16 Electronic health information management systems

The continued expansion and growth in global technologies is aiding the development of many new electronic health information management systems to improve efficiencies 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.

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 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.

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 11.2.4 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 11.2.4 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.

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 HRIP Act. 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 HRIP Act.

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

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 (eHRs), NSW Health data collections, and data warehousing systems.

16.3.1 Privacy and confidentiality undertakings for staff

Staff must sign a privacy undertaking on employment and when gaining access to electronic health information management systems (see Appendix 3) outlining their responsibility to observe the Health Privacy Principles and duties of confidentiality. Where staff are provided access to a number of health information management systems, each system should be clearly identified in the privacy declaration.

16.3.2 Training and informing staff

Staff accessing electronic health information management systems must be informed and regularly reminded of their responsibilities to patient privacy and confidentiality. This can be achieved through a combination of staff induction, staff meetings, training, staff newsletters, notices, posters, and so on.

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

Some examples of electronic notifications for NSW Health staff are:

> Example: "Remember you must only access the information necessary to fulfil your work duties. If in doubt, check with your senior manager, or for further information go to: www.health.nsw.gov.au/patients/privacy/Pages/default.aspx"

Example: “You are bound by strict privacy law and NSW Health privacy policies regarding access to, use and disclosure of the personal health information contained in <ABC> system. The principal governance policy governing <ABC> system is: <XYZ>
The principal privacy policy is: NSW Health Privacy Manual for Health Information.
The principal privacy law is: NSW Health Records and Information Privacy Act 2002

Example: “If you suspect a breach of the privacy or security of the <ABC> system, you should discuss this with your manager, and consider contacting the Privacy Contact Officer for your organisation. Details are available at: www.health.nsw.gov.au/patients/privacy/Pages/privacy-contacts.aspx”

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 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 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 log-ins 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 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. 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:

- Name and ID of employee or contractor
- Position or designation of employee or contractor
- Name and MRN of health record accessed
- Date and time access commenced
- Date and time access ceased
- Section(s) of the health records viewed
- Where possible, Device ID (eg. MAC ID and IP Address)

Audit functionality may include:

1. Creation of an audit record each time a user accesses, creates, updates or archives personal health information via the system.

2. 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.

3. When a record is updated, a record of the original data, who entered the new data, and at which time and date, should be retained.

4 A log of message transmissions used to transmit messages 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 pro forma Privacy Leaflet for Patients (see Appendix 5).

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, i.e. 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 meet the same records documentation quality standards and requirements as paper records, for example, when 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.

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. Electronic health records should be retained in compliance with the State Records General Disposal Authority (GDA) 17 Public Health Patient 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 & 7 (see Section 12 Patient access and amendment (HPPs 6, 7 & 8)).

16.8 National eHealth Record

The National eHealth Record, also known as the Personally Controlled Electronic Health Record (or PCEHR), is being trialled by the Commonwealth Government Department of Health, as an optional way for patients to view a summary of their health records online.

Participating NSW Health agencies will make health information available to the health providers which individuals have authorised as part of the eHealth Record program.

It is not intended that the eHealth Record will replace, or should be relied upon in place of, health records maintained by a health service. The purpose of the eHealth Record is to provide individuals with an online tool to manage and view a summary of their health records in accordance with Commonwealth eHealth policy.

For further information, go to: www.ehealth.gov.au

Further guidance

- Section 9.2.3 Computer systems and applications
- Section 11 Using & disclosing personal health information (HPPs 10 & 11)
- Section 13.3 Linkage of health records (HPP 15)
- PD2013_033: Electronic Information Security Policy – NSW Health
- PD2012_069: Health Care Records – Documentation and Management