Hospitals

My Health Record expansion program

Data breaches and cyber security

What is My Health Record?

My Health Record commenced in 2012 and was then known as the Personally Controlled Electronic Health Record (PCEHR). Operated by the Australian Digital Health Agency, My Health Record is a secure online summary of a consumer's health information that can be accessed by authorised healthcare providers taking part in their care. Consumers with a My Health Record will be able to set privacy settings, which allows them to control what goes into the record, and who sees it.

Health Service obligations to keep health data safe and secure

- In Australia, all health services are required by law to protect the security and privacy of individual health information.
- The applicable legislation for public and private entities may vary depending on jurisdiction. The Commonwealth's Privacy Act 1988 (Privacy Act) applies to Australian government entities and all private sector health service providers, regardless of size.
- The Privacy Act requires that health service providers take "reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure" (APP 11.1).
- Most importantly, mandatory requirements apply if a notifiable Data Breach occurs.

What is a notifiable data breach?

A 'notifiable data breach' refers to a data breach that meets the criterion set out under s 75(1) of the My Health Records Act, so that it must be reported to the relevant regulator. This includes:

- an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record;
- an event or circumstance has occurred or arisen OR an event or circumstance that may have occurred or arisen, and;
- the event or circumstance has compromised the security or integrity of the system OR the event or circumstance may have compromised the security or integrity of the system.

Depending on the circumstances, where there is a notifiable data breach, there may or may not be an additional requirement to notify a healthcare recipient of the breach.

Example of a compromise to the security and integrity of My Health Record:

A My Health Record registered health service discovers that an external party has hacked into its IT system. As its IT system connects to the My Health Record system, there is a possibility that the successful intrusion allowed the hacker to use the organisation's credentials to log into the My Health Record system and access information.

This would be considered a circumstance that has arisen that may compromise the security and integrity of the My Health Record system. As such, the health service would be required to comply with s 75 of the My Health Records Act when reporting and responding to the potential breach.

What should you do when you become aware of a notifiable data breach?

Health Services must report a notifiable data breach as soon as practicable after becoming aware of the breach. However, reporting the breach should not be at the expense of initial efforts to contain it. Further, any steps taken by the health service to rectify or contain the breach do not relieve the health service of its reporting obligations.

What is the purpose of data breach notification?

Providing notification in the case of a data breach involving personal information is consistent with good privacy practice. Notification allows affected healthcare recipients to take any necessary action to protect their information and to ensure the ongoing security and integrity of, and confidence in, the My Health Record system. This recognises the sensitivity of the information the system contains.

The requirements imposed on health services by the My Health Records Act 2012 aim to ensure that breaches are dealt with effectively and are prevented in the future. Breach notification provides an important feedback loop for the System Operator's maintenance of system security, and enables swift containment of a breach and preventative action. It also ensures that oversight bodies (such as the OAIC) are made aware of a breach and can investigate the matter where appropriate.

To whom should your health service report a data breach?

Health services must report a notifiable data breach to the System Operator. State and territory health services may also voluntarily report data breaches to their local privacy regulator in addition to reporting to the System Operator (refer to key contacts).

The System Operator must then notify all affected healthcare recipients if:

- a health service asks the System Operator to notify affected healthcare recipients of a confirmed data breach
- a health service asks the System Operator to inform healthcare recipients that would be affected of a potential data breach
- if there is a reasonable likelihood that the data breach occurred, and
- the effects might be serious for at least one healthcare recipient.

What happens if a notifiable data breach is not reported?

The Information Commissioner has the power to seek a civil penalty if a health service fails to report a notifiable data breach. This includes where a health service:

- fails to report a notifiable data breach as soon as practicable after becoming aware of it
- reports a notifiable data breach to only the System Operator but not to the OAIC, or vice versa.

The civil penalty is an amount up to 100 penalty units.

How does My Health Record protect people's health information?

- My Health Record balances safety and security with the benefits available to consumers and healthcare providers at the point of care.
- The security and privacy of My Health Record is treated seriously and the system is built to industry standards for storing and processing sensitive information.
- My Health Record is protected by security controls that protect health records from unauthorised access, and to guard against cyber-attacks.
- The security controls include encryption, secure gateways, and firewalls, authentication mechanisms and malicious content filtering.
- The Cyber Security Centre monitors for suspicious activities. The centre will trigger an investigation and suspend registration when required.
- Criminal penalties can include up to two years in jail and up to $126,000 in fines. Civil penalties can incur up to $630,000 in fines

My Health Record Cyber Security Centre

- The My Health Record has in place robust authentication mechanisms to prevent unauthorised access.
- As of 2017, My Health Record has been in operation for over five years and over 5.2 million Australians have a record. During this time, there have been no known security breaches.
- Every time a healthcare provider accesses a My Health Record, a log is automatically created. This allows an individual to monitor every access to their My Health Record.
- The Australian Digital Health Agency's Cyber Security Centre has responsibility for the ongoing security of the My Health Record system.
- The Cyber Security Centre has robust controls in place to prevent a malicious attacker from gaining access to health records.
- The Cyber Security Centre continually monitors the system for evidence of unauthorised access.
- This includes utilising real-time monitoring security tools that are configured and tuned to detect events of interest, or notable events.

Key contacts

Digital Health Standards and Advisory
Department of Health and Human Services
myhealthrecordexpansion@dhhs.vic.gov.au

Office of the Victorian Information Commissioner
Privacy and Data Protection
Phone: 1300 666 444
PO Box 24274 Melbourne VIC 3001
https://www.cpdp.vic.gov.au/

System Operator
Phone: 1800 723 471
My Health Record
Box 9942 Sydney NSW 2000

For further information

Select this link: My Health Record or visit <https://www.myhealthrecord.gov.au/>

To receive this publication in an accessible format phone **9096 0749** using the **National Relay Service 13 36 77** if required, or email **myhealthrecordexpansion@dhhs.vic.gov.au**

Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne. |