SHARED ELECTRONIC MEDICAL RECORDS

MY HEALTH RECORD

Changes from an opt in to an opt out model of the Federal My Health Record (*MHR*) system have reignited concerns about whether appropriate safeguards are in place to protect the privacy of patients in Australia, when their health records are uploaded onto the MHR database.[1] To increase participation by healthcare providers and patients, the health records of all Australians will automatically be uploaded onto the database unless they opt out between 16 July and 15 October 2018.[2] There will be ability to opt out after this date, however a My Health Record cannot be deleted once it has been created. It can only be deactivated and removed from the view of bot h the patient and the healthcare provider.

The MHR system is the Australian government's digital health record system containing online summaries of an individual's health information. The advantage of an interoperable MHR system is portability, facilitated communication between healthcare professionals, systemised medication and allergy reviews, and emergency access for first line responders. However, these benefits could also be achieved by giving patients meaningful control over their records rather than implementing an opt out model.

The legislative framework for the MHR system is the *My Health Records Act 2012 (MHR Act), My Health Records Rule 2016,* and *My Health Records Regulation 2012*. If a healthcare recipient is registered in the MHR system, a healthcare provider may upload health information about the patient to the MHR system, unless the record is one which the patient has advised the healthcare provider not to upload or the record is not to be uploaded under prescribed laws of a State or Territory. Health information may be collected, used, viewed and shared from a patient's MHR for the purpose of providing healthcare to the patient, subject to limited access controls set by the patient (or if none are set, default access controls).

<u>Opt in v.opt out</u>

Schedule 1 of the MHR Act permits the Minister to apply the opt out model to all healthcare recipients in Australia if, after a trial, "the opt out model results in participation in the My Health Record system at a level that provides value for those using the My Health Record system". In response to low opt in numbers the Minister is unilaterally applying the opt out model. This is despite recent survey results claiming that over 60% of Australians would not consider opting in and that 51% of Australians are concerned about the privacy and security of their health information.[3] When referring to the proposed legislation in 2015, Phillip Ruddock stated that "to be capable of justifying a proposed limitation of human rights," (in this case, privacy) "a legitimate objective must address a pressing or substantial concern and not simply an outcome regarded as desirable or convenient." [4] The move from an opt in to an

[1] Alexander, H. (Oct 15, 2015) 'Significant privacy concerns' over myHealth system *The Sydney Morning Herald*

[2] To support the uptake of digital health services, the Council of Australian Governments (COAG) Health Council approved Australia's National Digital Health strategy (2018-2022).

[3] GlaxoSmithKline Australia Pty Ltd. (2018) "Digital Healthcare Attitudes in Australia" http://au.gsk.com/en-au/behind-the-science/everyday-health/digital-healthcare-attitudes-in-australia/

[4] Alexander, H. (Oct 15, 2015) 'Significant privacy concerns' over myHealth system *The Sydney Morning Herald*

opt out model is about achieving the convenient outcome of getting registration numbers up and is not related to improving health outcomes or dealing with patient's issues about trust and privacy.[5]

To permit patients to control their privacy settings and make informed choices, the process of opting out should be easily understood, requiring minimal time and effort.[6] In practice, the opt out process is cumbersome to implement and, in many cases, patients do not have the capability or capacity to exercise these controls, for example, if confined in hospital, those with mental health problems or those just trying to navigate to the page that allows opt out.

In summary, the process of opting out is not simple, particularly for those who are not internet savvy. Patients should be aware that opting out after mid October 2018 will only deactivate access, not delete the records uploaded.

Consent

An opt out model does not provide for participants to give meaningful consent to their participation over the collection, use and disclosure of health information.[7] The main elements of consent include being adequately informed, voluntary consent, specific consent and the capacity to understand and communicate consent. Voluntary consent depends on whether an individual has a clear, effortless option not to consent. However, opt out consent relies on inertia and apathy rather than encouraging control by an informed participant.

The MHR system operates on the basis that patients provide "standing consent" to the uploading of documents by healthcare providers until that consent is withdrawn by the patient.[8] Standing consent is neither specific nor informed. It places the burden on the patient to check every document before it is uploaded.

The MHR Act limits when and how health information can be collected, used and disclosed. Unauthorised collection, use or disclosure is both a breach of the MHR Act and an interference with privacy. However, one of the exceptions to that prohibition is where an individual has given consent to the use or disclosure.[9] It is concerning that healthcare providers and third parties are able to rely on consent, to obtain sensitive health information from the MHR database, when patients' expectations are that this information is not being shared. The Australian Digital Health Agency is only now scrambling to tighten up its third party agreements to add better data breach notification, data collection and consent

[5] Walsh, D., Passerini, K., Varshney, U. and Fjermestad,J. (2010) Legal issues in the transition to electronic records in health care. n: D'Atri A., Saccà D. (eds*) Information Systems: People, Organizations, Institutions, and Technologies.* Physica-Verlag HD p325

[6] Office of the Australian Information Commissioner "Chapter 7: APP 7 — Direct marketing" https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-7-app-7-direct-marketing

[7] Australian law Reform Commission "Australian Privacy Law and Practice (ALRC Report 108), 62. The Privacy Act and Health Information, Consent" https://www.alrc.gov.au/publications/62.%20The%20Privacy%20Act%20and%20Health%20Information/consent

[8] Australian Digital Health Agency "Digital health and patient consent" https://www.digitalhealth.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/patient-consent; accessed 17 July 2018

[9] S66(2) MHR Act

provisions.[10] This highlights how poorly thought out aspects of the MHR have been and how little regard is given to using the highest standards of consent. As proved problematic in the recent HealthEngine scandal,[11] the option to consent should not be bundled with other purposes nor should providers simply meet the formal requirements of consent.

Given that the elements of consent are muddied in various processes relating to the MHR, patients need to be aware of the options to withdraw or limit their consent.

Access

- *Patient access*- In the default setting, all healthcare providers will be able to access a patient's MHR. Alternatively, the level of access has to be determined by the patient for each healthcare provider they visit. [12] Patients can apply a Record Access Code to the entire record (restricting access except in emergency); or restrict access to specific information in their record or revoke health provider access, by applying a Limited Access Document Code to that specific document.[13]

  Therefore, to quarantine sensitive documents from other health data, every document uploaded from that particular healthcare provider must be restricted by the patient. The practicalities, therefore, of navigating privacy settings end up disadvantaging those that hope to get the most of the MHR but are not internet savvy. Otherwise, patients must flag to their doctor that certain information is not to be uploaded.[14] For example, it may not be appropriate for psychotherapy notes to be made available in general medical records or be made available to non-registered health professionals or health professionals in an unrelated field.

  The MHR system permits patients to choose to be notified by email or text message when a healthcare provider organisation accesses the MHR for the first time or in a medical emergency.[15] However, limiting audit to only first time use and to a healthcare "organisation" ignores the real possibility that information may be accessed by an insecure individual in that organisation, whether authorised or unauthorised, or a hacker. Proper auditing needs to be specific and visible to the patient, permitting them to decide what level of notification is desired.

- *Authorised access and unintentional breach*- The MHR default access control position permits the employees of a medical practice or other authorised organisation (nurses,

[10] Clare Blumer & Pat McGrath (24 July 2018) "My Health Record agency adds 'reputation', 'public interest' cancellation options to app contracts" http://www.abc.net.au/news/2018-07-24/digital-health-agency-changes-my-health-record-app-contracts/10026644; accessed 24 July 2018
[11] Han, E (July 2018) "Scandal-hit HealthEngine axes third party referrals, patient reviews" https://www.smh.com.au/healthcare/scandal-hit-healthengine-axes-third-party-referrals-patient-reviews-20180705-p4zpoe.html
[12]Australian Digital Health Agency "Access by Healthcare Providers" https://myrecord.ehealth.gov.au/portal/help/privacy_and_access/access_by_healthcare_providers#how_do_i_find_the_restrict_access_to_your_my_health_record_page; accessed 16 July 2018
[13] Australian Digital Health Agency (14 May 2018) "Media release - My Health Record opt out date announced" https://www.myhealthrecord.gov.au/news/media-release-my-health-record-opt-out-date-announced
[14] AMA Position paper (2016) Shared Electronic Medical Records, p2. https://ama.com.au/position-statement/shared-electronic-medical-records-revised-2016; accessed 16 July 2018
[15] Australian Government, Australian Digital Health Agency, My Health Record https://www.myhealthrecord.gov.au/for-you-your-family/howtos/see-who-has-viewed-my-record

admin staff) to access a patient's health record, for the purpose of providing healthcare to the patient.[16] This means that legitimate users could take advantage of their access for other than patient care (e.g. ex-spouses and coworkers). Commonly, the incidence of negligence or human error increases with increased access.[17] To safeguard against unintentional breaches, sensitive records should be sequestered and disclosure limited to the minimum persons necessary to perform a task.[18]

S.70 of the MHR Act permits the system operator to disclose health information when it "reasonably believes" it is necessary to investigate or prosecute a crime, to counter "seriously improper conduct" or to "protect the public revenue". A Parliamentary Library advice has warned that this represents "a significant reduction in the legal threshold for the release of private medical information to law enforcement" as there is no routine requirement to obtain a warrant. It is clear that the federal government is concerned about this, as the Parliamentary Library advice was withdrawn and later reissued, omitting the relevant line and adding information about the Privacy Act. The advice also noted that, currently, a patient's consent was needed to release their medical records and "law enforcement agencies can only access a person's records (via their doctor) with a warrant, subpoena or court order".[19]

The Privacy Act 1988 does not prevent disclosure without a court order or warrant. Although APP6 permits use or disclosure of health information for a secondary purpose with the patients consent or if the secondary purpose is directly related to the primary purpose of collection, there are exceptions.[20] Most importantly, exceptions apply if the use or disclosure is required or authorised by or under an Australian law (not necessarily with a warrant) or a court/tribunal order; or for an enforcement related activity by an enforcement body (APP 6.2(e)).

In the light of concerns raised by commentators, doctors and privacy specialists, the government has indicated that there will be changes made to the legislation regarding the requirement for a warrant for disclosure of information (as well as the issue of the deletion of records if a person opts out of the system), but the draft legislation is not yet available.

- *Unauthorised access*- Criminal and civil penalties apply if a person collects uses or discloses information from the MHR, without authorisation.[21] However, sanctioning

[16] Unless the patient sets their own access controls.
[17] Negligence is still the leading cause of data breaches in Europe. Kierkegaard, P.(2012) Medical data breaches: Notification delayed is notification denied *Computer Law & Security Review* 28:163-183 at p.183; personal data of 26 million US veterans was stolen from the home of a computer analyst in an apparent burglary. Frieden, T & Walton, M. (May 23, 2006) FBI seeks stolen personal data on 26 mill vets *CNN.com* http://edition.cnn.com/2006/US/05/22/vets.data/
[18] Axelrod, C.W (2015) Ensuring online data privacy and controlling anonymity. in: *Emerging Technologies for a Smarter World* (CEWIT), 12th International Conference & Expo http://ieeexplore.ieee.org/document/7338156/
[19]Karp, P (28 July 2018) "Police can access My Health Record without court order, parliamentary library warns" https://www.theguardian.com/australia-news/2018/jul/25/police-can-access-my-health-record-without-court-order-parliamentary-library-warns; accesses 30 July 2018
[20] Office of the Australian Information Commissioner Chapter 6: APP 6 — Use or disclosure of personal informationhttps://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information; accessed 30 July 2018
[21] S 59 MHR Act

> those responsible for loss of information or hacking, is, in itself, not an effective deterrent and does not protect patients' privacy.[22]
>
> Singapore, considered one of the most sophisticated cyber security countries, was not able to ward off hackers stealing the health records of 1.5 million Singaporeans.[23] Its government acknowledges that no system is infallible. Creating an enormous data base provides greater opportunity for unauthorised access to information and loss of information, an important factor in the call, globally, for the abandonment of central data storage for health records.[24] The Australian Federal government cannot demonstrate that it has the capacity, or resources, to prevent such unauthorised access.

The MHR system does not provide a clear election not to have certain information uploaded.[25] Patients need to be aware that there is the risk of unauthorised access and unwarranted disclosure of their heath records to third parties and enforcement agencies. Measures to engage privacy settings and to receive access notification, while inadequate, should be used by the patient.

Secondary Use of Data

The Federal government has recently released the "Framework to guide the secondary use of My Health Record system data", which is being introduced in 2020.[26] Patients will be able to opt out of the use of their data, for secondary purposes, by clicking on the 'Withdraw Participation' button. Any data that is classified as being 'Restricted Access' or information remaining after opting out, will not be retrieved for secondary use purposes. However, examples of permitted secondary use of data include development of new and improved health care products and services, clinical decision support systems and technology innovations. These are fairly broad applications.

Although, the Framework will not permit "solely" commercial secondary uses such as direct marketing to consumers, that prohibition is extremely vague. Already, HealthEngine has acknowledged that it has a data-sharing arrangement with the MHR system though the precise nature of that arrangement has not been made public.[27]

---

[22] Shenoy, A & Appel, J. (2017) Safeguarding confidentiality in electronic health records *Cambridge Quarterly of Healthcare Ethics* 26: 337-341 p.339

[23] The Australian (20 July 2018)"Singapore says hackers stole 1.5m health records" https://www.theaustralian.com.au/national-affairs/health/singapore-says-hackers-stole-15m-health-records/news-story/c372cc1f4136a0b93316f0a1a15ffcfe; accessed 24 July 2018

[24] Incidents at City of Hackney in the UK, where 160,000 children records were lost, highlights the problem of why anyone should be able to access so many children's records. Professor Anderson Prof of Security Engineering Cambridge University: in Lansley, A. (Dec 24, 2007) Opposition calls for rethink on data storage *Digital Health* https://www.digitalhealth.net/2007/12/opposition-calls-for-rethink-on-data-storage/

[25] Consumers Health Forum of Australia (June 2015) Submission to the Electronic Health Records and Healthcare Identifiers: legislation discussion paper. p.4

[26] Department of Health (May 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; accessed 16 July 2018

[27] Pat McGrath, Clare Blumer and Jeremy Story Carter, ABC Investigations (26 June 2018) "Medical appointment booking app HealthEngine sharing clients' personal information with lawyers" http://www.abc.net.au/news/2018-06-25/healthengine-sharing-patients-information-with-lawyers/9894114; accessed 16 July 2018

The MHR Act permits rules to be made to use deidentified information for research purposes (s.109 (7A)). In a reaction to recent revelations that this data could be easily reidentified the Commonwealth introduced the *Privacy Amendment (Re-identification Offence) Bill 2016 (Bill*) that adopts a punitive approach towards information security researchers and research conducted in the public interest. At the time that the Bill was introduced, the Privacy Commissioner, Timothy Pilgrim, noted that the Bill is not comprehensive and would not affect those that are exempt from the *Privacy Act 1988 (Cth)*. He also made the point that "Where de-identified information is publicly released, agencies should therefore be mindful that entities outside Australia will be able to access the information but may not be subject to the jurisdiction of the Australian Privacy Act."[28]

The Bill is on hold for the moment and the Framework, is just a framework. Amendments can still be made, so that patients can give explicit consent for each disclosure of medical or health data to a third party, not just a withdrawal or opt out option.

Summary of the NSWCCL position

- NSWCCL does not support the current opt out model in principle and because implementation of the present MHR system exposes Australian citizens to unnecessary and unacceptable privacy risks. Consent in an opt out model relies on apathy rather than encouraging control by the patient. In practice, the MHR opt out process is cumbersome to implement and, in many cases, patients do not have the capability or capacity to exercise the controls to opt out or implement access restrictions. It is recommended that, unless there are specific health reasons for not doing so, individuals opt out of the MHR.
- Once the three month opt out period is over, it will still be possible to opt out but uploaded records will only be deactivated and removed from view. Instead, records should be completely deleted if a person opts outs, at any time.
- Uploading of health records by healthcare providers is permitted by "standing consent" until that consent is withdrawn by the patient. It is recommended that patients exercise their right to withdraw consent and advise their doctors when certain information is not to be uploaded.
- Current audit and privacy measures (and express provisions, such as S.70 MHR Act) do not eliminate the risk of unauthorised access, unintentional breaches and unwarranted disclosure of patients' health records. Proper auditing needs to be specific and visible to the patient, permitting them to decide what level of notification is desired. Disclosure of records should be limited to the minimum number of persons necessary to perform a task. Enforcement agencies should only be able to access the MHR with the appropriate warrants or court orders. In the absence of these measures, patients should avail themselves of existing privacy settings and access notifications.
- The Federal "Framework to guide the secondary use of My Health Record system data" is being introduced in 2020. It is recommended that the Framework be amended to not only more rigorously limit secondary use but also ensure explicit consent for

[28] Office of the Australian Privacy Commissioner "Privacy Amendment (Re-identification Offence) Bill 2016 — submission to the Senate Legal and Constitutional Affairs Legislation Committee" https://www.oaic.gov.au/engage-with-us/submissions/privacy-amendment-re-identification-offence-bill-2016-submission-to-the-senate-legal-and-constitutional-affairs-legislation-committee; accessed 16 July 2018

each disclosure of health data to a third party (not just a withdrawal/opt out option or bundled consent).

Michelle Falstein
Convenor
Privacy Action Group
NSW Council for Civil Liberties