Obligations and Compliance Requirements - PCEHR Regulatory Framework

The information below highlights key obligations and compliance requirements for healthcare provider organisations under the PCEHR regulatory framework.

The full requirements for participating in the PCEHR system are set out in the PCEHR Act and Rules.

1. PCEHR Act

The PCEHR Act is available at: http://www.comlaw.gov.au/Details/C2012A00063.

The Act establishes the PCEHR System Operator, who is responsible for the operation of the system, and PCEHR advisory bodies. It provides for a framework to allow for the registration of consumers and other entities, specifying eligibility criteria, authorising them to participate and imposing obligations on them to maintain the security and integrity of the PCEHR system. It prescribes the circumstances in which registered entities can collect, use and disclose information in consumers' PCEHRs.

The Act allows for a range of remedies, including civil penalties, where there is an unauthorised use, collection or disclosure of information in a consumer's PCEHR or where certain actions occur that might compromise the integrity of the PCEHR system (see list of penalties below). The Information Commissioner (see http://www.privacy.gov.au/law/other/the-ehealth-record-system) is able to investigate any interference with privacy.

Penalties

The PCEHR Act includes a number of provisions with civil penalties; those relevant to healthcare provider organisations are:

- sections 59 and 60 – unauthorised collection, use or disclosure of health information in a consumer's PCEHR; $13,200 (individual) $66,000 (body corporate) – noting that the fault elements ensure that participants who inadvertently or mistakenly access a PCEHR do not contravene the provision.;
- section 74 – providing insufficient information to identify an individual who makes a request for access to a consumer's PCEHR; $11,000 (individual) $55,000 (body corporate); and
- section 76 – failure to notify the PCEHR System Operator, within the required timeframe, of becoming ineligible to be registered as a registered healthcare provider organisation. $ 8,800 (individual) $44,000 (body corporate);

The PCEHR Act also provides for multiple breaches being subject to multiple penalties etc (Part 6).

In addition to these provisions, there is a range of other sections in the PCEHR Act that impose obligations and requirements on healthcare provider organisations.

For example, sections 42 to 46 of the Act make provisions for registering healthcare provider organisations, including when a healthcare provider organisation may apply, when they are eligible for registration, registration itself, and conditions of registration—uploading of records, etc, and non-discrimination in providing healthcare to a consumer who does not have a PCEHR etc.

Under s45 it is a condition of registration of a healthcare provider organisation that

- the healthcare provider organisation does not upload a record for PCEHR purposes to other than an appropriate repository (ie of a type as listed in the Act); or
- upload a purported shared health summary unless the record would, when uploaded, be the shared health summary of the registered consumer; or
- if uploading the record would involve an infringement of copyright; or
- where the consumer has advised that the record is not to be uploaded.

Under s46 it is a condition of registration that the organisation does not refuse to provide healthcare to a consumer because

- the consumer is not registered;
- or otherwise discriminate against a consumer in relation to the provision of healthcare because the consumer is not registered.

Similarly, a healthcare provider organisation must not refuse to provide healthcare to a registered consumer because the consumer has set particular access controls on his or her PCEHR.

2. PCEHR Rules

The PCEHR Rules are available at: http://www.comlaw.gov.au/Details/F2012L01703

The rules prescribe requirements for access control mechanisms, identity verification, the handling of specified types of records, and participation requirements, including security requirements for healthcare provider organisations.

Rules that involve specific obligations or requirements for healthcare provider organisations are described below.

Non-compliance with the PCEHR rules can result in cancellation of participation.

Default access controls

The Systems Operator specifies the default access controls, which among other things allow a registered healthcare provider organisation that uploaded a record to a consumer's PCEHR to access that record. If the organisation is no longer on the access list for the consumer's PCEHR, the organisation may still access the record but not through the consumer's PCEHR.

Access Flags

Healthcare provider organisations set and maintain access flags in the PCEHR system. Healthcare provider organisations are not required to develop or redesign clinical information systems for this purpose. It is also important to note that the adding of registered healthcare providers organisations to, or the omitting of organisations from, the access list for a consumer's PCEHR is managed by the PCEHR system in accordance with the access flags that have been set by healthcare provider organisations. It is not something that local clinical information systems need to manage.

Access flags only relate to accessing information in the PCEHR system. Once information has been downloaded from the PCEHR system, access flags no longer have any effect. This means that access flags will not restrict arrangements for information exchange between organisations in a network hierarchy where information has been downloaded into local clinical information systems. Instead, existing Commonwealth, state or territory privacy and health information laws and professional obligations will apply to the collection, use and disclosure of that downloaded information (section 71 of the Act).

Rule 8. Access control mechanisms must include use of access flags

Rules 8 and 9 set out requirements for access control mechanisms that must include the use of access flags. Access flags determine which additional healthcare provider organisations can be added to/omitted from the access list for a consumer's PCEHR. Access flags must be set in the context of the organisations's network hierarchy (where applicable) - a hierarchy comprises a seed organisation and one or more network organisations. A seed organisation sets and maintains the access flags for organisations in its network hierarchy.

Rule 9. Principles for assigning access flags

Access flags must be set and maintained for registered healthcare provider organisations in a network hierarchy in a manner that balances reasonable consumer expectations about the sharing of information as part of providing healthcare to the consumer and arrangements within healthcare provider organisations for access to health information.

A registered healthcare provider organisation that is a seed organisation must ensure that access flags assigned within its network hierarchy are regularly reviewed and adjusted as necessary to remain consistent with the above principles.

Processes are available to enable the System Operator to request the seed organisation to make reasonable changes to the access flags within the network hierarchy, if the Systems Operator reasonably considers that access flags have not been assigned within a network hierarchy, or in a manner inconsistent with the above principles, or in an otherwise inappropriate manner.

A registered healthcare provider organisation must not unreasonably refuse to comply with such a request.

Rule 18. Restriction on uploading records other than shared health summaries

The effect of rule 18 is that all records uploaded by registered healthcare provider organisations to the PCEHR system must be prepared by an individual healthcare provider to whom a healthcare identifier has been assigned under paragraph 9(1)(a) of the HI Act. In addition, shared health summaries can only be created by a medical practitioner, a registered nurse or a registered Aboriginal health practitioner.

Rule 19. Effective removal of records

Rule 19 provides that the System Operator may direct a participant in the PCEHR system to effectively remove a record where the System Operator reasonably considers that the record contains a defamatory statement or affects, or is likely to affect, the security or integrity of the PCEHR system.

A participant in the PCEHR system who is given a direction under subrule (1) must comply with the direction.

3. Participation requirements

Registered healthcare provider organisations are required under section 76 of the Act to notify the System Operator in writing within 14 days of ceasing to be eligible to be registered.

The *PCEHR (Participation Agreements) Rules 2012* specify that an organisation must enter into a participation agreement with the System Operator in order to be and remain registered as a healthcare provider organisation.

The **PCEHR (Participation Agreements) Rules** are available at:
http://www.comlaw.gov.au/Details/F2012L01704
See also the Registration Guide for healthcare organisations, which gives information on what healthcare provider organisations must do to participate as registered organisations:
http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_1/$file/HCP-Registration-PM.pdf

Rule 25. Healthcare provider organisation policies

Subrule 25(1) requires that, in order to be eligible to register, healthcare provider organisations must have in place a written policy that reasonably addresses the matters specified in subrule 25(4). In summary, those matters are:

- the manner of authorising persons within the organisation to access the PCEHR system, including the manner of suspending and deactivating the user account of any authorised person (paragraph 25(4)(a));
- the training that will be provided to persons before they are authorised to access the PCEHR system, including in relation to how to use the system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the PCEHR system and the consequences of breaching those obligations (paragraph 25(4)(b));

- the process for identifying a person who requests access to a consumer's PCEHR and providing identification information to the System Operator, ensuring the organisation is able to satisfy its obligations under section 74 of the Act (paragraph 25(4)(c));
- the physical and information security measures of the healthcare provider organisation, including the procedures for user account management required under rule 27 (paragraph 25(4)(d)); and
- mitigation strategies to ensure PCEHR-related security risks can be identified, acted upon and reported expeditiously (paragraph 25(4)(e)).

If the healthcare provider organisation reasonably considers that it is not necessary for its policy to address certain matters otherwise required, on the basis of the organisation's limited size, the organisation's policy need not address those matters. This subrule is intended to exempt sole practitioners and very small healthcare provider organisations from having to address all the matters otherwise required – for example, because there are no other staff that need training.

Subrule 25(6) contains a number of administrative and procedural requirements in relation to policies required under subrule 25(1), including in summary that policies are:

- written in a manner that enables the organisation's performance to be audited against the policy (sub-paragraph 25(6)(a)(i));
- kept current (sub-paragraph 25(6)(a)(ii));
- uniquely identifiable by version (paragraph 26(6)(b)) and each version of an organisation's policy must be retained in accordance with any applicable record keeping obligations (paragraph 25(6)(d)); and
- reviewed no less than once a year for the identification of new risks, and that the review include consideration of anything that may result in unauthorised access, misuse or unauthorised disclosure of information or accidental disclosure of information, and of any changes to the PCEHR system or relevant laws since the last review (paragraph 25(6)(c)).

Written policies must be communicated, accessible and enforced in relation to employees and any healthcare providers to whom the organisation supplies services under contract (paragraph 25(2) and 25(3)).

Rule 26. Policy to be provided to the System Operator on request

Rule 26 requires that, if the System Operator requests in writing that a healthcare provider organisation provide a copy of its policy to the System Operator, the organisation must comply within seven days. The request by the System Operator may relate to the organisation's current policy or one in force on a specified date.

Rule 27. User account management within healthcare provider organisations

Rule 27 requires that the information technology systems of healthcare provider organisations, used for the purpose of accessing the PCEHR system, employ reasonable information security access management practices, including in summary:

- ensuring that only those people who require access as part of their duties are authorised to access the system (paragraph 27(a));
- uniquely identifying individuals using the healthcare provider's information technology systems and protecting that unique identity using a password or equivalent protection measure (paragraph 27(b));
- following robust and secure password and/or access management practices (paragraph 27(c));
- ensuring user accounts for persons no longer authorised to access the PCEHR system prevent access (paragraph 27(d)); and
- suspending a user account that allows access to the PCEHR system as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised (paragraph 27(e)).

Rule 28. Retention of record codes and document codes

Healthcare provider organisations must ensure that people using their information technology systems to access the PCEHR system via or on behalf of the organisation do not keep any record of a consumer's record code or document code for future use to access the consumer's PCEHR or records in the consumer's PCEHR.

4. PCEHR (Assisted Registration) Rules

The PCEHR (Assisted Registration) Rules are available at Assisted Registration Rules

These rules enable healthcare provider organisations to assist consumers to register for their PCEHR.

Consumers can currently register for a PCEHR through a Medicare office, by telephone, by the Internet, or by mail. Assisted registration will provide another channel for registration.

Medical practices may choose to offer assisted registration to vulnerable consumers (such as those in aged care and with chronic illness) who will benefit from having a PCEHR and who would be much more likely to apply to register if their medical practice assists them to do so. Participation in assisted registration by medical practices is entirely voluntary.

Medical practices can charge a consumer for providing assisted registration. However, the rules state that healthcare providers must inform patients that they can apply for registration on their own through the other channels. A Medicare rebate will not apply to any charge for assisted registration.

The new Assisted Registration Rules require that a healthcare provider organisation providing assisted registration must (in summary):

- be registered with the System Operator;
- record in writing consumer consent to be registered through assisted registration and to the uploading of information to their PCEHR, and retain this record for at least three years or provide it to the System Operator for retention for at least three years;
- use reasonable care in identifying a consumer before asserting the consumer's identity to the System Operator. Guidance will be provided to organisations for this purpose;
- implement a policy that addresses the manner of authorising and training employees to provide assisted registration; how consumer consent will be recorded and retained; and the process and criteria for identifying consumers for assisted registration.

These requirements are covered in the following rules.

Rule 6. Identification of consumer

Rule 6 requires that an employee must exercise reasonable care when identifying a consumer and must be satisfied that the consumer is the person making the application to register. This decision will be informed by the organisation's policy on identifying consumers. Guidance on identifying consumers will be published online by the System Operator to inform this policy. The employee must not knowingly or recklessly register a consumer fraudulently.

Rule 7. Consumer consent

Rule 7 requires the healthcare provider organisation to record a consumer's consent in writing. Subrule 7(2) provides that the consumer's consent must be recorded in the approved form. Paragraph 39(a) of the Act requires that, for a consumer to apply to the System operator for registration, the application must be made in the approved form. This form will be available in paper and electronic form, allowing the healthcare provider organisation to select the form most appropriate to their business.

This form which records the consumer's consent must be retained for audit purposes. The healthcare provider organisation can choose to store the form itself (in whatever manner chosen by the organisation) or it can be sent to the System Operator to be stored (subrule 7(3)). The form must be retained for at least three years. If the organisation chooses to send the form to the System Operator, it must do so no more than 30 days after the consumer has given the consent.

Rule 8. Must inform consumer of alternative methods of registration

Before providing assisted registration for a consumer, a registered healthcare provider organisation must inform the consumer that an application to register may be made at a Medicare office, by telephone, by the Internet, or by mail.

This rule is intended to address circumstances where healthcare provider organisations may choose to charge a consumer for providing assisted registration. The organisation will be unable to impose a charge under Medicare, however it may impose a charge outside Medicare for services they perform.

Rule 9. Healthcare provider organisation policies

Rule 9 requires that a healthcare provider organisation that chooses to provide assisted registration for consumers must have in place a written policy that addresses certain matters in addition to those already required under rule 25 of the *PCEHR Rules 2012*.

The additional matters that must reasonably be addressed by the organisation's written policy are:

- the manner of authorising persons within the organisation to provide assisted registration to consumers on behalf of the organisation;
- the training that will be provided to persons before they are authorised to provide assisted registration;
- the manner of recording consumer consent and the process for handling that consent, i.e. whether it is retained by the organisation and/or sent to the System Operator and the associated process; and
- the framework for identifying whether a consumer is a known customer. This may include the organisation's preferred model for being satisfied that a consumer is a known customer of the organisation, the preferred types of identity documents to be provided, and the steps to be taken if the employee of the organisation is uncertain about a consumer's identity. Guidance on identifying consumers will be published online by the System Operator to inform such policies.