# 16 Electronic health information management systems

The continued expansion and growth in digital technologies is aiding the development of many new electronic health information management systems to improve efficiency and quality of care within NSW Health.

Electronic health information management systems require robust security and governance policy and practices in place to maintain the integrity of the data and the trust of the people of NSW.

Such policies assist staff compliance with their privacy obligations and reduce the risk of privacy and security breaches through effective communication and management processes (see Section 14.4 Breach of Health Privacy Principle(s) by an employee).

The fundamental principles for management of, and access to, electronic health information management systems are provided below (see Section 16.3 Fundamental principles). These principles should be incorporated into local security and governance practices in order to maximise the benefits of electronic health information management systems and minimise the privacy and security risks.

When new electronic health information systems are being planned and designed, they should be subject to Privacy Impact Assessments (PIAs) to ensure privacy considerations have been addressed. This is particularly important where new technologies are to be introduced that impact treatment arrangements, for example, remote patient monitoring or use of vendor platforms to manage clinical images.

Health information about an individual must not be included in a health records linkage system unless express consent has been obtained. Exemptions exist where an entity may be lawfully authorised, or not required to comply. This extends to where the inclusion of the record falls under an exemption under HPP 10(1)(f) or HPP 11(1)(f).

*Further guidance:*

- IPC Guide to Privacy Impact Assessments

## 16.1 Electronic health records

Electronic health records differ from paper health records in ways that warrant special consideration. Firstly, it is possible to have a single electronic health record simultaneously accessible at multiple sites, giving more people access. Secondly, it is possible to control access to an electronic health record in ways that are not possible with a paper health record.

Health records in relation to a particular patient may consist of both hard copy (paper) and electronic health records (sometimes referred to as a *hybrid* record). When handling personal health information, it is important to consider whether relevant health information is held in the other format and whether both the electronic health record and the hard copy health record need review when making a decision about the health information contained in the records.

Electronic records may also include data collected for remote patient monitoring and data collected by vendor systems engaged for patient care purposes. Those arrangements will be subject to contractual arrangements that manage the access and security of health records, like any NSW health record.

## 16.2 Data collections and data warehousing

Data collections and data warehousing systems are subject to the *Health Records and Information Privacy Act 2002* and therefore Health Privacy Principles 10 and 11 regarding use and disclosure of personal health information will apply (see Section 11 Using & disclosing personal health information (HPPs 10 & 11)). There are a range of reasons why NSW Health will establish data collections, including:

- provision of clinical care to patients and in some circumstances their families
- public health surveillance
- performance monitoring
- service management and improvement
- service planning and policy development
- allocation of funds
- public accountability
- research in accordance with guidelines by the NHMRC (see Section 11.2.5 Management, training or research).

Health Privacy Principles 10 and 11 allow for the above uses of personal health information as they fall into the definition of a 'directly related purpose' (see Section 11.2.1 Directly related purpose) or meet the criteria for a management or research activity

(see Section 11.2.5 Management, training or research).

NSW Health data collections can often be based on statistical or other data and so may not include 'identifiable' information. Where identifiable information is not included, privacy laws do not apply (see Section 16.2.1 Identified and de-identified data).

### 16.2.1 Identified and de-identified data

Within some NSW Health data collections, data may be classified in various ways such as: fully identified data, semi-identified data, re-identifiable data and de-identified data.

For example, data can be classified as:

- Fully identifiable: required for patient care purposes and other secondary purposes
- Partially identifiable: may be used for management purposes, for example to group cardiac patients by condition, postcode, age group or sex for various management purpose including waiting lists, ward requirements, surgical access etc.
- Re-identifiable: this might be for hospital or ward operational reporting and will not identify an individual unless linked with other data (for example, date of surgery, hospital, address may be re-identifiable)
- Un-identified / fully deidentified: for certain research purposes and has been carefully stripped of all identifiers.

Whilst these may be valid and useful classifications for management of information, they are not used in the privacy laws. When considering the implications under privacy law for the access, use or disclosure of health information held in any context within NSW Health, regard needs to be had to the definitions of 'personal health information' used in the *Health Records and Information Privacy Act 2002*. These provide that 'information about an individual whose identity is apparent or can reasonably be ascertained from the information' is personal information and therefore regulated by the *Health Records and Information Privacy Act 2002*.

If there is a reasonable chance that the information is potentially identifiable, it will fall within the ambit of the privacy law controls, unless it is otherwise lawfully exempt.

Clearly, whether information can be considered de-identified will be dependent on the specific circumstances which arise in any disclosure.

Privacy laws and policies only apply to identified data (also see Sections 5.1 Health information, and 5.2 Personal information).

*Further guidance:*

- Section 5.3 De-identified information
- De-Identification Decision-Making Framework, OAIC and the CSIRO
- *Fact sheet: de-identification of personal information*, Information and Privacy Commission (IPC)
- Privacy issues and the reporting of small numbers, HealthStats NSW, NSW Health

## 16.3 Fundamental principles

Electronic systems facilitate access to personal health information. Staff and health providers should be aware of their obligation to restrict access to what is clinically necessary for patient care, or otherwise authorised under the law. Systems to audit user access and protect security to ensure compliance with these obligations should be in place.

The following principles provide guidance on how to address privacy issues when accessing electronic health information management systems, such as electronic health records, NSW Health data collections, and data warehousing systems.

### 16.3.1 Privacy and confidentiality undertakings for staff

Staff who have access to electronic health information management systems (eMRs) must sign a *NSW Health Privacy Undertaking* on employment and when gaining access to each eMR and other systems, outlining their responsibility to observe the Health Privacy Principles and duties of confidentiality.

A *NSW Health Privacy Undertaking* must be signed where staff, contractors, vendors and others are provided with extended or project access to health information management systems or other sensitive information in their employment.

The *NSW Health Privacy Undertaking* reminds staff about their obligations when accessing and using personal and health information in their day-to-day work.

### 16.3.2 Training and informing staff

Staff accessing electronic health information management systems must be informed and regularly reminded of their responsibilities in relation to patient privacy and confidentiality. This can be achieved through a combination of staff induction, staff meetings, training, staff newsletters, notices (including pop-up reminders in electronic systems) and posters.

Providing staff with brief privacy messages at critical decision points in the system may be an effective way of reminding staff of privacy obligations.

See section 6.1.4 Staff communication and alerts, for examples of electronic notifications for NSW Health staff about privacy obligations.

*Further guidance:*

- Section 6.1.2 Staff training
- Section 14 Complaints handling

### 16.3.3 Access protocols

The approval process for access applications to electronic health information management systems should have robust governance systems to minimise opportunities for inappropriate use and disclosure. Features of robust access protocols include:

- Access to electronic health information management systems should be provided on a 'needs only' basis. Consideration should be given as to whether access to de-identified data, or limited identified data, is sufficient for the staff member's work requirements.
- Where access to identifiable data is required, the purpose/business requirement should be documented as part of the access application.
- Access should be specific to job requirements or for the duration of a project, and then reviewed/renewed at appropriate intervals, depending on the business needs.
- Staff (and any other users) who are provided with access to any system containing personal health information should have a secure individual login which should not be shared. Health organisations should have processes in place to discourage the sharing of passwords. Sharing passwords significantly decreases security controls and exposes the health information to unauthorised access, use and disclosure. Generic passwords should only be used for systems which contain de-identified information, generally used for analysis and reporting.
- Robust processes must be in place for regular review of access arrangements for individuals, for example, where staff move into a new role access levels should be reviewed and if staff leave the organisation their logins to all systems, including remote access functionality, should be disabled.
- Clear criteria for approval for access to an electronic health information management system must be followed and documented, for example:
  - confirmation of each applicant's employment status and position
  - the name of each system to which access is to be provided and the associated level of access to be provided
  - confirmation that the application has been approved by the Line Manager
  - confirmation that each applicant/manager has provided requirements for access
  - confirmation that if access is for a specific project, the requested time period for access is appropriate to meet business needs and liaison with system administrators will occur to ensure access is reviewed as approved.

### 16.3.4 Auditing

Audit functionality is a mechanism which can be incorporated into electronic health information management systems holding personal health information.

Data quality which includes the completeness and accuracy of health information (both demographic and clinical) is an important principle in the management of health information (HPP 9). As part of audit functionality, electronic health information systems should have control mechanisms that assess and report on data quality.

Audit records of access to health records should be maintained on an ongoing basis. Audit reports and notifications should be generated regarding access to health records as required. Systems should be in place to appropriately manage security and minimise unauthorised breaches of access.

Key elements that support a robust audit process may include:

- The ability to run an audit report which identifies the name and ID of the user, their position/designation, and the name of the patient (and MRN) of the record accessed.
- The ability of any audit report to set out the time when access to a record commenced and ceased, and parts of the record that were accessed.
- Reminders to staff that audits are proactively conducted to promote privacy awareness and compliance. This might include auditing access to a VIP hospital attendance (politician, celebrity etc.) or a random patient sample.
- A protocol for managing privacy audits and potential staff breaches with appropriate thresholds for disciplinary referral.

Audit functionality may include:

- Creation of an audit record each time a user accesses, creates, updates or archives personal health information via the system.
- A log which uniquely identifies the user, the data subject (the patient), the function performed by the user, and the time and date at which the function was performed.
- When a record is updated, a record of the original data, who entered the new data, and the time and date, should be retained.
- A log of message transmissions containing personal health information.

The organisation should carefully assess and determine the retention period for these audit logs, with particular reference to clinical professional standard and legal obligations, in order to enable investigations to be carried out when necessary.

### 16.3.5 Informing patients

Patients should be made generally aware that their personal health information will be managed using electronic systems, and that systems are in place to prevent unauthorised access to information held in these systems. This is included in the *Privacy Leaflet for Patient.*

*Further guidance:*

- Section 9.2.3 Computer systems and applications
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)

## 16.4 *Evidence Act 1995*

The *Evidence Act 1995* does not preclude electronic records being used as evidence unless their veracity can be questioned. To minimise the possibility of records converted from paper being open to challenge, the equipment and scanning processes must be capable of scanning to 100% accuracy with no possibility of corruption or manipulation of images. Control processes should be implemented to ensure that images cannot be altered between scanning and storage or while stored. Scanning processes should include quality control checking mechanisms to ensure the captured image is legible and reproducible.

## 16.5 Accountability

Information accountability means that the use of information should be transparent, so it is possible to determine whether a particular use is appropriate and in accordance with the 15 Health Privacy Principles, and that the system enables individuals and health services to be held accountable for any misuse of information.

Accountabilities should be clearly articulated for the system which delivers the record to ensure the integrity of electronic health records. Backup and recovery solutions are required in case of disaster.

Whoever enters the information into the health record is accountable for the accuracy of the information. Some staff will have additional responsibility for ensuring the overall accuracy of the health record and the care with which the details have been documented.

## 16.6 Access and quality control

The area over which the electronic health record is available is important, for example, individual facility, campus or health service. The broader the system, the greater the need for tighter network and access controls.

Where the electronic health record system covers multiple facilities, the health records may contain a mix of entries from different sources or partial copies of health records from other facilities. The ability to maintain a single, logical health record in this situation is critical. This can be achieved through various means such as individual patient identifiers, employee numbers, appropriate labeling of each transaction and adequate version control. Identification and authentication of the person making the entry is important.

Electronic health records should are to meet the same records documentation quality standards and requirements as paper records, for example, when clinical inaccuracies are identified in the health record, the inaccurate data should not be deleted. The original data must be retained as a contemporaneous record, flagged that it has been identified as inaccurate and the amendment entered as a dated notation, making the record complete and accurate. This is different from corrections (or updates) that may relate to changes in demographic data, for example, or information that has been incorrectly attached to the wrong patient's record (where to retain the information in the wrong electronic record could potentially breach patient privacy). Governance processes should be in place to manage the different clinical requirements for the management of errors and amendments.

## 16.7 Patient access

It is important to ensure that the right of patients to access their own health records is not compromised by the introduction of electronic health records. Health facilities should have local policies, compliant with privacy obligations which allow patients access to their health records. Technologies in some circumstances allow some patient-facing capabilities, for example portals and smart phone applications, which allow patients to view subsets of their own information.

Electronic health records should be retained in compliance with the *GDA-17-General Retention and Disposal Authority Public health services: patient/client records*. Fees and charges raised for access to health information should be consistent with NSW Health policy.

Adequate viewing, printing and copying facilities should be readily available. All requests for access to health information must be in accordance with Health Privacy Principles 6 and 7 (see Section 12 Patient access and amendment).

## 16.8 My Health Record

NSW Health services have access to the My Health Record system via HealtheNet, subject to access controls that may be set by the patient. The *My Health Records Act 2012 (Cth)*, regulates most aspects of My Health Record. NSW Health organisations are subject to mandatory data breach notification requirements for breaches relating to the My Health Record. Health services are required to notify the Australian Digital Health Agency of data breaches involving My Health Record.

### 16.8.1 Mandatory security and access requirements

All health services must ensure that their local processes comply with the Policy Directive *My Health Record Security and Access (PD2019_054)* in relation to the following:

- Information security, privacy, and access controls must be in place.
- Access to the My Health Record System for NSW Health purposes must only occur through NSW Health's HealtheNet Clinical Portal.
- Access to My Health Record is auditable via HealtheNet.
- Districts are strongly encouraged to maintain records of the individuals who have access to and/or received training to access the My Health Record system.
- If a patient requests that documents relating to a particular episode of care not be uploaded to My Health Record, the documents must not be uploaded.

***Further guidance:***

- *My Health Record Security and Access (PD2019_054)*
- *Office of the Australian Information Commissioner, 'Guide to mandatory data breach notification in the My Health Record system'*
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)
- Section 13.3 Linkage of health records (HPP 15)
- *NSW Health Electronic Information Security Policy Directive (PD2020_046)*
- *Health Care Records – Documentation and Management (PD2012_069)*