Privacy Controls in the Personally Controlled Electronic Health Record (PCEHR)

nehta | eHealth

→ | Access Controls

Access to information within the PCEHR System will be moderated by a series of access controls managed by the individual. These include:

Establishing an access list – this is a list of organisations that are permitted to access an individual's PCEHR. An individual can control how an organisation is added (or removed) from the list.

Setting basic access controls – these controls enable all healthcare organisations involved in providing healthcare to the individual to access the individual's PCEHR.

Setting advanced access controls – these controls include setting up a Provider Access Consent Code (PACC) without which access to the individual's PCEHR is not possible, except in an emergency; restricting organisations from being on the access list; and managing document level access.

Emergency Access - access controls may be overridden in situations where the individual requires emergency care, in line with current laws and practices.

→ | Document Controls

Clinical documents will be uploaded to an individual's PCEHR unless an individual asks for them not to be uploaded. Although the onus is on the individual exercise this option, healthcare providers should be conscious of whether a clinical document may or may not be suitable for uploading or is likely to be sensitive to the individual concerned.

If a clinical document is loaded to an individual's PCEHR and the individual would like it to be removed, they may request the clinical document to be 'effectively removed' from their PCEHR. This means that the document is no longer visible but remains available for forensic purposes only within the bounds of the PCEHR legislation.

An individual can protect certain documents on their PCEHR from being viewed by establishing document access settings. Access controls can allow those documents considered sensitive by the individual to only be seen by a limited group of healthcare providers chosen by that individual. If an individual does not wish to restrict their PCEHR in any way, access will essentially be open to any healthcare providers legitimately involved in their care.

→ | Participation

The PCEHR System is a voluntary opt-in system with individuals being able to withdraw their participation at any time.

Individuals who wish to register for a PCEHR will need to have a verified Individual Healthcare Identifier (IHI). An IHI is automatically assigned to individuals who have an active Medicare or Department of Veterans' Affairs (DVA) enrolment. The small percentage of the population who are not enrolled in these programs will be able to get an IHI by visiting a healthcare professional or by applying to the HI Service Operator, Medicare Australia.

Individuals who decide not to have a PCEHR will not be disadvantaged in terms of being able to access healthcare services.

Healthcare organisations can choose to participate in the PCEHR system and will need a healthcare organisation identifier (HPI-O). They must agree to use appropriate authentication mechanisms to access the PCEHR and use software that has been conformance tested to be used with the PCEHR system.

→ | Security

Privacy and security are critical aspects of the PCEHR System. In order for the system to deliver the improved health outcomes that it promises to deliver, it must be trusted by its users. Here are some of the technical and non-technical controls by which security is maintained within the PCEHR system:

- Governance - all participants and organisations comply with relevant rules, specifications and laws
- Authentication of users accessing the PCEHR System.
- Robust audit trails - the PCEHR System will record details of every access made to an individual's PCEHR. Individuals will be able to view this information through an online audit record and make enquiries and complaints should they suspect that their record has been accessed inappropriately.
- Proactive monitoring of access to the PCEHR System to detect suspicious or inappropriate behaviour.
- Rigorous security testing, to be conducted both prior to and after commencement of operation of the PCEHR System.
- Education and training of users of the system.

Privacy Controls
in the
Personally Controlled
Electronic Health Record
(PCEHR)

Legislative Privacy and Security Controls

→ | Penalties

The *Personally Controlled Electronic Health Records Bill 2011* **(Draft Bill)** sets out civil penalties for any unauthorised collection, use and disclosure of health information contained in a person's PCEHR. These civil penalties will apply to individuals as well as other entities, including corporations.

Some penalties incorporate fault elements. For example, the fault element in section 51 is designed to ensure that liability does not arise where there is inadvertent or mistaken access to a person's PCEHR. The Draft Bill does not affect any existing criminal laws.

In addition, an act or practice that contravenes the Draft Bill in connection with a consumer's health information included in a consumer's PCEHR would be taken to be an interference with privacy for the purposes of the *Privacy Act 1988* (Cth). This would enable complaints to be made to the Office of the Australian Information Commissioner.

→ | Permitted Collection, Use & Disclosure

All the permissible collections, uses and disclosures of health information in a consumer's PCEHR are listed in the Draft Bill. If it is not listed in Part 4, Division 2 of the Draft Bill, it is an unauthorised handling of that information.

Participants in the PCEHR system are only permitted to collect, use or disclose the health information in a consumer's PCEHR where:

- such collection, use or disclosure is for the purpose of providing healthcare to the consumer and is consistent with the access controls set by the consumer;
- the consumer consents;
- the consumer would have reasonably expected this collection, use or disclosure;
- it is necessary to lessen or prevent serious threat to life, health or safety; or
- it is authorised by law.

→ | PCEHR System

The PCEHR system will not replace or hold all the information contained in healthcare providers' records. Instead, the PCEHR system will draw upon information held in conformant repositories (held in Australia only) to provide a summary view of a consumer's key health information.

An entity which operates a conformant repository will be required to apply to the PCEHR System Operator to register as a repository operator and will be subject to stringent requirements. The data held within the PCEHR System is subject to the *Privacy Act* alongside the PCEHR legislation. The Draft Bill defers to existing privacy laws in respect of data held in local systems.

→ | Governance

The Draft Bill sets out the governance arrangements for the PCEHR system, establishing the System Operator and two advisory bodies. The Draft Bill states that the System Operator will initially be the Secretary of the Department of Health and Ageing or another body established by the regulations. The advisory bodies and their functions follow:

- The **jurisdictional advisory committee** will advise the System Operator on matters relating to the interests of the Commonwealth, states and territories, and any other functions which are prescribed by the regulations. The jurisdictional advisory committee will ensure state and territory involvement in the operation of the PCEHR system.
- The **independent advisory council** will advise the System Operator on matters relating to the operation of the system, and in particular consumer security, privacy and clinical matters relating to its operation, from the perspective of the stakeholders' fields of experience. It will ensure the involvement of key stakeholders, including consumers and healthcare providers and the provision of key expertise in the operation of the system.

The Exposure Draft PCEHR Bill
was introduced 23 November 2011.

This fact sheet was correct at 1 December 2011.

→ **For up to date information about privacy protection in the PCEHR, please contact NEHTA at:** admin@nehta.gov.au