9 Retention, security and protection (HPP 5)

HPP 5 deals with the management of personal health information while it is held by a health service. It requires that:

- the information is **kept for no longer than is necessary** for the purposes for which the information may lawfully be used
- the information is **disposed of securely**
- the information should be protected, by taking such **security safeguards** as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse.

9.1 Retention and disposal of personal health information

HPP 5 operates subject to other lawful requirements. As public sector agencies, health services are subject to the requirements of the *State Records Act 1998*. That Act has extensive provisions as to the minimum length of time public records should be retained.

Health services should therefore refer to relevant General Disposal Authorities (GDA 17, 28, 36 and 42) issued by State Records NSW in determining how long to retain and how to dispose of health records.

Further guidance:
- PD2012_069: Health Care Records – Documentation and Management
- PD2013_033: Electronic Information Security Policy

Available from State Records NSW at www.records.nsw.gov.au

- General Disposal Authority No. 17: Public health services: Patient/Client records
- General Disposal Authority No. 28: Administrative Records
- General Disposal Authority No. 36: Imaged or microfilmed records
- General Disposal Authority No. 42: Public Health Services: general practice records

9.2 Security of personal health information

HPP 5 requires personal health information must have appropriate security safeguards to prevent unauthorised use, disclosure, loss or other misuse. What will be considered appropriate will vary depending on the way information is being stored and used.

NSW Health has a range of policies to ensure appropriate levels of security are in place, depending on the nature of the information and the way it is stored.

Further guidance
- Section 13.3 – Linkage of health records (HPP 15)
- Section 16 – Electronic health information management systems
- PD2013_033: Electronic Information Security Policy – NSW Health
- PD2009_076: Use and Management of Misuse of NSW Health Communications Systems
- NSW Premiers Circular No. M2007-04: Security of Electronic Information

9.2.1 Hard copy health records

9.2.1.1 Storage

Hard copy health records containing personal health information should be kept in lockable storage or secure access areas when not in use. Precautions, such as not storing health records containing personal health information in a public area should be taken, where practicable. Care should be taken not to leave documents containing personal health information on work benches or anywhere they may be visible or accessible to unauthorised people, including clinical areas, meeting rooms and publicly accessible areas.

9.2.1.2 Access at patient bedside:

Where practicable, health records should not be left at the patient bedside and where health records are held at the patient bedside they should be limited to what is necessary for safe patient care, for example, medication and observation charts and care plans. Detailed clinical notes and results reports such imaging and laboratory reports should always be retained securely at the Nurses' station.

Any bedside health record remains confidential. Access to these health records by the patient is only permitted with supervision by clinical staff. This is to assist staff to provide the patient with a full explanation about their health information contained in their health record and to avoid potential misunderstandings or misinterpretation arising with regards to their diagnosis and treatment.

Access to health records by family or other visitors is only permitted with supervision by clinical staff and with consent from the patient (or their authorised representative). Such consent should be documented in the health record.

If the patient, family or other visitors request further access, including copies of the health record, they should be referred to the Health Information Service (also see Section 12 Patient access and amendment (HPPs 6, 7 & 8)).

Staff should take reasonable steps to ensure it is clear that health records held at the patient's bedside are confidential and should not be accessed when clinical staff are not present. Placing a prominent notice on the front of health records held at the patient's bedside is an example of one strategy to manage privacy. See Appendix 4.3 for sample wording.

9.2.1.3 Disposal

Paper records containing personal health information should be disposed of by shredding or pulping, in accordance with the provisions of the *State Records Act*. Where large volumes of paper are involved, specialised services for the safe disposal of confidential material should be employed, and certificates of disposal obtained from the contractor.

Further guidance

- Section 9.1 – Retention and disposal of personal health information

9.2.2 Images and photography

Privacy rules only apply to personal health information where the identity of a person is reasonably ascertainable (in this case, from an image). Images referred to in this section do not include diagnostic imaging, such as x-rays or MRI scans.

Further guidance on the use of images for education or conference purposes see:

- Section 9.2.7 Training and presentations
- Section 11.2.4 Management, training or research

In certain clinical contexts, the recording of patient images may be required for the care and treatment of a patient. Some examples include:

- photographing burns, wounds, cancers, or congenital conditions to monitor response to treatment
- audio-visual recording of patients under clinical observation

It is important that the equipment used is appropriate for the purpose, for example, has the necessary level of resolution and quality to meet the clinical purpose. In relation to certain types of service situations, additional security and personal privacy issues may also arise.

For this reason, health services should consider adopting local protocols and policies. These can address these issues, including identifying the type of equipment appropriate or authorised for use in different clinical settings, and provide guidance to ensure images are captured and stored in the ongoing health record.

From time to time, emergency situations may arise where a personal device is used to capture and store images and health information for clinical use, due to the urgent need for care or treatment or advice. In such situations, staff should take particular care to transfer all data from the device to the local health records management system, in accordance with local health records management policy. The image must then be permanently deleted from the personal device.

Patient consent is not required where the capturing of images is a necessary part of diagnosis or clinical care or treatment. However, where practicable, the patient should be made aware that this is to occur, or has occurred, and the reasons why it is clinically necessary.

Staff should consult with:

- **Health Information Service** for assistance with local image management and medico-legal requirements.
- **Information Technology Department** for guidance on local image management, technical and security provisions.
- **Sexual Assault Service** with regards to images of injuries sustained by victims of sexual assault.

Photographic and audio-visual images, whether reproduced in hard copy or maintained in digital format, form a part of the patient's personal health information and as such are part of the health record. The health service must therefore provide for the secure storage, access to, use and disclosure of, these health records. The photographic image/audio-visual image should be linked to, or stored in an electronic health record system. If this is not possible, digital images should be securely stored, indexed and be easily accessible and retrievable.

The use of personal smart phones (or other personal devices) by staff to capture images of patients for non-clinical purposes is generally not permitted. The NSW Health Code of Conduct and other policies provide some guidance in this area.

Further guidance

- NSW Health Code of Conduct, Section 4 (regarding use of social media)
- NSW Government Social Media Policy & Guidelines, available at: www.advertising.nsw.gov.au/strategic-communications/social-media-policy
- Australian Medical Association: Clinical images and the use of personal mobile devices, available at: https://ama.com.au/article/clinical-images-and-use-personal-mobile-devices

9.2.3 Computer systems and applications

The Electronic Information Security Policy – NSW Health (PD2013_033) supports NSW Health in meeting its obligations for protecting personal health information.

Reference should also be made to the local security rules for computer systems and applications, including electronic health information management systems (see Section 16 Electronic health information management systems).

Staff with access to electronic applications, such as an electronic health record, may only access, view and use the system for purposes directly related to their work.

NSW Health staff may only view, access, use and disclose personal health information when it is necessary for them to do so to carry out their work duties.

If in doubt, staff should seek advice from a senior manager, local Health Information Service or Privacy Contact Officer. Staff should be provided with the appropriate level of access to physical and electronic health records (i.e. full, partial or no access) in accordance with their role and their work requirements.

Subject to the specific NSW Health policies on security of personal health information stored in an electronic environment, key privacy factors arising from HPP 5 are:

9.2.3.1 Storage

A secure physical and electronic environment should be maintained.

Further guidance

- Section 16 Electronic health information management systems

9.2.3.2 Employer-owned portable media

The storage or transfer of personal health information on portable media such as USB, CD, or laptop should be limited to employer-owned media, and should be on a temporary needs basis only. Reasonable steps must be taken when storing or transferring information in this way to reduce the risk of unauthorised access to the information, such as developing password entry into documents or systems.

For guidance on health information held on a personal device, such as a smart phone, see Section 9.2.2 – Images and photography

9.2.3.3 Disposal

Authorised disposal of health records should be done in such a way as to render them unreadable and leave them in a format from which they cannot be reconstructed in whole or in part.

Personal health information must be deleted from hardware, (including computer hard drives, printers and photocopiers) before being recycled, disposed of or sent back to a leasing agent or contractor.

Health services should ensure secure removal of the hard disk drive (HDD) from redundant PCs by designated staff. The contents should then be disposed of securely and safely by, or on behalf of, the health service. A Certificate of Destruction should be retained to confirm secure destruction.

Storage and disposal of electronic health records must be in accordance with the State Records Authority disposal and retention requirements.

Further guidance

- Section 9.1 Retention and disposal of personal health information
- Section 16 Electronic health information management systems

9.2.4 Safeguards when delivering and transmitting information

Health services should first ensure the proposed use or disclosure is authorised under HPP 10 (Use) or HPP 11 (Disclosure).

If the use or disclosure is authorised the following minimum standards should be applied when providing the information. Requirements necessary to maintain secure delivery will vary depending on the medium of transmission of the information.

9.2.4.1 Telephone

Personal health information, including admission and discharge dates, should not be given over the telephone unless it has been established that the caller has legitimate grounds to access the information and their identity can be confirmed.

- Only those authorised by the health service should give patient information by telephone. It is a matter for local determination which staff members should be so authorised.
- Personal health information should not be left on voice mail. The caller's name or the clinician's name and contact number may be provided where the patient is likely to recognise the name. Otherwise, the name of the health service may be used, if applicable.

9.2.4.2 Use of Short Message Service (SMS)

SMS may be used for communication with patients for administrative purposes, for example, to confirm an appointment, to request that the patient contacts the health service, etc.

Where patients agree to being sent their test results by SMS, health services are increasingly using SMS as a standard practice of communication with patients, including, for example, Sexual Health Services.

Even where SMS communication is standard practice, patients should, if they request it, be given other options to receive information or results.

9.2.4.3 Facsimile

Some patient information is still provided by facsimile (fax). The following steps are recommended when sending personal health information via fax:

- Fax machines used for transmission of personal health information should be secure for example, they should be located so that only authorised persons can access documents.
- Fax cover sheets should carry an appropriately worded privacy notice. See Appendix 4 for sample wording.
- The fax number should be carefully checked, and if there is any doubt as to whether the number is correct (the number may be hard to read or has not been used for a considerable time) the recipient should be contacted to confirm it.
- Store regularly used fax numbers in the fax machine's memory. Stored numbers should be checked on a regular basis to ensure they are current.
- When using a new fax number or sending to a new or unfamiliar recipient, consider telephoning the recipient prior to sending a fax.

9.2.4.4 Mail

- Packaging of mail and courier items should be secure and care should be taken that addresses are complete and correct.
- Mail should be marked 'Confidential: Attention …'
- Consideration should be made as to whether it is appropriate to use envelopes displaying the health service's details. For example, health services may wish to consider using unmarked envelopes where mail is sent to patients receiving health services which they may wish to keep confidential from other persons who may access a shared mailbox.

9.2.4.5 Transmission of electronic documents (discharge referrals/ summaries)

NSW Health has a number of systems which generate electronic documents (e.g. discharge summaries and referrals (eDRS)) to external health care providers (such as general practitioners, specialists and allied health care providers), as part of providing ongoing care in the community. These systems rely on the accuracy and currency of the providers nominated by patients to receive information. Given this, health staff should:

- check the accuracy of patient information updated in auto populated fields (including current address, GP, authorised representative) at each admission
- have processes in place to manage a consistent and single source of general practitioner, specialist and other community providers' details at the health service level
- record accurate and complete community provider details
- have processes in place to authenticate and monitor the accuracy of service provider details and to update this data on a regular and frequent basis
- provide all relevant staff with education and training on their data collection responsibilities and the importance of policies and procedures in relation to provider details
- include an appropriate privacy notice in each transmission message (see Appendix 4.2).

9.2.5 Use of email

9.2.5.1 Email within NSW HealthNet

NSW HealthNet comprises electronic transmission within NSW Ministry of Health, agencies and health services comprising NSW Health. Email within NSW HealthNet is generally secure however, staff must take care to comply with local health information policies when sending personal health information via email.

In order to provide adequate security of personal health information, the following security measures should be considered:

- Use of email should not replace the recording of personal health information in electronic or paper health care records. However, an email containing health information used for the purposes of providing treatment or ongoing healthcare is likely to constitute a health record, in which case the email should be incorporated into the patient's health record.
- The subject title of emails which include personal health information should include 'Confidential'.
- Emails which include personal health information must include patient identifiers to ensure that the content of the email, or the email itself, is filed against the correct patient. The national standard for patient identification requires that the following details are provided in all circumstances when referring to a patient: patient's name, sex, date of birth, and Medical Record Number (MRN).
- As with all use of personal health information, only include health information which you know to be required for the purpose of the email communication.
- Double check that the email address is correct. Wherever practicable, request that the recipient provides you with their email address by emailing you first.
- Take particular care not to inadvertently copy unintended recipients when sending the email.
- Exercise caution when using the 'Reply All' function. Always check that it is appropriate for the content of your email to be provided to recipients.
- Password-protection or encryption of personal health information for emails sent within NSW Health for purposes outside of patient care, for example, for health service funding, insurance or other management purposes.

For guidance on health service activities which are considered to be directly related to patient care, see Section 11.2.1 Directly related purpose.

9.2.5.2 Email external to NSW HealthNet

The NSW Health Electronic Information Security Policy states that transmission of personal health information to destinations external to NSW Health are not considered secure, and should be password-protected or encrypted prior to transmission in accordance with local health service policy.

Care should be taken to avoid including patient details in the email subject title or text. The recipient should be made aware of the password via telephone or separate email.

Emails and attachment containing personal health information should be deleted from the recipient's inbox (and trash emptied) within a reasonable timeframe.

Further guidance

- Electronic Information Security Policy (PD2013_33)
- Communications – Use & Management of Misuse of NSW Health Communications Systems (PD2009_076)

9.2.6 Printing and copying

The more copies of personal health information that exist, the more likely it is that a breach of privacy may occur or that the incorrect version will be used. For this reason health records containing personal health information should not be copied or printed unless it is essential to do so.

When printing documents containing personal health information, the person printing should personally remove the document from the printer. If personal health information is printed regularly, consideration should be given to placing a dedicated printer in a secure area. This will minimise the chances of inadvertent access by unauthorised people and counteract the danger of print jobs being lost in large print buffers.

9.2.7 Training and presentations

The anonymity of patients should be maintained during case presentations, demonstrations, research activities and at seminars and conferences. Where possible, fictitious data should be used.

Consideration should be given to de-identification of photos, slides and other visual aids. When identification of individuals is necessary, the consent of the patient should be obtained.

Identifiable and potentially identifiable information can be used in limited circumstances for training purposes, including those involving clinical placements, and only in compliance with NSW Privacy Commissioner's Statutory guidelines on training. Staff should also seek advice from their local Privacy Contact Officer.

Further guidance

- Section 11.2.4 – Management, training or research
- NSW Privacy Commissioner's *Statutory guidelines on training*: www.ipc.nsw.gov.au/privacy/ipc_legislation.html

9.2.8 Conversations

It is important to ensure that patient information is not discussed in public areas such as corridors or lifts or anywhere where it is likely to be overheard.

Meetings to discuss patients should not be held in coffee shops, cafeterias or other public areas.

9.2.9 Visibility of computer screens

Users should be mindful of using electronic devices that contain and display health records in public areas, and where possible, ensure that the computer screen cannot be seen by anyone other than the user.

If left unattended, the computer screen should be locked to limit access to personal health information. Screen savers and locks should be used where possible to reduce the chance of casual observation.

9.2.10 Whiteboards, patient journey boards, etc. in public view

It is common practice to display limited personal health information about patients on wards using a whiteboard, electronic board, patient journey board, and so on. The purpose for displaying patient information

in this way is to enable staff to deliver safe and efficient clinical care for patients. Displaying limited personal health information in this way enables fast and effective communication between staff.

Care must be taken to limit the display of personal health information to what is essential for this purpose, for example, to include surnames only, to exclude diagnosis, and where possible to use colours, symbols or abbreviations which are easily recognisable to staff. Clinical information should remain in the patient's health record.

The use of whiteboards, patient journey boards, etc. in public view, should be supported by written business rules to ensure appropriate use at all times, and appropriate governance to ensure compliance with privacy requirements.

Further guidance

- 'Patient Journey Boards: Balancing Clinical Benefit and Privacy Obligations', available at: www.health.nsw.gov.au/wohp/pages/patientjourney.aspx