client/patient records.

Further Reference:
- NSW Health Policy Directive PD2013_033 Electronic Information Security Policy
- Department of Premier & Cabinet Circular M2007/04 Security of Electronic Information

**Standards:**

**********
22. Security of Medical Gases

Policy:
NSW Health Agencies are required to ensure, in consultation with staff 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 cannot be eliminated, effectively minimised.

Medical gases can take the form of gas cylinders of a range of sizes including bulk tanks, and gas delivery plant and piping.

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

Standards:
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):
- Ensure access to any storage and gas plant areas is restricted by use of doors, barriers and signs. Sources are to be secured against unauthorised removal, tampering, vandalism and misuse.
- Ensure appropriate access control procedures are developed and implemented
- Document the location of medical gases both in the bulk storage facility and at the ward level.
- Ensure records are kept for medical gases used for fieldwork. They should 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.
- Ensure procedures are implemented for reporting theft, tampering and damage to medical gases.

Bulk Medical Gas Storage:-
- Bulk storage facilities are housed within a secure compound that can be locked and signposted in accordance with relevant Standards, and Dangerous Goods Regulation.
- Sign posting should include parking restrictions around the compound as well as a dedicated sign advising heavy frosting is a normal function of the bulk storage facility.
- Line of sight to the compound is advised to prevent opportunities for unobserved interference with equipment.
- Filtering systems are to be housed in a secure room with restricted access.
- Access to bulk medical gas compounds is to be restricted to selected persons such as the contracted supplier, maintenance staff, security staff and people who will be involved with the ongoing management of the service.
• 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.
• Fit locking devices to exposed valves.
• If the compound is located in the vicinity of a populated car park – consider fitting bollards at strategic points as a protection measure against accidental damage such as backing into the fence.
• If the compound is located in an area where there is a possibility of vandalism consider CCTV monitoring, and the fitting of bollards to prevent vehicles being purposely driven into the compound. Bollards will also act as a deterrent or enforcement mechanism to parking restrictions.
• 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 – so as to allow department isolation in the event of a fire.
• Staff are to be educated as to how to isolate bulk medical 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 staff through the security education program to report suspicious behaviour, unusual vehicle parking/movements or loitering in the vicinity of the medical gases storage area.

Storage of Portable Cylinders of Medical Gases
Facilities are to consider replacement value of cylinders which can represent a significant amount of value (some portable medical gas cylinders are worth up to $1000 each).

• Identify staff to be entrusted to accept new/replacement cylinders and loading of spent/exhausted cylinders.
• On changeover – accept only cylinders in good structural condition, correctly identified through the cylinder identification label (located at the head) – reject cylinders with damaged cylinder valves – reject any cylinder that has no identification label. Reject cylinders with no or damaged date tags (these are also a reference to heat damage).
• Storage compounds/areas should be subjected to a risk assessment prior to being used for the storage of medical gases.
• The area is to be located in a secure purpose dedicated area position in a well-ventilated external area – the area should be weatherproof, stable level ground, and free of ignition possibilities.
• Discourage internal compounds or storage opportunities lower that 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.)
• Ensure portable medical gas storage compound is adequately illuminated – to include paths of travel of collect and return, within duress alarm coverage, and consider CCTV monitoring.
• Separate full and empty medical gas cylinders – it may be appropriate to separate some medical gases rather than store commonly in one area.
• Sign post compound in accordance with the Dangerous Goods Regulations:- included in the signposting should be dangerous goods class diamond, HAZCHEM notification, No-smoking signposting naked flame warnings, parking restrictions.
• Where appropriate, fit bollards to prevent unauthorised parking, possible vandalism opportunities and allow accessibility to change over practices.
• Pressure gauges and regulators should be stored internally.
• Encourage all staff 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 staff to remove and arrange replacement of any cylinder that has fallen over or been exposed to unusual heat related conditions.
• Changing valve assembles should only proceed once hand cleaning agents have completely dried. Aquium and some hand gels used in Healthcare facilities contain a lubricant. There is a slight possibility of Aquim coming into contact with the male thread of the valve which in turn if threaded into the female coupling – can create a leak possibility.

**Portable Medical Gas – storage at a Ward level**

• Store in a dedicated area – where patients and visitors cannot tamper with full cylinders.
• Store in closed valve position.
• Do not allow portable medical gas cylinders to stand unattended for extended periods at a ward level – eg in corridors, patient rooms or store rooms.
• Entonox and Nitrous Oxide should be stored in a secure manner ie lock and key to discourage misuse and accidental damage.
• Report suspicious behaviour if observed where medical gas cylinders are stored.
• Ensure appropriate access control procedures are developed and implemented.
• Document the location of medical gases both in the bulk storage facility and at the ward level – important point when considering storage areas – and dealing with evacuation possibilities or briefing emergency services.
• Ensure records are kept for medical gases used for fieldwork e.g. hospital in the home. They should 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.

**Transport of medical gas cylinders:**

Prior to leaving

• Consider weight and safest place to transport cylinder/s.
• Try and transport only one cylinder at a time.
• Plan the trip and book a vehicle that has a fixed metal partition separating the rear compartment from the passenger seating (this allows a secure structure to fix medical gas cylinders to be installed). If the transport of medical gas cylinders is to be a regular occurrence, then attempts should be made to allocate a dedicated vehicle with purpose installed straps or method to secure the cylinder into position,
• Check the cylinder for leaks.
• Check the valve assembly to ensure the cylinder is completely turned off, and 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.
Transport the medical gas cylinder in the boot – if a passenger vehicle with fixed rear seating.

Store the medical gas cylinder on the floor in well of the off side passenger back seat (deemed the safest place in a MVA) if there is a need to transport a second or subsequent number of medical gas cylinders, or no boot space is available.

Remove the medical gas cylinder at the first opportunity on arriving at destination –

Do not store an unrestrained medical gas cylinder in the rear load compartment of a hatchback or station wagon.

Do not transport with valve assembly/regulator fitted.

Do not store any portable medical gas cylinder in the front passenger compartment.

Do not leave a medical gas cylinder/s for extended period in a closed unventilated vehicle.

Do not attempt to use seat belts to secure medical gas cylinders. The safest position is to lay a cylinder down.

Do not lay a medical gas cylinder on the back seat.

IN THE EVENT OF A VEHICLE TRANSPORTING MEDICAL GASES BEING INVOLVED IN A MOTOR VEHICLE ACCIDENT – WARN EMERGENCY SERVICES AT THE FIRST OPPORTUNITY OF THE PRESENCE OF THE CYLINDERS, WHERE THEY ARE LOCATED AND WHAT TYPE OF MEDICAL GAS IS BEING TRANSPORTED

**********
23. Security of Radioactive Substances

Policy:
NSW Health Agencies are required to ensure, in consultation with staff and other duty holders, that all reasonably foreseeable security risks associated with radioactive substances are identified, assessed, eliminated where reasonably practicable or, where they cannot be eliminated, effectively minimised.

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

Standards:
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):

- 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.
- Maintain records of the location of radioactive substances and irradiating apparatus.
- Ensure records are kept of all radioactive substances discharged from the premises which include the following information:
  - The type of radioactive substances discharged.
  - The estimate of the total activity of the radioactive substances discharged.
  - The manner in which the radioactive substances were discharged.
  - The date on which the radioactive substances were discharged.
- Ensure any loss or theft of radioactive material, as required by the Radiation Control Regulation 1993, is reported to:
  - The officer responsible for radiation safety.
  - The Chief Executive Officer or Facility Manager.
  - The Director-General of the Ministry of Health.
  - Police and Radiation Control Section, Environment Protection Authority.

As much information as possible about the source should be given.
Note: In emergency situations involving suspected or actual damage, spillage, loss or theft of radioactive substances the Radiation Control Section of the Environment Protection Authority should be contacted.

- Ensure, where a local radiation safety manual is prepared, the manual includes a section on the security of radioisotopes used and/or stored in those facilities. All radioisotopes used or stored within a facility and their subsequent disposal must be recorded in a register. No unauthorised access to radioisotopes is to be permitted.
Security during Transportation of Radioactive Substances:

- Ensure only authorised persons undertake the escort of radioactive substances when being transported within an organisation.
- When radioactive substances are transported by road, the transport needs to be in accordance with the legal requirements as per Section 25 of the Radiation Control Regulation 2003 and the Safe Transport of Radioactive Material Code of Practice – 2008 (Australian Radiation Protection and Nuclear Safety Agency).

**********
24. Fire, Evacuation and other Emergencies

Policy:
NSW Health Agencies are required to ensure, in consultation with staff and other duty holders, that all reasonably foreseeable security risks associated with fire and other events that may result in evacuation or significant upheaval are identified, assessed, eliminated where reasonably practicable or, where they cannot 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 should also be incorporated into disaster and service continuity plans.

Standards:
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):

- Risk assessments must include consideration of the following:
  - Accounting for staff, patients 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
  - 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 should be contacted in the event of a fire or other emergency and when this contact should occur
The specific role of NSW Health Agency staff and emergency services. This includes the roles of unit staff, e.g. 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)

Details on assembly points.

NSW Health Policy Directive PD2010_024 *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.
25. Bomb Threat/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 staff, 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.

The Department of Premier and Cabinet procedures for reporting security incidents have been incorporated into this chapter.

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, e.g. 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 risk assessment determines another control is more appropriate (a risk assessment may also identify additional controls necessary to address 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 relevant outcomes
of the risk assessment undertaken in the workplace and must be consistent with the Australian Standards Codes for Emergencies (as set out in the local Emergency/Rainbow Flipchart).

- Provide 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 manager 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 staffed 24/7, calling 000 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.

Australian National Terrorism Threat Level (New section)

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.

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.
Security and Housekeeping:

- Good quality door fittings, locks and alarms to deter after hours penetration of the workplace must be installed (refer to Chapter/s 9 and 11 of this Manual for more information)
- Entry/Exits points must be restricted or minimised (refer to Chapter 9 of this Manual for more information)
- Assessment of the need to install surveillance equipment (closed circuit television 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 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 and surveys must be conducted
- The services of professional advisory bodies such as the Australian Bomb Data Centre, 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.

Routine security checks in the workplace (white level inspections)
While it is important that staff are routinely vigilant about unexplained changes in their working environment, during periods where the Government determines that the terrorist alert is probable (or above), a structured program of inspecting workplaces and common/public areas is implemented that includes the following:
- They occur at the start of each shift
- Staff 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.
- Staff advise their manager, or a designated contact person, that they have conducted a check or there is a process in place where staff report by exception ie they advise if their scan indicates something is out of place.
- Staff are given instruction on how to carry out a ‘white level inspection’.

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 Appendix 25.2 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
(HASFAC) and/or the nominated position with responsibly for local emergency/incident co-).

- 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 local Police station must be called. If the immediacy of the threat is unclear the 000 number must be used.
- The role of NSW Health Agency staff 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 radio controlled devices such as two way radios, duress alarms and mobile telephones could cause detonation of a device.
  - Guideline for conducting a search of premises.
  - Documented protocols for evacuation (including prioritisation of patients and identifying multiple evacuation routes). Protocols must information on assembly points and processes for searching prior to evacuation.
  - 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 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 publically displayed.

Samples of an Incident Report (Appendix 25.1) and a Threat Procedure (Appendix 25.2) are attached to this Chapter.

**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). NSW Health Protection Unit and policy documents can be referred to (http://www0.health.nsw.gov.au/policies/PD/2005/pdf/PD2005_132.pdf).

**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 should 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 staff and a call made for assistance, in line with local procedures.
Identifying suspicious items:
Suspicious items may display a combination of the following characteristics:
- Excessive securing material i.e. Tapes and wrapping
- Excessive weight
- Protruding wires or tin foil
- Oily stains and discolorations
- Visual distractions i.e. Packages marked as "Fragile–Handle with Care," "Rush–Do Not Delay," "Personal," or “Confidential.”
- Excessive postage
- Chemical or solvent smells or unusual odours
- Incorrect titles, names or addresses
- Common words misspelt
- Either unusual or foreign origin
- 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.

Responding when an Item is assessed as suspicious:
- If an item is considered suspect, local procedures consistent with the standards 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 staff:
  - 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
  - DO NOT USE RADIO TRANSCEIVERS, CORDLESS PHONES OR MOBILE TELEPHONES NEAR THE OBJECT.
  - 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 he/she is expecting the item. If a return address is on the article, check with the originator
  - Isolate the article. Place the suspect item in a safe isolation area (if safe to do so). The isolation area must be remotely located from the screening point and provide for the safety of employees and minimum damage to buildings should the suspect mail item suddenly function.
  - Consider whether evacuation is necessary. Evacuation must always be considered in the event of a potential bomb threat. Evacuate the immediate area and 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 should 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 should 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.

Managing Post Incident Issues:
NSW Health Policy Directive PD2014_004 *Incident Management Policy* provides a framework for managing post-incident issues such as incident reporting, and incident investigation.


Related NSW Government Policy:
- Procedures for Reporting Security Incidents (Department of Premier and Cabinet Circular c2007-44)

Related NSW Health and Other Resources:
- AS4083 Planning for Emergencies in Health Care Facilities
- Bombs: Defusing the Threat (Australian Bomb Data Centre)

Further Information:
For further information contact:
Australian Bomb Data Centre
GPO Box 361
CANBERRA ACT 2601
Telephone: 02-628 70750
Fax: 02-628 70770
Email: abdc@afp.gov.au
Appendix 25.1

Sample Bomb Threat or Threatening Telephone Calls Incident Report

(refer to Emergency Flipchart/Rainbow Chart - Code Purple)

Instructions:

- Keep calm and sound calm. Use delaying tactics to gather details to complete this form.
- Gather as much information as possible to the questions listed below at number 4 in the table (Bomb Threat Checklist in the Emergency Procedures manual)
- Concentrate on the caller’s voice and background noises to provide as much information as possible at number 5 in the table ‘Other information’
- If there is a bomb threat or physical threat against a person or a place, the Police (000) must be alerted immediately. Stay calm and keep talking to the caller while attracting the attention of other staff and indicating to contact the designated person.
- Do not hang up the phone at the end of the conversation. You must inform the supervisor (or direct colleague if supervisor is not available) then go to a private area to write down what was heard, to ensure the information is as accurate as possible.

Details:
1. Time, date of the call and the information provided on the handset screen
   
   Date:   Time:   Info on screen

2. Trace the telephone call
   (Insert information relevant to the particular telephone system being used)

3. Nature of the call (please circle):
   Bomb threat   Threat of violence   Abusive   Other

4. Information to obtain from the caller

| If a bomb or violence threat: Who or what is being threatened (name of person or place) |
| Exact wording of threat or telephone call: |

<table>
<thead>
<tr>
<th>For a Bomb Threat</th>
<th>For a Threat against a person or an abusive other call</th>
<th>For Chemical, Biological or Radiological Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>When is the bomb going to explode?</td>
<td>Is there a threat against a particular person or place?</td>
<td>What kind of substance is in it?</td>
</tr>
<tr>
<td>Where did they put the bomb?</td>
<td>If a threat of violence against a person or place is made</td>
<td>How much of the substance is there?</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>When did they put it there?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Why are they making this call?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How will the substance be released?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What does the bomb look like?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What would they like to see done about the problem?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the substance a liquid, powder, or gas?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What kind of bomb is it?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What will make the bomb explode?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Did they place the bomb?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Why did they place the bomb?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information about the caller</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What is the caller’s name?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Where is the caller?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Where does the caller live?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other information</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Other information about the call

<table>
<thead>
<tr>
<th>Voice</th>
<th>Speech</th>
<th>Manner/Attitude</th>
<th>Telephone call</th>
<th>Background noise</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ man</td>
<td>□ fast</td>
<td>□ calm</td>
<td>□ local</td>
<td>□ music</td>
</tr>
<tr>
<td>□ woman</td>
<td>□ slow</td>
<td>□ angry</td>
<td>□ STD</td>
<td>□ talk</td>
</tr>
<tr>
<td>□ child</td>
<td>□ distinct/culture</td>
<td>□ emotional</td>
<td>□ overseas</td>
<td>□ typing</td>
</tr>
<tr>
<td>□ unknown</td>
<td>□ impeded</td>
<td>□ loud</td>
<td>□ public</td>
<td>□ children</td>
</tr>
<tr>
<td>□ est age</td>
<td></td>
<td>□ soft</td>
<td>□ private</td>
<td>□ traffic</td>
</tr>
</tbody>
</table>
6. Information about the person taking the call

   Name:

   Contact Telephone number:

   Facility name:

   Location:

   Please complete this Incident Report immediately following the threatening telephone call and hand it to (designated person eg the nominated position with responsibility for local emergency/incident co-ordination).
Appendix 25.2

Sample Procedure for Bomb Threats or Threatening Telephone Call

In the event of a bomb threat or threatening telephone call

- **Staff must:**
  - Remain calm, control emotions and not shout
  - Complete the Incident Report
  - Try to keep the caller talking as long as possible
  - Try to raise the alarm to ensure appropriate action is commenced as soon as possible (ie call supervisor/emergency co-ordinator)
  - **DO NOT HANG UP THE PHONE,** even after the caller has hung up (it can make it easier to trace the caller)
  - After the call has finished contact the emergency co-ordinator or supervisor and inform them:
    - That a bomb threat or threatening telephone call has been received
    - Of their name, telephone number and location
    - Details of the threat.

- **The emergency local co-ordinator must:**
  - Call the police and tell them:
    - That a bomb threat or a threatening call has been made or a suspicious item located
    - Their name, address, telephone number of the facility
    - The exact location of the suspicious object or the details of the threat
  - If a suspicious item - arrange for a staff member to be at the appropriate facility entrance, where it is safe to remain, to guide the police to the suspicious item by the quickest route. Once a suspicious item is found the senior police officer is responsible for managing the situation.
  - Co-ordinate the evacuation by selecting the evacuation route and searching the evacuation and assembly point routes prior to the evacuation.

- **If a suspicious item is located staff must:**
  - Remain calm, control emotions and not shout
  - **DO NOT TOUCH THE OBJECT OR COVER IT OR MOVE IT**
  - Evacuate the immediate area and prevent re-entry
  - Contact the local emergency co-ordinator or 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

**WARNING:** **DO NOT USE RADIO TRANSCEIVERS, CORDLESS PHONES OR MOBILE TELEPHONES NEAR THE OBJECT.**
26. Violence

Policy:
NSW Health Agencies are required to ensure, in consultation with staff 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.

Note: Attention is drawn to the agreement between the NSW Nurses’ Association and NSW Health that in isolated facilities/units a minimum of two nurses or midwives must be rostered on each shift. If a second nurse or midwife is not available on a shift then a security officer or health and security assistant (HSA) should be hired or other appropriate personnel be in attendance.

This agreement occurred in 1996 and also stated that similar attention should be paid to the needs of community health staff who attend patients in isolated circumstances or in locations without ready access to support.

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.

Standards:
The Work Health and Safety Regulation 2011 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. Examples include, a unit located in a separate building, a unit separated from other units by administration or storage areas (i.e. areas not occupied 24/7), a nurse working alone in a unit separated from other units by closed doors, a community or hospital-in-the-home nurse working alone with patients where there may be a potential threat from the patient or their family or visitors.

NSW Health policy ‘Zero Tolerance Response to Violence in the Workplace’ (Policy Directive PD2005_315) provides more detailed information on NSW Health standards for preventing and managing violence in the workplace.

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):

- Ensure security issues are considered and addressed in the design of new facilities and upgrades (refer to Chapter 4 for further standards).
- Ensure appropriate communication systems (e.g. mobile phones, satellite phones, two-way radios, GPS tracking devices), duress alarm systems (including remote duress alarms used by community and outreach staff) and protocols are
implemented, particularly for those working in high risk units, the community or at isolated sites/units (refer to chapters 11 and 16 for further standards).

- Ensure duress alarm systems are installed and used in priority areas such as emergency departments, mental health units and drug and alcohol clinics (refer to chapter 11 for further standards).
- Restrict access through the use of key/electronic access to areas that hold cash, drugs, equipment, other valuable assets, or confidential documents (refer to chapters 10 and 11 for further standards).
- Ensure an adequate number of trained staff to respond to duress alarms
- Ensure training needs are assessed and required training provided (as outlined in NSW Health Policy Directive PD2012_008 Prevention and Management of Violence Training Framework).
- Ensure the provision of appropriate security services by regularly reviewing security needs (refer to chapter 14).
- Ensure identification of risks and violence prevention is incorporated into clinical protocols, e.g. prompt diagnosis and treatment of delirium, and drug or alcohol dependency.

Providing Secure Staff Accommodation

- Limit access to staff accommodation by key or card control access system.
- Ensure surrounds, parking areas and paths between the facility and accommodation are well lit, and that, as far as possible, there is good line of sight with no areas where a person could hide (ie overgrown bushes).
- Ensure windows, doors and locks can be properly secured while still allowing for adequate ventilation.

Responding to Violent Behaviour:

NSW Health Agencies must support staff in responding to violent behaviour and incidents. Support may include:

- Allowing staff to attend police station during work hours.
- Providing a support person when making statement to police.
- Supporting staff who are having problems with violence from an inpatient, community patient or patient family.
- Ensuring that staff have adequate communication equipment such as phones that work in the areas that they visit.
- Ensuring staff are able to attend training.

All officers, managers and staff must be aware that a range of options exists when faced with violent individuals. These responses will depend on a number of factors including the nature and severity of the event, whether it is a patient, visitor, intruder, or staff member and the skills, experience and confidence of the staff involved. This response may include immediately triggering a duress response as defined in Chapter 29 of this Manual.

When confronted with violent behaviour, there are immediate and short-term options available to staff, presented in no particular order, which include the following:

- Issuing a verbal warning.
- Seeking support from other staff.
- Requesting that the aggressor leave.
- Requesting review by a clinician.
- Using verbal de-escalation and distraction techniques.
- Retreating.
- Utilising NSW Health security and/or clinical restraint policies as appropriate.
- Utilising NSW Health sedation policies as appropriate.
• Initiating internal emergency response in line with local protocols (refer to Chapter 29 - Duress Response Arrangements).
• Initiating external emergency response in line with local protocols eg external security services, police.
• Providing police with the necessary information to enable an assessment of whether charges will be laid against a perpetrator.
• More than one strategy may be used as considered necessary. However, if a staff member feels unsafe at any time they should retreat, if possible, and call for back-up. At all times the key priority is to prevent injury.
• Chapter 15 (Security in the Clinical Environment) provides guidance where a staff member has to engage in evasive self defence or physical restraint to manage a violent individual.

When considering options the following points should always be kept in mind:
• Where the aggressor is a patient, the possibility of an underlying clinical condition contributing to the violent behaviour must always be a consideration, therefore assessment by a clinician at the earliest opportunity should be considered.
• When confronted with violent behaviour it is important to remain calm and assess the level of threat as this will allow decisions to be made as to the most appropriate action.
• Regardless of action taken, de-escalation and containment should always be the primary considerations.
• Be aware of the potential for violence, recognise contributing factors/warning signs, stay calm, initiate early, appropriate action.

In some cases violent behaviour is not a one-off incident but reflects a pattern of behaviour for an individual, and longer term options to manage repeated violent behaviour should be considered such as:
• Formal patient management plans.
• Written warnings.
• Conditional patient treatment agreements.
• Exclusion of visits.
• Conditional visiting rights.
• Patient alerts in conjunction with support management plan.
• Recognition of inability to treat in certain circumstances.
• Taking out an AVO to protect staff.

If faced with an armed hold-up situation the priorities are:
• Safety of self and
• Safety of others.

Chapter 27 (Armed Hold-up) provides more detailed information on what to do if faced with an armed hold-up situation.

**Managing personal threats against individual staff members**
Where threats are made against an individual staff member the following must occur:
• All such threats should be immediately reported to the appropriate manager, and to 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 staff, until more detailed information can be gathered.
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.
- Tightening access control to areas where the affected staff member is working.
- Maintaining a security presence in the relevant work area.
- Ensuring the affected staff member does not work alone.
- Ensuring the affected staff member carries emergency communication equipment on their person including a personal duress alarm with person-down capability (as per chapter 11).
- Relocating the affected staff member to a different work area.
- Ensuring that the necessary file flagging and communication, regarding the risks, with other shifts occurs.
- Providing the affected staff member (and / or their family members where the threat arises from the staff member’s 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 should 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:

- Is the identity of the perpetrator known?
- Has the perpetrator got 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 was the threat made against (more than one person ie staff, family members etc)?
- How was the threat made (e.g. 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 (assault, sexual assault, death threat, did it include reference to weapons etc)?
- How long is the threat likely to pose a risk to the affected employee?
- 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 staff member 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 perpetrator have a known history of violence?
- Has the perpetrator made past attempts (successful or unsuccessful) to carry out the threat?
- Does the perpetrator have the means, access and/or opportunity to carry out the threat?
- Is it known if the perpetrator has access to firearms?

Sources of information in relation to the above may include the following:

- Treating clinicians.
- Staff members providing care to the person making threats.
- Family or other associates of the person making the threat.
- Security personnel.
- Incident 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 staff member.

- In addition to any immediate actions taken, other internal risk controls may include any/all of the following:
  - Providing on-going support to the affected staff member and providing assurance that their safety is of the highest priority.
  - Consulting with the affected staff member in determining any potential short and long term risk control options.
  - If an inpatient, transferring the patient to a different facility.
  - Formally advising the perpetrator that if they attempt to enter the particular facility, police will be immediately called.
  - Ongoing controlled access to, and/or security presence in, areas where the affected staff member is working.
  - In consultation with the affected staff member, relocating the affected staff member to a different work area or providing alternate duties until the risk subsides.
  - Having security personnel accompany the affected member to and from their car.
  - Considering leave options, if that is a staff member’s preferred option
  - Supporting application for an apprehended personal violence order (APVO).

- Where the risk assessment suggests the affected staff member 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 etc additional action may be necessary. Such action should be specific to the circumstances, be based on advice from police and be determined in consultation with the affected staff member.

- Depending on the seriousness of the threat, such action may include:
  - Arranging for a security risk assessment of the affected staff member’s accommodation.
  - Improving physical security of the accommodation premises.
  - Providing communication devices and/or personal alarms.
  - Relocating the affected staff member at the NSW Health Agencies cost until the threat subsides.

**NSW Health Policy Zero Tolerance Response to Violence**

NSW Health has adopted a policy of zero tolerance to all forms of violence in the health workplace.

The term ‘Zero Tolerance to Violence’ means that all actions, as far as practicable, will be taken to prevent violence, and that in all violent incidents, appropriate action will be taken to protect staff, patients and visitors from the effects of such behaviour.

This means NSW Health Agencies must ensure that all risks of violence and violent incidents need to be promptly, appropriately and consistently managed to prevent their occurrence, escalation and to minimise their impact on staff, patients and visitors. For further information please see the NSW Health policy ‘Zero Tolerance Response to Violence in the Workplace (Policy Directive 2005_315)."
Managing Post Incident Issues:
PD2014_004 Incident Management Policy provides direction to health services regarding the management of both clinical and corporate incidents, including the provision of appropriate feedback to patients, families/support persons and clinicians, and the sharing of lessons learned to prevent patient harm. This policy describes a statewide system for managing clinical and corporate incidents in order that health practitioners, managers and staff respond effectively to them.


*****
27. Armed Hold-Up

Policy:
NSW Health Agencies are required to ensure, in consultation with staff and other duty holders, that all reasonably foreseeable risks associated with threats with weapons are identified, assessed, eliminated where reasonably practicable or, where they cannot be eliminated, effectively minimised.

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

Standards:
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):

- Risk assessments include assessment of all vulnerable areas within the NSW Health Agencies, including but not limited to banks and retail outlets on site, ATMs, Emergency Departments, wards that could be perceived as having drug stores, community service staff and vehicles that could be perceived as carrying drugs, pharmacies, pharmaceuticals storage areas and cashiers’ counters to determine if:
  - The location of such facilities is secure and monitored by CCTV
  - Entries and spaces where a getaway vehicle may park are monitored by CCTV
  - Cash and accountable drugs are kept to a minimum within these areas and
  - The routes and times are varied when cash and drugs are conveyed to and from the facility
  (Refer to Chapter 5 of this Manual for more information on identifying security issues when leasing out or leasing premises).
- Ensure the duress alarm system does not make a noise when triggered (see chapter 11) as this could escalate an armed robbery into a hostage situation.
- Ensure procedures are in place for the safe transport of cash and drugs
- Ensure all drugs are kept in a locked cupboard, away from the line of site of patients and the public.
- Develop procedures in consultation with staff, security and WHS experts for the response to and management of incidents involving weapons including armed hold-ups. Procedures should be aligned with AS 4083 as amended from time to time.
- Ensuring that training is provided to workers on armed hold-up procedures and procedures for dealing with incidents involving weapons generally
- Reviewing current strategies to reduce security risks.

What to do in the Event of an Armed Hold-up:
- Local procedures, based on Appendix 27.1, must be developed and reflect the following elements:
  - Survival strategies for staff during an armed hold-up
  - Evacuation where appropriate
  - Details on who should be contacted in the event of an armed hold-up and when this contact should occur. Duress response teams must be trained to ensure they can adequately respond to this type of incident.
  - The role of NSW Health Agency staff and emergency services
- A nominated emergency co-ordinator and delegates (in the absence of the co-ordinator)
- Isolating the site
- Preserving the site following the incident.

A sample procedure has been included (Appendix 27.1) to this Chapter for the information of NSW Health Agencies.

Managing Post Incident Issues
PD2014_004 Incident Management Policy provides direction to health services regarding the management of both clinical and corporate incidents, including the provision of appropriate feedback to patients, families/support persons and clinicians, and the sharing of lessons learned to prevent patient harm. This policy describes a statewide system for managing clinical and corporate incidents in order that health practitioners, managers and staff respond effectively to them.


**********
Appendix 27.1

Sample Procedure

What to do in the Event of an Armed Hold-up in progress:
The protection of life is the most important consideration. Staff should not knowingly place themselves or anyone else at unnecessary risk.

- During an armed hold-up staff should:
  - Co-operate with the perpetrator’s instructions
  - Assume and behave as if the weapon is real or loaded
  - Remain calm, control emotions, avoid eye contact and make no sudden movements
  - If spoken to give a succinct reply in simple, plain English, and do not use words that may be confronting to the perpetrator.
  - Not attack the perpetrator or touch anything they may have handled
  - Note the perpetrator’s clothing and any other distinguishing features
  - Not challenge the perpetrator
  - Attempt to stay facing the person
  - Activate any alarm if safe to do so, noting that activating an audible alarm may escalate the incident.

- Where an individual comes upon an armed robbery in progress they must dial 000 and ask for the police or contact the nominated emergency co-ordinator at the facility and tell them:
  - The name, address and telephone number of the facility
  - The name of the person making the report and their position
  - The reason for the call
  - Whether the robbery is still in progress
  - The exact location of the robbery and the number of intruders
  - What the intruders looked like
  - What vehicles were used if known
  - What weapons were used

What to do immediately after an Armed Hold-up:

- After an armed hold-up the manager, or other delegated person of the affected area should:
  - Ensure that people requiring treatment are immediately taken to the Emergency Department
  - Alert EAP provider and arrange for provision of counselling.
  - Provide psychological and practical support for all staff and others involved in or witnessing the incident
  - Secure any relevant CCTV footage
  - Close the area where the robbery took place if possible and advise people not to touch anything at the scene
  - Ask all witnesses to wait for the police to arrive or ask for their name, address and telephone number if they insist on leaving
  - Provide witnesses with pen and paper and ask them to write down a description of events while waiting for the police.
  - Advise witnesses not to discuss the robbery until interviewed by the police
  - Ensure all witnesses are offered counselling. Witnesses who are staff of the NSW Health Agency can access their EAP or other post incident support services.
- Ensure media issues are appropriately managed and arrange an area where a press conference can be held if necessary
- Advise unauthorised staff not to speak to the media
- Ensure the names of injured people are not given to the media. Provide CCTV footage to police to aid investigation.

After an armed hold-up staff should:
- Dial 000 and ask for the police or contact the nominated emergency co-ordinator at the facility and tell them, as far as possible:
  - The name, address and telephone number of the facility
  - The name of the person making the report and their position
  - The reason for the call
  - Whether the robbery is still in progress
  - The exact location of the robbery and the number of intruders
  - What the intruders looked like
  - What vehicles were used if known
  - What weapons were used
- Look after others directly involved or affected by the hold-up
- Advise the manager/supervisor of the incident
- Activate any alarms, if safe to do so, if not previously activated
- Dial 000 and ask for the police or contact the nominated emergency co-ordinator at the facility and tell them:

What the designated Emergency Co-ordinator should do when they are advised of an Armed Holdup:
- Ask the facility switchboard to advise senior personnel on duty of the incident and to stand-by in case of injury
- Arrange to evacuate surrounding area if the hold-up is still in progress and post sentries to stop unsuspecting people walking into a dangerous situation
- Co-ordinate the scene until the police arrive
- Ensure a return to normal working practices as soon as possible

What security personnel should do during and after an armed hold-up:
- Observe from a safe distance, remain unobtrusive and where necessary evacuate the surrounding areas and post sentries to stop unsuspecting people walking into a dangerous situation
- Do not place themselves, or anyone else, at risk
- Keep onlookers away from the scene
- Sounds the alarm if it is safe to do so

What the switchboard operator should do during and after an armed hold-up:
- Ask anyone reporting a hold-up
  - His/her name
  - Location of the incident
  - If the incident is still in progress (if the incident is in progress police are to be advised on 000 immediately and other details gathered after)
  - If there are any injuries
  - The number of perpetrators, descriptions, direction and means of escape
- If the police have not been contacted dial 000 and ask for police. Tell them all the details that have been gathered from the person reporting the hold-up
- Report the hold-up to the emergency co-ordinator or the most senior member if the emergency co-ordinator is not on duty
28. Weapons are not to be Used by NSW Health Security Staff

Policy:

The issuing of any weapons, including batons and handcuffs, to NSW Health security 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.

Undertaking the role of a NSW Health security staff member does not require the member to carry weapons.

Furthermore, the presence of batons and handcuffs is not in keeping with the therapeutic environment security staff work within, and may aggravate situations with some patient groups.
29. Code Black Arrangements

Policy:
NSW Health Agencies are required to ensure that appropriate arrangements for providing a timely and effective response to code black situations (including response to duress alarms) are developed and implemented and regularly tested, in consultation with staff and other duty holders, and safety and security experts.

NSW Health Agencies are responsible for ensuring that staff members and others 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 PD2012_008 Violence Prevention and Management Training Framework.

Standards:
Despite all the strategies in place to minimise the likelihood of incidents occurring in NSW Health workplaces, incidents that require that an urgent team response is required by a staff member in the form of a Code Black response, can still occur.

It is important that all staff are aware that there is a range of options available when faced with violent events. These responses will depend on a number of factors including the nature and severity of the event, whether it is a patient, visitor, intruder or other person, equipment available to staff and the skills and experience of the staff involved.

One action available to all staff is triggering a duress response. This is referred to as a ‘Code Black’ and this term must be used where a staff member is facing a personal threat or physical attack (with or without a weapon involved) and is summoning assistance.

Separate response arrangements will need to be in place for other emergencies such as fire (Code Red), bomb threat (Code Purple), medical emergencies (Code Blue) and external emergencies (Code Brown).

All staff working in facilities should feel confident that when signalling a Code Black an effective response will be initiated. Staff must also be assured that it is better to trigger response/seek assistance early as this can prevent escalation.

Staff working in community/outreach (including domestic) settings 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 staff working in the community are confronted with a personal threat or attack.

Acceptance by managers that staff 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 Policy Zero Tolerance Approach to Violence in the Workplace.
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.

What is the aim of a Code Black response?
The aims of a code black response are to:
- Summon as a priority sufficient numbers of skilled multi-disciplinary personnel 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; and
- Demonstrate support for staff, patients and others in threatening or violent situations.

While the configuration of the Code Black Response Team and its options for managing an incident will vary from facility to facility depending on the availability of staff, the nature of the facility or unit within the facility and access to external services such as Police, all response plans must address the elements set out in the model Code Black Plan set out at Appendix 29.1.

The required reporting and recording of the incident must occur as soon as possible after the event utilising the local processes. Where the incident involved a patient information should be communicated to the medical officer in charge of the patient’s care, where they were not present during the incident.

Developing a Code Black response plan:
Code Black response plans must exist for all areas in a facility and must include:
- Consultation with staff, HSR/WHS representatives and security staff, during the development and review of Code Black response plans, must occur.
- The provision of appropriate personal protective equipment such as safety glasses to the Code Black Response Team.
- Identified escape routes and safe havens, and advice included to staff upon commencement of their engagement with the facility. In the event of community services they should be included in the patient care plan.
- The plan must be regularly evaluated and reviewed. Review must involve the input of all parties who may be involved in a Code Black response including external responders.

Elements of a suitable Code Black response:
- The response must be standardised as far as possible to reduce confusion.
- The response must reflect the available resources on each shift and in the local area, eg Police may not be available at night.
- The response must be tested via drills and a record of the drills maintained.
- The response must be as fast as possible.
- A quick and effective protocol for confirming that the response team’s attendance is needed, i.e. eliminate false alarms.
- The Code Black Response Team must have easy access to necessary equipment, as needed, such as safety glasses, gloves or mechanical restraints (for further information refer to Chapter 14 of this Manual).
- Procedures must include contingencies for the possibility of the simultaneous occurrence of Code Black situations.
- Procedures must clearly identify when, during the Code Black response the assistance of the Police should be sought, who in the Code Black Response Team makes that determination and how communication with the Police occurs.
• The response includes consideration of contingency plans while awaiting response.
• Procedures must ensure the availability of a suitable number of responders. Where staff numbers are limited or the facility is in a remote location, the limits of the options available to safely manage an escalating Code Black incident must be understood by team members eg restraint is not possible so the team will ensure staff and patients are moved to safety where a situation can not be de-escalated.
• In remote facilities where there are limited staff Code Black responses may include pre-arranged 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 SES. In these instances external responders must be able to quickly access the building, i.e. have their own codes or keys.
• Regular liaison with the local Police about facility and Police on-going cooperation should occur.

Training and practice
• The response must be regularly tested via drills and a record of the drills maintained.
• The Code Black Response Team must receive training together to ensure an understanding of roles, particularly as it relates to restraint.
• All Code Black Response Teams are Category 3 staff, as set out in the NSW Health Prevention and Management of Violence Training Framework, and as such must have completed all required training.

Code Black responders:
• Code Black responders must be identified for every shift.
• The code black responses must involve a multi-disciplinary team response with sufficient numbers of clinical and security or other personnel to provide for the safe management of a patient or another individual.
• Each shift must have a designated Code Black Response Team. Those on the Code Black Response Team must be able to cease their duties to respond when needed.
• The Code Black Response Team must include a delegated clinical leader and an agreed assembly point to muster prior to entering the area were the Code Black Incident is occurring and agreed single points of entry to each work area so the response to the incident proceeds in an ordered way with all members of the response pre-briefed and entering as a team.
• As part of the mustering, team members will discuss and be clear on who will bring the Code Black kit, who will communicate with the treating clinicians and establish any relevant information such as the patient’s legal status, undertake the initial assessment and direct actions upon arrival, who will commence and lead de-escalation/communication and any further action to occur and who will determine when the team will withdraw for their own safety.
• 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, hyperflexed joints and ensure the minimal amount of force only is maintained throughout the restraint.

Identifying responsibilities for all staff:
• The Code Black response plan must clearly state the responsibilities of all staff to:
  • Use personal protective equipment, safe havens and escape routes, as provided.
• Attend training in violence prevention and management and participate in Code Black drills as necessary.
• Fulfil any delegated role and responsibilities in the command, control and coordination of a Code Black response, and provide immediate advice to the appropriate person where there is an inability to perform the role eg illness or injury.
• Document involvement in the Code Black incident in accordance with procedures.
• Participate in any operational review and debriefing of a Code Black incident, and
• Cooperate with changes to procedures and any other preventive measures identified through any risk management or post incident investigation processes.

The Code Black response plan must clearly state the responsibilities of managers to:
• Ensure staff are given skills to identify early intervention opportunities in order to prevent escalation of the incident or where they need to activate a duress alarm, to prevent a delayed response to the incident.
• Ensure staff are given training so they are able to utilise the protocols for summoning assistance, and use any equipment, eg duress alarms including a ‘hands-on’ session with the actual equipment to be used.
• Ensure the release of staff to attend training and arranging the backfilling of positions as necessary.
• Ensure adequate numbers of staff are available to respond to Code Black calls and are able to leave their duties to respond when a Code Black incident is occurring.
• Contingency plans must be in place to ensure a Code Black response can still occur even where staff are absent and where there is more than one incident occurring simultaneously.
• Ensure staff are provided with post incident assistance, such as medical treatment or counselling if required.
• Ensure that incidents are reviewed to identify any additional controls needed to prevent re-occurrence of the incident type, or to identify improvements to the planned response.

Determining how staff will summon assistance:
Within a Code Black response procedure communication protocols should be included which:
• Determine, devices which best suit the local needs and contexts of the workplace (e.g. fixed or mobile duress alarms, mobile telephones, radios, remote geographic positioning duress beacons, etc).
• Provide clear instructions for staff on how to seek assistance and use the devices provided.

It should be recognised some areas of NSW will not have adequate duress signal strength or a response to a duress activation due to a number of factors that facility managers may have little or no control over, e.g. the remoteness and the ability of the service to accept advance technology, the terrain and the ability of the terrain to allow a uninterrupted signal to be sent, distances between the services measured against adequate response. Where this is the case other arrangements must be in place to allow staff to summon assistance.
Managing Post Incident Issues:
Code Black response plans must incorporate the need to record the details of code black call and the response provided.

NSW Health Policy Directive PD2014_004 Incident Management Policy provides standards for incident types that must be reported to the Ministry of Health and PD2005_234 Effective Incident Response Framework provide 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.


Post incident investigations and operational debriefs must consider information from all staff involved in the incident.

*******
Appendix 29.1

Model Code Black Response
(refer also to standards set out in the Emergency Procedures/Rainbow Chart)

Local Code Black Procedures must include the following elements:

- **Capacity to identify a situation / incident which requires a Code Black response:**
  - A Code Black incident is any incident where a staff member is facing a personal threat or physical attack (with or without a weapon involved).
  - A request for assistance from a staff member must be triggered early before things escalate.
  - There is a culture of no blame for staff members who feel threatened and call for assistance.
  - The roles and responsibilities of all staff (including managers) are set out.

- **Code Black Response Team Members:**

  **In hours:**

<table>
<thead>
<tr>
<th>Role in the Response Team</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  **After hours:**

<table>
<thead>
<tr>
<th>Role in the Response Team</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The procedure must identify what arrangements operate where another incident occurs prior to the Code Black Response Team completing the management of an incident.

- **Calling for Assistance  Simple and clear communication:**

  **Initiating a Code Black:**
  - There is a ‘one call’ or alarm trigger from the person calling for a response – through a duress alarm or telephone to a central co-ordinating person.
  - If through a telephone to a central co-ordinating person provide:
- Name and title
- Location of the incident
- Nature of the incident
- Whether the Police are required immediately

**While awaiting a response:**

- Department manager to ensure staff take action to protect themselves and others (ie moving out of the vicinity of the incident, or outside of the reach of the individual).
- Staff attempt to de-escalate the incident or keep the individual engaged if it is safe to do so.
- Staff to scan and assess the immediate environment to reduce risks, as a precaution.
- The clinical team leader ensures the treating team is paged and advised of incident.
- Ensure someone is available to meet the Code Black Response Team, direct them to the areas of the incident and provide known details of the incident.

**There is a planned team response:**

- There are sufficient numbers of personnel responding to meet needs and the scope of possible actions that can be undertaken by the Team eg if there are not sufficient numbers to undertake safe restraint then the team will assist in ensuring staff and patients are moved to safety where de-escalation has not been successful.
- Team is multidisciplinary (Medical / Nursing / Security / others).
- There is a designated clinical leader who is identified prior to any response.
- There is an agreed assembly point to enable a better co-ordination of response and avoid responding team members entering unsafe areas on their own or creating disturbance by entering from multiple doors.
- The clinical team leader ensures all designated team members are in attendance and informs an agreed person to followup on missing team members.
- Responders remove name tags/lanyards/pens/scissors/jackets etc that may be used as weapons or used to constrain them during the incident.
- Ensure arrangements are in place where there is a need to access medications (eg Code Black Drug Box)
- The procedure must set out the specific roles to be undertaken by members of the team during the incident management (medical/nursing/security) – this may be flexible if the individual appears to be engaging with a particular team member.
- All team members must act under the direction of the clinical team leader, unless they are incapacitated. There should be pre-arranged agreement on which team member is to be the second in charge.

**During the response:**

- There is an immediate assessment of the situation by the clinical team leader - is this situation appropriate for intervention by the team?
- The response team may decide not to intervene and call the Police and then the role of the team may be to keep others away from the area.
- There are protocols for likely events such as
  - De-escalation
  - Restraint (and options for continued management of patients & non-patients)
  - Sedation
  - Retreat
  - Securing the scene
  - Crowd security
  - Back up / hand over to security agencies
- The response team is stood down by the clinical team leader.
- There is clear documentation of the response and intervention recorded by a nominated team member and agreed by all team members as accurate.
- Data is kept on every code black response. Data to include the time the team were required to be in attendance.

Where incidents involve weapons, the role of the response team is to secure the area and prevent others from entering the area while awaiting the response from Police.

Staff should take note of details of the offender and, as far as practicable, not touch any items that may be required as evidence by the Police.

- **After the response:**
  - There are plans put in place for the on-going medical management of the person (if relevant).
  - There is a review of the code black response by the manager of the Code Black Response Team.
  - Where it involves a patient, note of the incident is recorded in the medical notes and communicated with the treating clinicians if they were not present.
  - All incidents must be entered into the incident management system (IMS).
  - There is a review of the incident.
  - Staff involved in the response, or affected by the incident, are offered support.
  - Recommendations from the investigation are implemented.

- **Training and practice**
  - The response must be regularly tested via drills and a record of the drills maintained.
  - The Code Black Response Team must receive training together to ensure an understanding of roles, particularly as it relates to restraint.
30. Effective Incident Management

Policy:
NSW Health Agencies are required to ensure that the mandatory standards outlined in Policy Directives PD2014_004 (Incident Management Policy) are implemented.

Standards:
PD2014_004 Incident Management Policy
The purpose of the Policy is to ensure a consistent and co-ordinated approach to the identification, notification, prioritisation, investigation, analysis, and action for all incidents. Requirements for undertaking Root Cause Analysis and generating Reportable Incidents Briefs to the Ministry of Health are also specified and must be observed.

Managing post incident issues:

This chapter should be read in conjunction with Chapter 29 (Duress Response Arrangements).

**********