nehta

My Health Record Commonly Asked Privacy and Policy Questions

How to use this document: *The questions and answers below are aimed at assisting PHNs to be confident when answering questions about the My Health Record with regard to privacy obligations; patient control; accessing and uploading information to the My Health Record; and relying on information in the My Health Record.*
These questions have been generated through engagement with GPs, pharmacists, allied health practitioners, nurses, specialists and medical indemnity insurers.

PRIVACY OBLIGATIONS	
1. What are a healthcare organisation's privacy obligations when participating in the My Health Record?	• All healthcare organisations are under an existing professional and legal obligation to protect their patients' health information, regardless of their participation in the My Health Record. Establishing and maintaining information security practices is an essential professional and legal requirement for using digital health in the delivery of healthcare. • The My Health Records Rule sets out the privacy and security requirements that healthcare organisations must comply with to be eligible to be registered and to remain registered under the My Health Record system; this includes having a policy that sets out certain access and security procedures for the organisation. • NEHTA has drafted a template My Health Record policy that an organisation can adapt to meet their needs: http://www.nehta.gov.au/get-started-with-digital-health/registration/register-with-the-healthcare-identifiers-hi-service-and-the-my-health-record-system • NEHTA also has a worksheet that can guide an organisation to implementing security practices and policies in their organisations for when staff use digital health/the My Health Record: http://www.nehta.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/privacy-and-security
2. Is it true that the federal Privacy Commissioner (OAIC) found in an assessment that most registered practices do not meet the My Health Record privacy obligations?	• In 2015 the OAIC conducted a review of security controls of seven GP practices participating in the My Health Record system. The assessment found all of the GP practices had procedures in place to manage access to their systems including the My Health Record. However, the OAIC identified some deficiencies in the policies, and recommended improvements. • The OAIC recommendations are common with other existing information security obligations set out in the Privacy Act (in particular Australian Privacy Principle 11 – security of personal information), and the RACGP Computer and Information Security Standards (CISS): 1. *Review and update policies and procedures* (CISS Standard 1, 3 and 12) 2. *Consider restricting access to users of the My Health Record system to those who need to use it* (CISS Standard 4) 3. *change computer settings so that a user is required to enter a user name and password to deactivate a screensaver* (CISS Standard 3) 4. *conduct regular and ongoing privacy and My Health Record system access training* (CISS Standard 1.6) 5. *record the names of all employees that undertake My Health Record system training* (CISS Standard 1.6)
3. Why are there penalties for misuse of My Health Record information (up to $108,000 for individuals and $540,000 for organisations)?	• Misuse of a person's health information is a serious matter. The potential for damage is significant and this is reflected in current professional and legal obligations on persons such as healthcare providers to protect patient information. The My Health Record system contains health and other important information so penalties (both civil and criminal) are used, among other measures, to protect this information. • The penalties for misuse of the My Health Record system are for *reckless or intentional misuse*. If there is a mistaken access to a record by a provider, they will not be subject to the penalties. • The range of enforcement options for the Privacy Commissioner means that, depending on the severity of the breach of privacy, the Commissioner may instead require training, or an apology, as opposed to a penalty.

4. Are healthcare organisations obliged to report data breaches?	• In recognition of the special sensitivity of health information, the My Health Record legislation makes it mandatory for participants (including healthcare organisations) to notify the My Health Record System Operator of potential and actual data breaches involving the My Health Record system. The breach must be notified as soon as practicable, regardless of whether the breach has been resolved by the organisation. • A data breach is an unauthorised collection, use or disclosure of health information in an individual's My Health Record, or an event or circumstance that may compromise the security or integrity of the My Health Record system (for example, an employee's log on credentials have been compromised and an unauthorised party has accessed the organisation's clinical information system).
PATIENT CONTROL	
5. Can patients edit or remove what a healthcare provider uploads?	• A patient is not able to edit any document that has been uploaded by providers to their My Health Record. However, they have the ability to remove or restrict access to certain documents in their record.
6. Will a healthcare provider know if a patient has removed or restricted access to documents?	• A provider will not know if a patient has restricted access to a document or removed a document unless they are the clinical author of the document in which case they will be able to see that the document was removed. The likelihood that a patient has restricted access to a document is very low, with less than 1% of the 2.7 million individuals currently registered that have set restrictions on who can access their My Health Record documents. • Patients can consult a provider today and may omit information or not reveal everything about their health, whether accidentally or intentionally. Therefore it is important that existing methods of consulting and communicating with a patient continue, for example asking a patient about medications, allergies, adverse reactions, and taking a medical history.
7. If a patient requests a healthcare provider not to upload information to the My Health Record, must the provider follow that request?	• A healthcare provider must not upload information to the My Health Record where the patient has advised the provider not to upload that information. • Where the patient has requested that certain information be omitted from a document (e.g. a Shared Health Summary) then the provider should consider counselling the patient in relation to the risk of excluding the information from their record, and the benefit of ensuring all the relevant information is included. If the patient insists, and the provider is uncomfortable with uploading a document without that information included, then the provider should not upload any information.
ACCESSING THE MY HEALTH RECORD	
8. Does a healthcare provider need to gain the consent of a patient to view their My Health Record outside of a consultation?	• A healthcare provider does not need the consent of a patient to view their My Health Record when providing healthcare to the patient. A provider would be authorised to view a My Health Record outside of a consultation if it is connected with providing care to the patient – for example checking to see if test results have been uploaded. • Providers should remember that a patient has the ability to review an Access History that sets out information about organisations that have accessed their record, although the name of the practitioner that accessed the record is not displayed to the patient. Patients can also set up SMS or email notifications for when an organisation first accesses their record.

9. Is there a legal obligation to check an individual's My Health Record before making a clinical decision?	• There is no legislative obligation that requires a healthcare provider to view the My Health Record. • As is the case now, negligence could arise where a healthcare provider omits to consider relevant information in the treatment of a patient and this leads to injury to the patient. Whether the provider should have considered this information will be determined by reference to the expected standard of care, as established by reference to the practice of their peers. Over time, as use of the My Health Record becomes more common, standards *could* evolve which may mean it is expected providers view the My Health Record. • In the absence of any existing standards of care, the Australian Medical Association (AMA) has released some guidance to assist medical practitioners on how to use the My Health Record: https://ama.com.au/article/ama-guide-using-pcehr • A provider should contact their medical indemnity insurer if they are concerned about their medico-legal obligations with use of the My Health Record.
UPLOADING INFORMATION TO THE MY HEALTH RECORD	
10. Can healthcare providers upload information without telling the patient?	• A provider does not need to gain consent from the patient each and every time a document is uploaded to the My Health Record system. A consumer gives standing consent upon registration for all documents being uploaded to their record. (Note that for the opt-out trials the authority for a provider to upload documents to the My Health Record comes from legislation, not the consumer's standing consent). • However, there is particular sensitive information (such as HIV or AIDS) that under existing Public Health Acts require the express or written consent of a patient to share that information with other providers; those obligations still apply for the My Health Record, so that a provider wishing to upload that kind of sensitive information will need the additional consent of the patient to do so. • Wherever possible, it is preferable for the healthcare provider and the patient to be together when curating the content of a Shared Health Summary. This may help ensure the accuracy and currency of the information, and helps patients better understand their health conditions.
11. Does a healthcare provider need to check and curate all the documents that they upload to the My Health Record to ensure they are always up to date?	• When the provider uploads a document to the My Health Record, they must ensure that the information they upload is accurate, up-to-date and not misleading or defamatory. • If the provider discovers that information they have uploaded is clinically inaccurate, they should take steps to remove it and upload an amended version of that clinical document. • When important information about a patient changes, for example their medications or immunisations, and that provider has already uploaded a Shared Health Summary for that patient, a new Shared Health Summary should be uploaded.
12. How does the My Health Record affect copyright?	• Neither the My Health Records Act nor recent changes to the Copyright Act affect ownership of copyright in medical "documents", which may include written reports, specialist letters, pathology and diagnostic imaging results, sound recordings (e.g. a patient's heartbeat) or movies (e.g. an MRI video of a patient's heart functioning). • Whichever party owns the copyright will continue to own it – this could be the individual provider who authored the document, the entity that employs the authoring provider or a completely different entity.

13. Can a healthcare provider upload a letter received from a Specialist?	• For ***documents created <u>on or after</u> 1 March 2016***, the situation is simple for providers; regardless of who owns the copyright, medical documents may be uploaded to and used in the My Health Record system without infringing copyright. Medical documents may also be downloaded from, used and shared outside the My Health Record system for healthcare-related purposes, without infringing copyright.
	• For ***documents created <u>before</u> 1 March 2016***, more care is required for providers:
	  ○ where the uploading healthcare provider organisation *<u>owns</u>* the copyright in the document – the document can be uploaded to the My Health Record system;
	  ○ where the uploading healthcare provider organisation *<u>does not</u>* own the copyright in the document – the document must not be uploaded unless the copyright owner grants a broad copyright licence (including the right to sub-license) to the System Operator of the My Health Record system.
	• In practice, it is anticipated that most healthcare organisations will not upload medical documents created before 1 March 2016, unless they own the copyright in that medical document.

RELYING ON INFORMATION FROM THE MY HEALTH RECORD	
14. What if a healthcare provider makes a clinical decision based on information in the My Health Record and the information is wrong?	• Making a clinical decision based on information in the My Health Record is no different from making a clinical decision based on information from another provider – e.g. over the telephone, or from a clinical document authored by a third party. • The My Health Record is not designed to be, and should not be relied upon as being, a complete patient record. The My Health Record is also not designed to replace existing consultation and communication methods that a provider has with a patient. For example, asking the patient about their medications, allergies, adverse reactions and taking a medical history.
CHILDREN	
15. How is consent and the My Health Record managed with children?	• Authorised Representatives (such as a parent or legal guardian) will have control of their child's My Health Record from 0 to 14 years. After a child turns 14, they will be able to choose whether to manage their own My Health Record (from the age of 14 the System Operator presumes that a child has the capacity to make their own decisions in respect of healthcare, this is in line with existing policies of Medicare). If a child chooses not to take control of their My Health Record between 14 and 17, their Authorised Representative can continue to manage their record until they turn 18. • Once a child turns 18, Authorised Representative(s) will automatically lose access to that My Health Record. • A child between the ages of 14-18 who has not taken control of their record, will not have new Medicare Information flow to their record – this is in line with existing policies of Medicare information sharing.
16. Can a child under 14 control their own My Health Record?	• Anyone under 14 who can prove to the My Health Record System Operator they are a 'mature minor' can register themselves and can take control of their existing record. A mature minor needs to prove they have capacity to look after their own health information. Evidence of this could be a letter from their GP.

17. What is the obligation of a healthcare provider where a child requests not to include information in their My Health Record?	• A child between the ages of 14-18 can apply to have their own My Health Record or take control of their existing record. Where a child has control of their own My Health Record, and requests the provider not to upload information, this request must be followed by the healthcare provider. • While a healthcare provider will not know, simply by looking at the My Health Record, whether a child is in control of their own record, a provider can assume that a child aged 14-18 *could* be in control. Before uploading any information, the healthcare provider should ascertain whether the child is managing their own My Health Record, and if the child is managing their record, the provider must not upload the health information which the child has requested not to be uploaded. • Even if a child does not have control of their record, a healthcare provider should use their clinical judgement about whether or not to include that information in the record.
ACCESS BY INSURANCE COMPANIES	
18. Can insurance companies access the My Health Record?	• Insurance companies that are not directly involved in the delivery of healthcare for an individual are not authorised to access the My Health Record. • However, an insurance company that also provides a health service (e.g. optical, dental, allied health services) could become a participating healthcare organisation and access the My Health Record as part of providing care to patients. The healthcare service of the insurance company is prohibited from sharing an individual's health information with any other part of the insurance company that is not directly involved in providing health care to the individual.
19. Can a healthcare provider give copies of documents downloaded from the My Health Record System to WorkCover?	• Once documents are downloaded from the My Health Record into a provider's local clinical information system, use and disclosure of those documents are subject to local privacy laws – such as the Privacy Act, or state/territory privacy legislation. • A provider who is requested to give information to WorkCover should treat My Health Record system documents saved in their clinical information system the same as other third party clinical documents saved in their system. As is the case now, a provider should use their clinical judgement about providing WorkCover with third party clinical documents.
SECURITY	
20. What security measures are in place for the My Health Record system?	• My Health Record data is stored in Australia, in line with the Australian Government Information Security Manual and Protective Security Policy Framework. The My Health Record system implements high grade security protocols to detect and mitigate against external threats. • Security is a key design element of the system. Design features include audit trails, technology and data management controls, as well as appropriate security measures to minimise the likelihood of unauthorised access to information in a patient's record. In addition to these measures, the My Health Record system is protected by legislation. • Existing clinical standards also apply to information sourced from the My Health Record. Healthcare providers and organisations have an existing duty to keep their patients' health information confidential and secure and that continues for use of the My Health Record system.

Further information is available at nehta.gov.au and myhealthrecord.gov.au.