Australian Government
Office of the Australian Information Commissioner

March 2019

Privacy resource 23

Handling personal information in the My Health Record system

This business resource explains the obligations of healthcare provider organisations when uploading, collecting, using and disclosing health information from a patient's My Health Record. It also provides an overview of how the *My Health Records Act 2012* interacts with the *Privacy Act 1988*.

Key things to remember

- Healthcare provider organisations[1] that are registered to use the My Health Record system are authorised to collect, use and disclose health information in a patient's My Health Record for the purpose of providing healthcare to the patient. They are also authorised to upload health information to a patient's record unless the patient asks them not to.
- The *My Health Records Act 2012* (My Health Records Act) specifies a limited number of circumstances in which healthcare provider organisations are authorised to collect, use and disclose information from a patient's My Health Record for purposes that are not related to providing healthcare.
- The Information Commissioner can investigate breaches of the My Health Records Act and the *Privacy Act 1988* (Privacy Act).

Uploading information

Uploading health information about patients

The My Health Record system contains an online summary of a patient's key health information; not a complete record of their clinical history. It allows healthcare provider organisations to include relevant clinical documents in a patient's My Health Record that

[1] Under the My Health Records Act, 'healthcare provider organisations' are registered to use the system and are considered 'participants in the My Health Record system'. Individuals working for a healthcare provider organisation need to be authorised by their organisation to use the system. A sole practitioner who is registered to use the system will be considered a 'healthcare provider organisation' by the System Operator.

can be seen by other healthcare providers involved in their care. These documents include, for example, referral letters, prescription and dispense records, discharge summaries and shared health summaries.

Even though healthcare provider organisations are authorised to upload documents to a patient's My Health Record without the patient's express consent, it is good privacy practice to advise patients when information is being uploaded to their record. In addition, there are some circumstances in which documents must not be uploaded to a patient's record. These are when:

- a patient requests that a clinical record not be uploaded; or
- a prescribed State or Territory law prohibits healthcare provider organisations from uploading the patient's record or including in a record particular information without consent.[2]

Uploading health information about a third party

Under the My Health Records Act, healthcare provider organisations are authorised to upload information about a third party to a patient's My Health Record if that health information is directly relevant to the healthcare of the patient.[3] This allows healthcare provider organisations to record and upload a patient's family, social and medical histories in order to provide accurate diagnosis and treatment.

Example: Damien is receiving ongoing treatment for hypertension. He tells his GP that his mother has a heart condition. Damien's GP believes that the information about Damien's mother's heart condition is relevant to his treatment and therefore this information is included in his My Health Record.

The GP clinic is authorised by the My Health Records Act to upload the information, about Damien's mother, without seeking her consent, as the information is directly relevant to Damien's healthcare.

Authorised collection, use and disclosure

Collecting, using and disclosing information for the purpose of providing healthcare

In addition to uploading information to a patient's My Health Record, the My Health Records Act authorises healthcare provider organisations to collect, use and disclose information that is already contained in a patient's My Health Record for the purpose of providing healthcare to the patient. This collection, use and disclosure needs to be done in accordance with the access controls set by the patient or the default access controls if the patient hasn't

[2] Some states and territories have legislation that requires patients to consent to the disclosure of particular health information in a certain way or to provide consent expressly. Regulation 3.1.1 of the My Health Records Regulation 2012 prescribes certain state and territory law which cover certain notifiable conditions (such as HIV), as well as other matters (such as information which relates to a cancer diagnosis). Where these prescribed laws apply, consent must be obtained.

[3] This authorisation is also subject to certain state or territory laws, prescribed by the My Health Record Regulation 2012, which require third parties to consent to information being disclosed in particular ways.

set any. The system has been designed so that if a patient has set access controls these will automatically be applied to the patient's record and does not require the healthcare provider organisation to take any action.

More information on access controls is available on the Australian Digital Health Agency's My Health Records website.

The terms 'collects', 'use' and 'disclosure' are explained in the Australian Privacy Principles Guidelines. In addition, the My Health Records Act provides further clarification about the term 'use' of health information in a My Health Record by defining it to include the following:

a. accessing the information;

b. viewing the information;

c. modifying the information;

d. deleting the information.

Other authorised collections, uses and disclosures of health information

The My Health Records Act outlines circumstances that allow healthcare provider organisations to collect, use and disclose information in a patient's My Health Record in ways that are not consistent with the default access controls or the access controls set by the patient. These circumstances are outlined in sections 63 - 68 of the My Health Records Act and can occur when collection, use or disclosure is:

- necessary for the management of the My Health Record system (e.g. for correcting errors or omissions) and are reasonably expected by the patient;
- necessary to lessen or prevent a serious threat to an individual's life, health or safety and it is unreasonable or impracticable to obtain the patient's consent;
- authorised by law;
- consented to by the patient (i.e. the patient has given their consent for the information to be collected, used or disclosed in a particular way); or
- necessary for purposes that relate to a healthcare provider organisation's indemnity cover.

Unauthorised collection, use and disclosure of health information

Penalties for unauthorised collection, use or disclosure

A person that collects, uses or discloses health information from a patient's My Health Record in a way that is not authorised by the My Health Records Act, will breach the Act.[4]

A person that breaches the collection, use and disclosure provisions may be liable for a civil or criminal penalty.[5] These penalties only apply if a person knowingly handles information in an unauthorised way, or is reckless about whether it is unauthorised. A breach of these provisions is also considered an interference with privacy which may be investigated under

[4] The term 'person' is defined in the Acts Interpretation Act 1901 and includes a body politic or corporate as well as an individual.

[5] See Chapter 6 of Guide to privacy regulatory action.

the Privacy Act and subject to other enforcement action and other remedies – for further information see 'The relationship between the My Health Records Act and the Privacy Act'.

Data breaches

Section 75 of the My Health Records Act places a mandatory obligation on healthcare provider organisations to take specific actions when they become aware of an actual, or potential, data breach in their organisation which relates to the My Health Record system.

Private sector healthcare provider organisations are required to report data breaches to both the System Operator[6] and the Office of the Australian Information Commissioner (OAIC). State or Territory public sector healthcare provider organisations are required to report data breaches only to the System Operator.

Healthcare provider organisations must report an actual or potential data breach when they become aware that:

- a person has, or may have, contravened the My Health Records Act by collecting, using or disclosing health information in a patient's My Health Record in an unauthorised way;
- an event has, or may have, occurred that compromises, may compromise, has compromised or may have compromised the security or integrity of the My Health Record system; or
- circumstances have, or may have, arisen that compromise, may compromise, have compromised, or may have compromised, the security or integrity of the My Health Record system.

Civil penalties may apply to private sector healthcare provider organisations that do not notify the System Operator and the OAIC about a data breach, or a potential data breach. Even if a data breach has been resolved, healthcare provider organisations are still required to notify the System Operator and the OAIC about it.

Other actions that healthcare provider organisations are required to take when they become aware of a data breach, or a potential data breach, include:

- containing the breach;
- evaluating any risks that may be related to the breach;

If healthcare provider organisations do not take these other actions, they will not be subject to a civil penalty. However, they may be subject to other consequences, such as cancellation of their My Health Records registration. For further information on dealing with data breaches in the My Health Record system, see the OAIC's Guide to mandatory data breach notification in the My Health Record system.

Organisations may wish to develop a data breach response plan so that, in the event of a breach, there are set procedures and clear lines of authority which can assist organisations and their staff to contain the breach and manage the response. A data breach response plan is a framework which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken by an entity in managing a breach if one occurs.

For more information on developing a data breach response plan, see the OAIC's *Data breach preparation and response — A guide to managing data breaches in accordance with the* Privacy Act 1988 *(Cth)*.

[6] The System Operator is the Australian Digital Health Agency.

The relationship between the My Health Records Act and the Privacy Act

An authorisation to collect, use or disclose health information under the Privacy Act

When a person is authorised to collect, use or disclose health information under the My Health Records Act, this action is also authorised under the Privacy Act. This means that if a particular collection, use or disclosure is authorised by the My Health Records Act then it will not breach the Privacy Act.

The OAIC's enforcement and investigative powers

An unauthorised collection, use or disclosure of health information in a patient's My Health Record, is considered an 'interference with privacy' for the purposes of the Privacy Act. This means that an unauthorised collection, use or disclosure triggers the Information Commissioner's investigative and enforcement functions and powers under the Privacy Act. This allows the Information Commissioner to investigate complaints received from patients about the handling of information in their My Health Record and also to conduct investigations into the acts or practices of organisations that are believed to have breached the Act. The OAIC will usually try to resolve complaints through conciliation, if this is appropriate.

The Information Commissioner's enforcement powers under the My Health Records Act and the Privacy Act include:

- accepting an enforceable undertaking;
- making a determination;
- applying to a Court for an injunction; and
- applying to a Court for an order that a person pay a civil penalty.

It is open to the Information Commissioner to use a combination of enforcement powers to address a particular matter.

The Information Commissioner is also able to investigate and enforce compliance with other provisions of the My Health Records Act which are outlined in Part 5 of the Act. For further information on the OAIC's approach to using enforcement powers in relation to the My Health Record system, see the OAIC's My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016.

Downloading health information from a My Health Record on to a local IT system

Information held in a patient's My Health Record can be downloaded to a healthcare provider organisation's local IT system.

If information is downloaded onto a local IT system, only the information that is reasonably necessary to provide healthcare to the patient should be downloaded.

Once information is downloaded to a local IT system, the My Health Records Act no longer applies to the health information's collection, use or disclosure. Instead, it will be subject to the Privacy Act and/or the local state or territory health information and privacy laws and professional obligations just like other health information that healthcare provider organisations handle.

This means that private healthcare provider organisations will also need to comply with the Australian Privacy Principles (APPs), which are part of the Privacy Act. For example, under the APPs healthcare provider organisations are required:

- to notify patients that they are collecting their personal information (APP 5);
- to ensure that the personal information they collect is accurate, up-to-date and complete (APP 10); and
- to correct a patient's personal information, if the patient requests them to do so (APP 13).

Further information on the APPs is available in the APP guidelines.

Example: A physiotherapist who works at Ace Medical Centre (a private health clinic) is seeing a patient who has recently sprained her ankle. During the consultation, the physiotherapist accesses the patient's My Health Record to view a diagnostic image report uploaded by a radiologist. At this point, the My Health Records Act applies to how the information in the report is collected, used and disclosed.

The physiotherapist then downloads the diagnostic imaging report on to her own computer and two days later opens the file on her computer that contains the report in preparation for a consultation with the patient. The My Health Records Act does not apply to how the health information in the diagnostic imaging report is now used and disclosed.

As Ace Medical Centre is a private sector healthcare organisation, the physiotherapist employed by the Centre will need to comply with the Privacy Act and any other relevant state or territory legislation when handling the patient's health information.
For further information on which privacy legislation applies when handling health information outside of the My Health Record system, see the OAIC's State and territory health privacy webpage.

Finding out more about the My Health Record system

Further information about the My Health Record system is available at:

- The My Health Record website
- The Australian Digital Health Agency website
- The My Health Record system online training modules, which are available for clinical and nonclinical staff and cover organisation such as community pharmacies, residential aged care facilities, medical specialists, allied health and hospitals.

For further information

GPO Box 5218 Sydney NSW 2001 | **P** 1300 363 992 | **E** enquiries@oaic.gov.au

Or visit our website www.oaic.gov.au

The information provided in this resource is of a general nature. It is not a substitute for legal advice.