Australian Government
Office of the Australian Information Commissioner

November 2018

Privacy resource 22

Ways you can protect patient privacy when using the My Health Record system

Note: every individual with a Medicare or Department of Veterans' Affairs card who does not already have a My Health Record will automatically be registered to have a My Health Record, unless they tell the Australian Digital Health Agency that they don't want one between 16 July 2018 and 31 January 2019.

For further information, visit the My Health Record website or call the My Health Record Help line on 1800 723 471. You can also read the OAIC's opt-out FAQs.

This business resource provides tips on how healthcare provider organisations can protect a patient's privacy when using the My Health Record system, including how to protect the personal information of patients when assisting them to register for a record. It also provides background information on some of the features of the My Health Record system, such as the different privacy controls available to patients.

Key things to remember

- It is important for healthcare providers to have open communication with their patients and to reach a shared understanding of how the patient's My Health Record will be used.
- If healthcare provider organisations[1] are involved in a patient's healthcare, they will be able to access and download information in their patient's My Health Record, unless the patient has restricted the organisation's access to their record by setting access controls.

[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 (the Australian Digital Health Agency). This resource at times uses the term 'healthcare provider' when explaining responsibilities that individual healthcare providers also have.

- A healthcare provider organisation can upload information to a patient's My Health Record even if the patient has set access controls. A healthcare provider organisation should not upload information to a record if a consumer requests them not to.
- Access controls allow patients to restrict which healthcare provider organisations can access their My Health Record and which documents they can view.
- The *My Health Records Act 2012* (My Health Records Act) includes legally binding rules which set out further obligations when it comes to using the My Health Record system. It is important to be aware of a healthcare provider organisation's obligations under these rules as this will help ensure appropriate procedures and policies are in place to protect patient privacy.

What to consider when accessing a patient's My Health Record

The My Health Record system contains an online summary of a patient's key health information; it is not a complete record of their clinical history. It allows healthcare providers to include relevant clinical documents in a patient's My Health Record. These documents include, for example, referral letters, prescriptions and dispense records, discharge summaries and shared health summaries.

Healthcare providers may access a patient's My Health Record for a number of different reasons during the provision of healthcare to that patient. For example, if a patient has recently been discharged from hospital, healthcare providers may wish to access their My Health Record to view clinical documents, such as the hospital discharge summary. Another example is where a patient has broken their wrist and the healthcare provider accesses their My Health Record to view a diagnostic imaging report uploaded by a radiologist. This kind of information could help the healthcare provider during their next scheduled consultation with the patient.

It is important for healthcare providers and patients to have open communication about how their My Health Record will be used and when it has been accessed, so that the record is used in accordance with the patient's expectations. This is particularly important, because if a My Health Record was created for your patient following the opt-out period, two years' of Medicare information may be uploaded to their record the first time you view or upload information to their My Health Record.

Generally, healthcare providers should access a patient's My Health Record only for the purposes of providing healthcare to that patient.

Uploading information to a patient's My Health Record

A My Health Record can contain three sets of information — clinical, Medicare and personal. Healthcare providers will only be able to upload information into the clinical section of a patient's record. These clinical documents may include, for example:

- a Shared Health Summary, which is a document that summarises an individual's health status and includes important information such as allergies, medical history and immunisations. Only a medical practitioner, a registered nurse or an Aboriginal or Torres Strait Islander health practitioner can upload a Shared Health Summary to a patient's My Health Record;
- referral and specialist letters;

- event summaries, which are clinical documents that may be uploaded to an individual's My Health Record summarising one or more episodes of care; and
- discharge summaries, which is a record of an individual's hospital stay and any follow up treatment required.

Under the My Health Records Act, healthcare provider organisations are authorised to upload these types of documents to a patient's My Health Record. However, if a patient requests that a particular document not be uploaded, healthcare providers are required by law to comply with their request. If a healthcare provider intends to upload clinical documents to their patient's My Health Record, it is best practice to talk to the patient about the kind of information that will be uploaded. This will also allow the patient an opportunity to make an informed decision on whether documents are to be uploaded to their record.

Healthcare providers will also need to take reasonable steps to ensure that any information uploaded to a patient's My Health Record is relevant, accurate and up-to-date at the time of uploading.

Downloading information from a patient's My Health Record

Where it is for the purpose of providing healthcare, healthcare providers can collect health information from a patient's My Health Record by downloading it onto their local IT system, such as onto their computer or local clinical information system. Downloading information onto a healthcare provider's own IT system is considered a 'collection' of information from the My Health Record system, therefore must be done in a way that complies with the My Health Records Act.

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 1988* (Privacy Act) and/or local state or territory health information and privacy laws and professional obligations just like other health information that healthcare providers handle. For further information on these laws and when they apply, see the OAIC's State and territory health privacy webpage.

If healthcare providers do download information, they will need to ensure that they do not download more information than is necessary to treat the patient.

Removing documents from a patient's My Health Record

Patients or the authoring healthcare provider can remove documents from a My Health Record. Healthcare providers are only able to remove documents that their organisation has authored and uploaded.

If a patient removes a document it will not be available through the My Health Record to any healthcare providers involved in their care, including the author. Evidence of the document being removed will be provided to the authorising healthcare provider, however, how this is displayed may vary depending on the clinical information system used.

Modifying information in a patient's My Health Record

If a healthcare provider becomes aware that a clinical document that they have uploaded to a patient's My Health Record is incorrect, they should remove it and upload a new, correct version of the document.

Getting to know the different privacy controls available to patients

There are two features in the My Health Record system that allow patients to control access to documents in their record and to monitor who has viewed their record. These features are known as 'access controls' and 'access history'.

Access controls

The My Health Record system allows patients to keep their health information private by controlling which healthcare provider organisations can access documents in their record, and which documents can be accessed. They can do this by setting 'access controls'. Access controls are set at the healthcare provider organisation level, which means that they apply to the healthcare provider organisation rather than to individual staff members of that organisation. A patient can set access controls on all documents in their My Health Record except the Shared Health Summary, the Advance Care Directive and consumer entered Personal Health Summary which can be seen by all participating healthcare provider organisations.

If a patient has not set access controls, the default access controls will apply and healthcare providers will be able to view all clinical documents in their patient's My Health Record, as well as upload documents to their record.

Healthcare providers should be familiar with the access controls that a patient is able to set as they may impact on how healthcare providers use a patient's My Health Record.

The two access controls that a patient can set are:

- **Record Access Code:** Patients can limit access to their entire record by using a Record Access Code (RAC). If a patient has set a RAC, healthcare provider organisations will not be able to view documents in their patient's My Health Record unless the patient provides the provider with their RAC. Once a healthcare provider uses the RAC, they will only be able to see the documents that are marked as 'general access'. For subsequent use, the RAC will not be required
- **Limited Document Access Code:** A Limited Document Access Code (LDAC) also operates like a RAC with the exception that the use of the LDAC will not only allow access to the patient's My Health Record but healthcare providers will also be able to see documents that the patient marked as 'restricted'.

The access controls set by a patient can be bypassed in a situation where it is unreasonable or impracticable to obtain consent from the patient and the healthcare provider reasonably believes that access is necessary to lessen or prevent a serious threat to the patient or to another individual's life, health or safety.

Under the My Health Records Act, healthcare provider organisations must not discriminate against or refuse to provide healthcare to a patient on the basis that the patient has set particular access controls on their My Health Record.

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

Access history

The access history function allows patients to see which healthcare provider organisations have accessed their record.

Specifically, the access history page in a patient's My Health Record contains the following information:

- the date and time that a patient's My Health Record was accessed/edited;
- the healthcare provider organisation (rather than the individual healthcare provider), who accessed/edited the My Health Record; and
- details of the action that was performed (e.g. when a clinical document was created or removed, when individual contact details were amended, when representatives have been added or removed). This includes actions performed by external providers (i.e. Medicare) and patients when accessing their own My Health Record.

Understanding the rules made under the My Health Records Act

The suite of legislation and guidelines that regulates the operation of the My Health Record system includes the My Health Records Rule 2016 and the My Health Records (Assisted Registration) Rule 2015. These legally binding rules provide further information on the functions of the My Health Record system and set out the obligations of healthcare provider organisations in specific circumstances and scenarios. Being aware of a healthcare provider organisation's obligations under these rules will help to ensure that appropriate procedures and policies are in place to protect patient privacy and ensure the proper handling of their personal information.

An organisation's My Health Record policy

The My Health Records Rule 2016 is aimed at supporting the secure operation of the My Health Record system by prescribing, for example, how specific types of records should be handled and the access controls that allow patients to manage their My Health Record.

The rule also requires healthcare provider organisations to have a written policy that reasonably addresses a range of matters. This includes how the organisation authorises people to access the My Health Record system and the physical and information security measures that are established and adhered to by the healthcare provider organisation. An organisation's My Health Record policy will explain how staff members can access and use the system, so it is important that the policy is implemented well and clearly understood by everyone that needs to comply with it.

Assisted registration

The My Health Records (Assisted Registration) Rule 2015 sets out healthcare providers organisations' obligations when they choose to provide the option of assisted registration to their patients (for those who do not have a record yet, or who won't have one created during the opt-out period, such as children). Assisted registration allows healthcare provider organisations to assist their patients to register for a My Health Record.

As part of the assisted registration process, healthcare provider organisations will be handling a patient's personal information because they will need to verify the patient's identity and also review their Assisted Registration application form. During this process, healthcare provider organisations will need to handle their patient's information in accordance with their privacy obligations. Healthcare provider organisations should only collect information from a patient that is specified in the Assisted Registration application form.

Healthcare provider organisations that provide assisted registration must comply with the privacy laws of their jurisdiction. For example:

- if a healthcare provider organisation is a public healthcare provider of a state or territory, it will need to comply with the privacy laws of its state or territory; and
- if the healthcare provider is a private healthcare provider organisation, it will need to comply with the Privacy Act and any relevant state or territory laws.

For further information on which laws apply to different organisations, see the OAIC's State and territory health privacy webpage.

Healthcare provider organisations that choose to provide Assisted Registration must also develop, maintain and enforce an Assisted Registration policy that addresses the four matters specified in sub-rule 42(4) of the My Health Records Rule 2016. An organisation's Assisted Registration policy is required to:

- explain how the organisation will authorise its employees to provide Assisted Registration;
- outline the training that will be provided to an employee who is authorised to provide Assisted Registration;
- explain how the organisation will confirm consent of an individual; and
- explain how authorised employees will identify an individual for the purposes of Assisted Registration.

The Australian Digital Health Agency's My Health Record website contains further information for healthcare providers that provide assisted registration.

Finding out more about the My Health Record system

To find out more about the My Health Record system, see:

- the My Health Record website
- the Australian Digital Health Agency website
- the My Health Record online training modules, which are available for clinical and nonclinical staff and cover organisations 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