



28/06/2018

My Health Record Information Brief for Sex Workers

What is the My Health Record system?

My Health Record (MHR) is an electronic health record and the MHR system is a centralised database that retains all the MHRs. The MHR system has been around for more than five years. It is currently available as an opt-in service. This means that an individual must provide informed consent to create a MHR. There are already five million people with a MHR.

On the *16 July 2018*, MHR will move to an *opt-out* model with a three-month period to actively remove consent to prevent a MHR being created for all Medicare recipients by default. This means between the 16th of July and 15th October, you will have the opportunity to prevent a MHR being created on your behalf after the opt-out period ends. Once a MHR has being created under your name, you can access your MHR online where you can add, restrict or 'deactivate' information and apply other control features.

What information does MHR collect?

MHR record can store information, such as and not limited to:

- summary information uploaded by your doctor, such as discharge, follow-up care, referral letters, and event and health summaries;
- immunisation records;
- allergy information and any previous adverse reactions;
- data from your specialist, like psychologist or physiologist;
- data from your pharmacist such as prescription documents;
- Medicare and pharmaceutical benefits scheme information stored by the Department of Human Services;
- organ donation decisions;
- your pathology lab collection and results, such as blood tests; and
- your diagnostic imaging collection and results, such as x-ray reports.

Who can access your MHR?

Your MHR can be accessed by healthcare providers like doctors, specialists and hospital staff, in accordance with your privacy controls. The *Framework to guide the secondary use of MHR system data* indicates that MHR data can be accessed and used by third parties for 'research and public

health purposes¹, such as for surveillance or monitoring of individuals or populations, clinical trials and research. Third parties are granted access to MHR data for 'research and public health purposes' by the MHR Secondary Use of Data Governance Board. Individual consent of MHR holders is not required when granting access to third parties for 'research and public health purposes'. Additionally, the *MHR Act 2012* (Cth), the act governing the operation of the MHR system, indicates that MHR data can be released to third parties, such as insurance companies and 'enforcement' bodies, for purposes that are unrelated to health, such as when providing indemnity cover for health care professionals and for the prevention or prosecution of a crime without the need for a subpoena.²

What are the intended benefits of the MHR system?

- MHR will enable people to view their health information online, without the need to go to a healthcare provider. As a result, MHR could support people in participating more in their treatment decisions and support self-management of their healthcare.
- Once a MHR has been created, you can add, 'deactivate' (otherwise referred to as 'effectively delete') and monitor who has access to your MHR. You can monitor who has access to your MHR by creating access or pin codes which you can give to your healthcare providers to grant access to specific data on your MHR. Once a MHR has been created, you can still 'deactivate' your MHR data, however, it is not possible for you to completely delete the MHR or any of the data that has been uploaded onto the record. 'Deactivated' MHR data is retained in the MHR centralised database, can still be viewed by the MHR holder and accessed by law enforcement, however, it cannot be seen by healthcare providers.
- MHR may reduce unnecessary duplications, such as duplication of immunisations or tests, as you can retain a record of your health information and share this information with healthcare providers at your discretion.
- MHR can assist with better coordinating your health care, particularly for people with chronic or complex conditions as it allows all your health information from various healthcare providers to be uploaded onto a centralised database that can be accessed easily by the healthcare provider you have approved access to. For example, if you change doctors, with your consent, all of your test results and medical information can be easily accessible to your new doctor without the hassle of transferring your file to a new place.
- MHR may assist people in an emergency situation. For example, if you need emergency care and are unable to speak, healthcare providers can request from the MHR system for the privacy controls to be lifted for a maximum of 5 days if they 'reasonably believe that access to the My Health Record is necessary to lessen or prevent a serious threat to public health or safety'.³ This means healthcare providers in this emergency setting will have access to hidden or password protected records.
- MHR could assist healthcare workers in providing more informed health care as your medical history can be retained in one centralised database.

¹ Department of Health. (2018). *Framework to guide the secondary use of My Health Record system data*. [http://www.health.gov.au/internet/main/publishing.nsf/Content/F98C37D22E65A79BCA2582820006F1CF/\\$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf](http://www.health.gov.au/internet/main/publishing.nsf/Content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf). pg 2.

² *My Health Record Act 2012* (Cth).

³ Australian Digital Health Agency. (n.a). Emergency access. Retrieved on 27/06/18 from <https://www.myhealthrecord.gov.au/for-healthcare-professionals/emergency-access>.

What are the risks of MHR?

- When a MHR is created, the MHR settings are, by default, set on the lowest privacy setting for the widest sharing of your health information. You can change your privacy settings to restrict who can view your information. Changing your privacy settings requires the MHR holder to understand how the MHR system works, understand the content of each document uploaded into your MHR which may include complex scientific and medical information, make an assessment of the 'sensitivity' of the information, and who you want to share that information with. For those who have chronic or complex needs, such as people with HIV (including sex workers with HIV), you will likely have a lot of medical documentation that you will need to assess whether you want that information uploaded, 'deactivated' and/or shared.
- If a person chooses not to opt-out of the MHR system, registered healthcare providers are able to start uploading your health data into your MHR. This health data can be accessed by all other health professionals involved in your treatment and care unless you actively restrict their access. There is no requirement for a healthcare provider to obtain consent on each occasion prior to uploading clinical information. However, you can request a healthcare provider to not upload a particular document if you do not want this information on your record and the healthcare provider is obliged to follow your request.
- Your MHR record is owned by the federal government. Once a MHR is created and data is uploaded onto your MHR, it can never be completely deleted. You can, however, 'deactivate' data which means that the 'deactivated' data cannot be seen by healthcare providers but will be retained in the centralised MHR database. For sex workers, if you ever disclose your sex work or HIV status, or drug use and it is uploaded onto your MHR, it can never be completely deleted.
- The *MHR Act 2012* (Cth) allows for a number of third parties to access MHR data in a wide range of circumstances, such as for 'research and public health services' and reasons unrelated to health. For example, the *MHR Act 2012* (Cth) allows for MHR data to be accessed by an 'enforcement body' without the need for a warrant or subpoena, such as the police, the immigration department and a number of other departments, if it is 'reasonably' believed that access is necessary in the:
 - a) 'the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - b) the enforcement of laws relating to the confiscation of the proceeds of crime;
 - c) the protection of the public revenue;
 - d) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
 - e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.'⁴

⁴ Ibid. Section 70.

Due to the inconsistency of laws around sex work which vary state by state and the pervasive stigma and discrimination against us, having a permanent record of our sex work that can be accessed by a number of third parties without our consent should be considered in assessing our decisions around MHR. For sex workers there are additional considerations as our health is legislated under the criminal law in some jurisdictions. Vulnerability to the sharing of this information without the need for consent or a subpoena poses legitimate concerns for sex workers.

- Additionally, the 'third parties' that this information can be accessed may not have a holistic and human rights-based understanding of health raising further concerns about the potential for misinterpreting our health information.
- The Federal Government has stated that the MHR data will be de-identified when used for scientific or medical research. However, even if data is de-identified, it is still possible *re-identify* data. Last year, academics from Melbourne University demonstrated that it is already possible to identify people from supposedly de-identified health data from the Australian Medicare Benefits Scheme and the Pharmaceutical Benefits Scheme.⁵ It is already a danger that such information can reveal 'if someone is on HIV medication, has terminated a pregnancy, or is seeing a psychologist.'⁶ Also, it is more difficult to de-identify data for people from multiple sub populations and/or smaller communities, and the risks of re-identification are heightened.
- Currently health information stored in medical files can only be accessed by a third party provided they gain court approval. The *MHR Act 2012* (Cth) allows third parties, such as the department of immigration, law enforcement and insurance providers, to access MHR data without the MHR holder's consent or court approval in a range of circumstances. As a result, the *MHR Act 2012* (Cth) effectively lowers existing privacy health protections. Sex workers have a long history of having our sex work used to discriminate against us in legal, healthcare, goods and services, accommodation and many other settings. As sex workers in Australia do not have consistent or adequate anti-discrimination protections, sex workers who are discriminated against on the basis of sex work status have little or no legal avenues to redress discrimination.
- For sex workers experiencing multiple layers of criminalisation, stigma and discrimination, MHR may make retaining health privacy more difficult. For example, MHR can be used to prosecute HIV or STI related offences against sex workers with HIV or STI, particularly those operating in jurisdictions that explicitly criminalise sex workers with HIV or STI.
- There are also concerns that even if a sex worker does not disclose their HIV status or sex work, other information recorded in MHR could be used to determine an individual's sex work or HIV status. For example, the frequency of sexual health tests and results, referrals to specialists, notes from consultations with psychologists and prescriptions or records of PEP, PrEP or HIV medication could be used to infer sex work, HIV or drug use status.

⁵ Culnane, C., Rubinstein, B. I., & Teague, V. (2017). Health Data in an Open World. REF: <https://arxiv.org/abs/1712.05627v1> Accessed at 28/06/18

⁶ Badge, J. (2018). *Damaging our trust: Why my health record lets down sexual and gender minorities*. Star Observer.

How can you protect your privacy with MHR?

- You can opt-out of the MHR system between 16th July and 15th October, before a MHR is produced automatically for you.
- If you choose to have a MHR, you can control who views your health information by accessing your MHR online and changing your privacy settings or 'deactivating' data. However, if you 'deactivate' data, the information is not deleted, and a copy of the data will be retained in the MHR system.
- You can choose what information is uploaded onto your MHR by explicitly indicating to your healthcare provider that you do not want your health information uploaded each time you visit them.