A guide to *My Health Record:*

for Blood Borne Virus & STI healthcare providers to support their patients

ashm
Australasian Society for HIV, Viral Hepatitis and Sexual Health Medicine

Summary – should my patient use the My Health Record?

The ***My Health Record*** is an online summary of an individual's health information, accessible to any healthcare professional involved in the individual's care. It portends significant benefits for individuals in having their health information more easily accessible. The improved accessibility is of particular benefit for individuals with several comorbidities who have complex care arrangements involving multiple healthcare settings**.** The ability to select which documents are seen by whom allows the record to be tailored to individual preferences, so people who have experienced stigma and are sometimes criminalised due to their BBV status, or drug use or sex work experience, can confidently engage with the system. Nevertheless, questions remain about the security of the system, de-identification of data for research purposes, as well as the complexity of competently navigating the access controls.

Privacy and data use concerns are particularly important to consider for patients with BBVs and/or other potentially stigmatising conditions. A clear understanding is crucial of the system's operation, privacy access control features and the check-and-balances, including through the use of pin codes — and the ability to opt-out of secondary use. Patients can then make an informed decision about engaging with *My Health Record*. Healthcare providers can play a crucial role in talking through with their patients these different facets, to help them decide if/how much to engage in the *My Health Record*. Clinicians need to be aware that a patient may feel compelled to follow their direction about whether or not to engage with the record, so having an open discussion in a judgment-free manner is very important.

Recommendations:

Recommendation 1: Healthcare workers should support patients to understand the different access control measures through discussions and referral to resources.

Recommendation 2: Due to disparate views about the extent to which personal information can be adequately de-identified for secondary use for research, healthcare workers should advise any individuals with concerns about privacy of their health information to opt-out of secondary use.

Recommendation 3: For any young person with concerns about their parents/guardians accessing their health information, healthcare workers should explain to them their entitlement that their parents/ guardians will automatically have their access to the young person's record cut off at age 14. They should also explain that cutting access to parents/guardians can occur before the age of 14 on a case-by-case basis, with clinicians in a position to support the young person's request.

Recommendation 4: Healthcare workers should advise individuals with concerns about the inclusion of MBS and PBS data to activate the record themselves, which will then allow them to opt-out of that data being uploaded.

Overall Recommendation: *Healthcare workers should undertake discussions with patients about the benefits and privacy and security control options, to guide their decision-making around engaging with the My Health Record.*

Overview

My Health Record can hold a range of health information that an individual and their health care professional agree to add to the record. It is designed to facilitate the sharing of health information between healthcare providers for the benefit of the patient. It allows individuals to be more empowered in managing their own health, with individuals being able to tailor what information is shared with whom through the use of PIN codes.

There are however some important issues to discuss with patients regarding privacy and use of data, to help inform their decision as to whether to use the *My Health Record*, and if so, to what extent. For people who experience stigma due to living with a blood borne virus, because they have used drugs or have sex work experience, there may be particular concerns about using *My Health Record* due to the serious consequences from an unwanted disclosure of sensitive information. From the 31 January 2019, anyone eligible for Medicare will have a record created for them, unless prior to that they opted-out of the system. More information on how to opt-out is available here: https://www.myhealthrecord.gov.au/for-you-your-family/opt-out-my-health-record. With the advent of this opt-out system, there will be some individuals who are not aware that they have a record, and so the need for guidance from their healthcare providers is even more important.

Who is this guide for?

This guide has been developed to support healthcare providers in their discussions about the *My Health Record* with patients who may experience stigma and possible adverse consequences due to their living with a blood borne virus (such as HIV, HBV, HCV or co-infections) or sexual health concerns, because they use drugs or have sex work experience. Such individuals may have concerns about using *My Health Record* due to the serious personal consequences which may result from unwanted disclosure of health information, including criminal prosecutions and refusal of services. This guide should help healthcare workers to discuss the nuances of how the record may benefit patients, including how the record's access controls can help protect sensitive information and other issues that should they should be aware of.

What is in this guide?

This guide provides:

- snapshot of the My Health Record.
- explanation of the My Health Record's benefits, and key privacy and security aspects.
- background to the health record.
- exploration of privacy, sharing outside the health system, and security concerns.
- links to further information and referrals.

Section 1.

Snapshot of the *My Health Record*

My Health Record is an online summary of an individual's health information, and can contain a range of health information, including blood test results and discharge summaries — a more comprehensive list of information that can be uploaded is provided in Table 1 which follows. From the 31 January 2019, anyone eligible for Medicare will have a record created for them, unless prior to that they opted-out of the system.

A treating healthcare professional is not legally obliged to seek consent before uploading information, however, it would be good clinical practice to do so. In the event that a patient indicates they do *not* wish particular health information to be uploaded, this must be complied with. Any information that has been uploaded can be edited, modified or deleted by the patient[1]. There are access control features in the form of PIN codes that allow individuals to select which health professionals can see what record. In the case of emergency, the record can be unlocked without the code. At all times the individual can see who has accessed what record through an audit trail feature and redress for any improper handling of information can be taken to the Office of the Privacy Commissioner.

Deletion of record

At any time after the creation of their My Health Record, an individual can have it deleted upon request. At the time of publication, there was no guidance as to how to do this, due to the relatively recent passage of the legislation providing for deletion.

ASHM notes, though, the complexities of access control measures, particularly for those less well engaged, health service literate or where they perceive possible negative repercussions from a provider (e.g. being seen as a difficult patient or fearing that services may be withdrawn or not fully delivered) including by being 'bullied' or coerced into keeping it.

1 https://www.myhealthrecord.gov.au/for-you-your-family/howtos/set-privacy-and-security-controls

What information can be captured?

The table below shows what information can be stored on the record[2]. The third column with 'Consent', indicates information for which it would be good clinical practice to upload only with consent, though this is not a legal obligation. As indicated in the third column, some information may be automatically uploaded.

Type of information	Description of information	Should be done with consent or automatically uploaded?
Health Care information	Medical history only (including test results, medical reports, scan results)	Consent
Medical History summary	Also known as a *Shared History Summary*, this can be compiled and added by the client, with support from health practitioner if desired	Consent
Event Summaries	Clinical documents detailing particular episode/s of care	Consent
Medications that have been prescribed	Healthcare professionals who use clinical software to prescribe and dispense medications can also upload a copy of this information directly to a patient's My Health Record	Consent
Hospital discharge summaries	The discharge summary specification supports a national standard for electronically capturing details of a patient's hospital stay in a structured format	Consent
Referral letters from doctor(s)		Consent
Advance care planning documents		Consent
Personal health notes	These are added by the individual, and can't be accessed by health care providers	Consent
Medicare and Pharmaceutical Benefits Scheme (PBS)	This information is drawn from records of the Department of Human Services	The system may automatically upload – see discussion in section 3 – Privacy
Organ Donation decisions	Those that are included on the Australian Organ Donor Register	The system may automatically upload – see discussion in section 3 – Privacy
Immunisations	Those that are included on the Australian Immunisation Register	The system may automatically upload – see discussion in section 3 – Privacy

Table 1 – *What information can be captured on the My Health Record?*

2 https://www.myhealthrecord.gov.au/for-you-your-family/whats-in-my-health-record

How would My Health Record benefit a patient?

There are a range of benefits for individuals who chose to use *My Health Record*[3]. These include:

- A single location for individuals' health information, allowing easy access for the individual as well the healthcare workers involved in their care. This is of particular benefit for individuals with several comorbidities who have complex care arrangements involving multiple healthcare settings.
- Reducing the repetition of unnecessary bloods tests for people with BBVs.
- Allowing individuals to access health information they would otherwise not be able to see or get and empowering people, particularly those with complex and/or chronic conditions to be more active in the management of their healthcare, including though greater access to their health information, facilitating improved patient-provider communication. More specifically, if the doctor sees the patient has gone for a test or followed through with a referral, this provides a moment where the doctor can positively reinforce the patient's behaviour, thus helping maintain higher levels of motivation (engagement in health). This is particularly important when there are mental health (depression or suicidal ideation) and neurocognitive concerns and the patient is fatiguing, with concomitant compliance challenges, loss to follow-up, or at risk of disengaging in care.
- Reducing risk of adverse drug events though more comprehensive view of current medications.
- Providing improved access to health information when transitioning between care providers.
- Benefiting individuals who live in rural/remote areas, who often need to travel long distances for treatment to see a range of GPs or other healthcare providers[4].

Privacy, sharing information and security issues for BBV affected populations

Patients with a potentially stigmatised condition such as a BBV who may benefit from the *My Health Record* may hold reservations about the privacy and security of sensitive information, due to fears of inadvertent and/or deliberate disclosures that could lead to police investigation, prosecutions, denial of services, and workplace/social stigma.

a) How confident can a person with a BBV be that their privacy will be protected?

To address concerns around the privacy of health information, there are access control mechanisms that allow individuals to select who can see what information so someone with HIV, for example, can limit who sees their HIV-related information.

To upload health information to a patient's *My Health Record*, a healthcare worker does not need the patient's consent. However, to meet ethical obligations, good clinical practice would be to do so only once the patient has provided consent. There is a positive legal obligation not to upload a record if the patient has requested that.

This allows patients to protect their privacy by telling their doctor not to upload information they believe to be too sensitive. To limit access to any information that they *have* decided to have uploaded, there are two control mechanisms; setting a Record Access Code (RAC) to provide access for the individual's *My Health Record* to selected healthcare organisations only; and controlling access to specific documents to limit who can view them through the creation of a special Local Document Access Code (LDAC). To employ these access controls requires a nuanced understanding of the *My Health Record* system by both the patient and healthcare worker, including basic IT literacy. There is further information on access controls in section 3.

3 https://www.myhealthrecord.gov.au/for-healthcare-professionals/what-is-my-health-record/benefits-my-health-record-for-healthcare

4 http://ruralhealth.org.au/media-release/country-lives-can-be-saved-online-health-records

b) Do patients with a BBV have to worry about their information being shared outside the healthcare system?

Some individuals express concerns about the sharing of health information with individuals and entities who are not healthcare providers. Below is an overview of such individuals'/entities' capacities to access the *My Health Record*; there is further information on the following in section 3, as indicated by the hyperlinks.

Government agencies

Amendments were made to the legislation to prohibit disclosure of health information to enforcement agencies or other government departments without a court order. Therefore, BBV affected individuals can be assured that sensitive health information will not be inappropriately disclosed to police.

Secondary use of information for research

Secondary use of health information for research, policy and planning purposes is generally allowed in a de-identified form, unless the individual has opted-out of this use.

Secondary uses must be of public benefit and cannot be "solely" commercial. According to the head of the Australian Digital Health Agency (ADHA) health insurance organisations will not be allowed to participate[5]. IT experts have expressed concerns about how effective de-identification is, given a previous instance of reidentification of individuals following the release of PBS and MBS data[6].

Following last minute amendments, insurers and employers are prohibited from accessing any information in the My Health Record or asking the individual to disclose their information, even where de-identified.

Young people

From the age of 14, young people are deemed competent by the Australian Digital Health Agency of controlling their record and from this point, their parents/guardians will automatically be removed as authorised representatives[7]. From then on, the young person has the option to allow their parents/ guardians access to their record.

c) What security measures exist in the My Health Record

Security of data is important for confidence in the *My Health Record*. According to the ADHA, "*My Health Record* data is stored in Australia, and is protected by high grade security protocols to detect and mitigate against external threats. To help consumers maintain confidence in the integrity of the record, there is the audit log which captures: the name of every healthcare organisation that accessed the record; when it was accessed; the nature of the access, such as viewing a document or uploading a shared health summary; and the role of the person who accessed the record, such as General Practitioner (if available)[8].

Data security experts have expressed reservations about the protections for *My Health Record*, citing data breaches that have recently occurred in Singapore, as well as a previous serious data security breach of the my.gov.au website that can contain among other information, PBS and MBS information.

As there are significant benefits to be gained by patients from using the *My Health Record*, healthcare workers should support their patients to be fully informed of the different privacy and security features, so that the patient can then decide if the record is appropriate for them.

5 Tim Kelsey, head of the (ADHA) https://www.abc.net.au/news/science/2018-07-15/my-health-record-questions-answers-security-privacy-police/9959622

6 https://www.smh.com.au/technology/revealed-serious-flaws-in-mygov-site-exposed-millions-of-australians-private-information-20140514-zrczw.html

7 https://www.myhealthrecord.gov.au/news-and-media/my-health-record-stories/legislation-strengthens-privacy

8 https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/my-health-record-system-security

Section 2.

Background to the My Health Record

a. Timeline

The *My Health Record* first came into being in 2012 with the Personally-controlled electronic health record (PCEHR) as an opt-in record. In July 2018, the Government announced that the *My Health Record* would become opt-out. This means that from the 31 January 2019, all individuals who have not opted-out, will have a record created for them.

b. Number of participants

As an opt-in record, there were over 5 million people enrolled as of May 2018, including some as part of a compulsory sign-up that occurred in several trial regions in 2016[9]. As of October 2018, 1.1 million have opted-out of the *My Health Record*[10] . There are on-going discussions in respect to the opt-out model, and as things evolve, ASHM will advise of any substantive updates.

c. Recent Parliamentary inquiries

The Parliamentary Inquiry into the My Health Records Amendment (Strengthening Privacy) Bill 2018 resulted in an agreement to remove the ability of the My Health Record System Operator to disclose health information in *My Health Records* to law enforcement and government agencies without an order by a judicial officer or the healthcare recipient's consent; and require the system operator to permanently delete all information for someone who has cancelled their *My Health Record*.

A second inquiry into the *My Health Record* was the My Health Record system Senate Inquiry. It released its recommendations in mid-October 2018, in which the majority recommend extending the opt-out period for another 12 months, as well as several privacy-enhancing measures. A number of these recommendations were adopted at the last minute, including strengthening protections for young people and people who have experienced family/domestic violence[11].

At the time of writing, the opt-out period had been extended to 31 January 2019.

Section 3.

What should patients consider before engaging with the My Health Record

a. Privacy

As discussed above, there are access control mechanisms that allow individuals to select who can see what information. To upload health information to a patient's *My Health Record*, a healthcare worker does not need the patient's consent. However, to meet ethical obligations, good clinical practice would be to do so only once the patient has provided consent. There is a positive legal obligation not to upload a record if the patient has requested that[12].

Discussions between healthcare workers and patients are thus crucial to ensuring that only information that the patient wants will be uploaded. The healthcare worker can advise their patient as to the usefulness of a particular piece of health information being uploaded. With BBV-related information, there should be a discussion of any risks associated with uploading the information, versus any benefits in having it uploaded. Patients with HIV may be worried about disclosure requirements prior to having sex,

9 https://www.myhealthrecord.gov.au/news-and-media/media-releases/my-health-record-opt-out-date-announced

10 https://www.smh.com.au/politics/federal/morrison-government-under-pressure-to-rewrite-my-health-record-legislation-20181024-p50bom.html

11 https://theconversation.com/report-recommends-overhaul-of-my-health-record-but-key-changes-not-supported-by-coalition-105290

12 https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/understand-when-you-can-view-and-upload-information

and potential consequent criminal prosecutions. Any decision should be informed by an understanding of the other access control mechanisms, as they may allow patients with stigmatised conditions to tightly control access to sensitive records.

Key access control features include setting a Record Access Code (RAC) to only allow access to selected healthcare organisations and the Limited Document Access Code (LDAC) which allows individuals to restricts access to specific documents within the *My Health Record*[13].

Case scenario:

Kris comes in to see his GP, Doctor Casagrande for an appointment following the previous week's appointment in which he was diagnosed with HIV. After checking how Kris is doing emotionally and psychologically and discussing treatment options, Dr Casagrande begins a discussion about how Kris could use the My Health Record to store HIV-related information.

Dr Casagrande explains that by default anyone involved in Kris' healthcare can access his record, but that there are ways that Kris could have his HIV-related information uploaded to the record while ensuring that is only seen by those involved in his HIV care. Dr Casagrande explains that Kris can limit access to the My Health Record to the Doctor's practice alone, so for the time being, no other healthcare organisations can access it. This would be done by Kris creating a record access code (RAC); only healthcare providers that he provides the code will be able to access his record. Dr Casagrande explains to him that Kris can later provide that code to other trusted healthcare organisations so they too can access his record. Kris says that he does have significant concerns about his HIV-related information being seen by other healthcare organisations not involved in his HIV care, and so will go ahead and create the RAC.

Dr Casagrande adds that for Kris to be extra confident that any HIV-specific information is protected from being viewed by anyone inappropriately, Kris could create local document access codes (LDAC). Kris says that he will use LDAC on the HIV-related information but won't bother using the LDAC on diabetes-related information, in relation to which he also sees his GP.

How to manage MBS and PBS data

When first activating their *My Health Record*, individuals are asked whether they would like two years of Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) data, along with Australian Immunisation Register and Australian Organ Donor Register data, included on their record. However, consent is not sought if a healthcare provider activates the account first[14].

This mechanism to bypass individual's consent could have serious consequences if, for example, hepatitis B anti-virals were uploaded unbeknownst to the individual. Healthcare workers should take the opportunity to discuss this with their patients, and advise them to activate the record themselves, and then exercise the choice to opt-out of MBS and PBS data being added, if they are not comfortable with that.

As using the access controls requires a fair degree of technological sophistication, healthcare providers can support patients by discussing these access controls and providing links/resources that clearly explain how to use these, including to the following:

- *How can I control who accesses My Health Record*[15].
- *Set privacy and security controls*[16].

13 https://www.myhealthrecord.gov.au/sites/g/files/net5181/f/hd117_guide_-_how_to_set_access_controls_v7_accessible_dv003_0.pdf?v=1522029562

14 https://www.itnews.com.au/news/my-health-record-data-could-be-uploaded-without-consent-492029

15 https://www.myhealthrecord.gov.au/sites/g/files/net5181/f/hd117_guide_-_how_to_set_access_controls_v7_accessible_dv003_0.pdf?v=1522029562

16 https://www.myhealthrecord.gov.au/for-you-your-family/howtos/set-privacy-and-security-controls

b. Sharing in non-healthcare context

- Government agencies:
  Amendments were made to the legislation to prohibit disclosure of health information to enforcement agencies or other government departments without a court order.

  This is a significant protection for people whose health conditions and/or behaviours are stigmatised and can be subject to criminal charges, or refusal of Government services/social security payments. Such concerns may exist for people with hepatitis C who have an injecting drug history or people with HIV who may be concerned about being criminally prosecuted for exposure or transmission of HIV, given that prosecutions have occurred across Australia. Healthcare providers can reassure their patients that their *My Health Record* information can only be disclosed to law enforcement authorities or government departments with a court order.

- Secondary use for research:
  As described earlier, de-identified health information will be available for the secondary uses of research, policy and planning, unless the individual opts-out. The information cannot be used for commercial and non-health-related purposes, including direct marketing to consumers, insurance assessments, and eligibility for social security benefits[17]. However, it may be released to commercial organisations if they can demonstrate that the use is consistent with "research and public health purposes" and is likely to be "in the public interest"[18]. Following last minute amendments, insurers and employers are prohibited from accessing any information – including de-identified - in the My Health Record or asking the individual to disclose their information.

  Concerns have also been expressed by IT experts that health information which has been de-identified can relatively easily be data-matched to re-identify individuals, such as when MBS and PBS data were released by the Department of Health in August 2016[19]. In this instance, University of Melbourne's School of Computing and Information Systems "found that patients can be re-identified, without decryption, through a process of linking the unencrypted parts of the record with known information about the individual such as medical procedures and year of birth".

  Given the disparate views about the anonymity of health information de-identified for research, it may be prudent to advise patients with privacy concerns to opt-out of secondary use until the there is more confidence in the de-identification of personal information.

- Young people:
  At the age of 14, a young person's parents/guardians will be automatically removed as 'authorised representatives' and so will no longer be able to access the young person's record. From this point on, the young person has discretion to provide access to their parents/guardians. Healthcare workers should support young people to decide whether it is in their best-interest to limit parental/guardian's access to their *My Health Record*[20].

  If a young person wishes to control their record prior to turning 14 years of age, the Australian Digital Health Agency (ADHA) will consider their competency on a case-by-case basis. This may include obtaining documentation from healthcare providers in support[21].

17 https://www.healthcareit.com.au/article/my-health-record-identified-data-be-made-available-third-parties

18 https://www.health.gov.au/internet/main/publishing.nsf/Content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf

19 https://www.smh.com.au/technology/australians-health-records-unwittingly-exposed-20171218-p4yxt2.html

20 https://www.abc.net.au/news/science/2018-07-26/my-health-record-teenagers-medical-privacy-concerns/10030762

21 https://www.oaic.gov.au/individuals/privacy-fact-sheets/health-and-digital-health/privacy-fact-sheet-21-young-people-and-the-my-health-record-system

- Protections for victims of domestic and family violence:
  According to the system operator, the ADHA is not obliged to notify people of certain decisions if doing so would put another person at risk. In addition, "parents subject to a court order, where they do not have unsupervised access to their child, or who pose a risk to the life, health and safety of the child or another person will no longer be eligible to be an Authorised Representative."[22]

c. Security

According to the ADHA, "*My Health Record* data is stored in Australia, and is protected by high grade security protocols to detect and mitigate against external threats. The system is tested frequently to ensure these mechanisms are robust and working as designed." An important safeguard to protect the information stored within the system, is the audit trail. The audit log displays:

- The name of the healthcare organisation that accessed the record;
- When it was accessed;
- The nature of the access, such as viewing a document or uploading a shared health summary; and
- The role of the person who accessed the record, such as General Practitioner (if available)[23].

Individuals can also set up an email or SMS alert for when a healthcare organisation accesses your record for the first time[24].

Data security experts have expressed reservations about the actual protection for *My Health Record*, citing data breaches that occurred in Singapore in July 2018 when hackers stole the stole the personal information of about 1.5 million people from the government health database[25]. They have also cited a previous serious data security breach of the my.gov.au website in 2014; this website can contain among other data, PBS and MBS information[26].

For anyone who is dissatisfied with the handling of their health information by the ADHA or a healthcare provider, they can contact the Office of Australian Information Commissioner[27].

22 https://www.myhealthrecord.gov.au/news-and-media/my-health-record-stories/legislation-strengthens-privacy

23 https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/my-health-record-system-security

24 https://www.myhealthrecord.gov.au/for-you-your-family/howtos/see-who-has-viewed-my-record

25 https://www.smh.com.au/business/consumer-affairs/attack-on-singapore-health-database-steals-details-of-1-5m-including-pm-20180720-p4zsre.html

26 https://www.smh.com.au/technology/revealed-serious-flaws-in-mygov-site-exposed-millions-of-australians-private-information-20140514-zrczw.html

27 https://www.oaic.gov.au/about-us/contact-us

Section 4.

Resources and additional reading

a. Guidance for healthcare workers on using the *My Health Record*
The ADHA has created resources to support healthcare workers understand the *My Health Record*, including their obligations in terms of information handling:
https://www.myhealthrecord.gov.au/for-healthcare-professionals

The AMA has provided some guidance for clinicians:
https://ama.com.au/gp-network-news/my-health-record

The office of the Privacy Commissioner has provided guidance specifically for healthcare providers:
https://www.oaic.gov.au/myhealthrecord/

b. Guidance for individuals on using the *My Health Record*
The ADHA has created many resources to support individuals to understand the *My Health Record*:
https://www.myhealthrecord.gov.au/for-you-your-family

For information specifically about opting-out:
https://www.myhealthrecord.gov.au/for-you-your-family

c. Privacy Commissioner information and complaints
The Office of the Privacy Commissioner (OAIC) has developed a range of resources to support individuals and organisations understand the privacy aspects of the *My Health Record*:
https://www.oaic.gov.au/privacy-law/other-legislation/my-health-records
https://www.oaic.gov.au/individuals/privacy-fact-sheets/health-and-digital-health/

Any individual who is dissatisfied with the handling of their health information by a healthcare provider or the Australian Digital Health Agency can contact the OAIC:
https://www.oaic.gov.au/about-us/contact-us

d. Community organisations have developed resources to support key people affected by BBVs
Positive Life NSW has developed the following resource(s) to support people with HIV:
https://www.positivelife.org.au/blog-advocacy-and-policy/opting-out-of-my-health-record.html

Hepatitis Australia has a comprehensive appraisal of *My Health Record:*
https://www.hepatitisaustralia.com/my-health-record/

Scarlet Alliance has developed a resource for sex workers:
http://www.scarletalliance.org.au/library/MyHealthRecords/