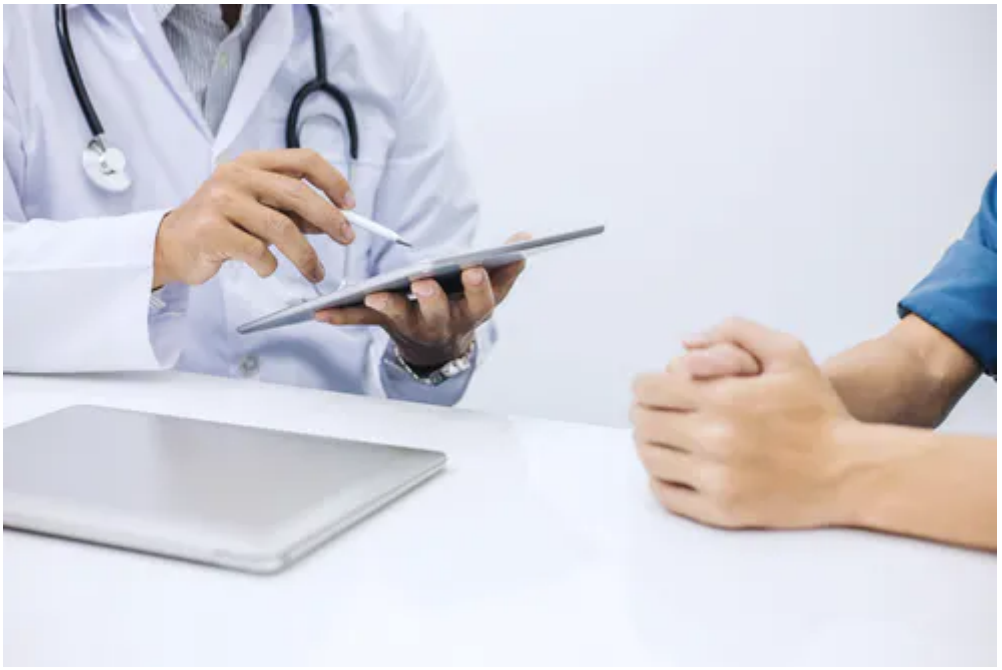
THE CONVERSATION

Academic rigour, journalistic flair



The opt-out period for My Health Record runs from July 16 until October 15. Shutterstock

My Health Record: the case for opting out

July 16, 2018 4.52pm AEST •Updated July 17, 2018 9.37am AEST

The My Health Record (MHR) opt-out period begins today and you have until October 15 to decide whether or not to be part of the scheme. You can read the case for opting in to My Health Record here.

Authors

Katharine Kemp

Lecturer, Faculty of Law, UNSW, and Co-Leader, 'Data as a Source of Market Power' Research Stream of The Allens Hub for Technology, Law and Innovation, UNSW

Bruce Baer Arnold

Assistant Professor, School of Law, University of Canberra

David Vaile

Teacher of cyberspace law, and leader of the Data Protection and Surveillance stream of the Allens Hub for Technology Law and Innovation, UNSW Faculty of Law, UNSW

Unless you take action to remove yourself from the My Health Record (MHR) system, the federal government will make a digital copy of your medical record, store it centrally, and, as the default, provide numerous people with access to it.

If you don't opt out during this period and later choose to cancel your record, you will no longer be able to access that record but the government will continue to store it until 30 years after your death. You will need to trust that it will not be breached.

There are three main problems with the MHR scheme.

Read more:* *The latest health data breach is one reason why I'll be opting out of MyHealthRecord

1. It can't be relied upon as a clinical record

Contrary to what many Australians may believe, MHR is *not* a clinically-reliable medical record, and was not designed to be. It is not up-to-date and comprehensive. As the Office of the Australian Information Commissioner (OAIC) points out:

> *The My Health Record system contains an online summary of a patient's key health information; not a complete record of their clinical history.*

If, for example, a doctor were treating a child in an emergency, the doctor could *not* rely on an MHR to know what medications the child has been prescribed up to that date. In an emergency, an unreliable record is a distraction, not a help.

Many doctors have in fact objected to the incompleteness and lack of utility of the MHR. A recent poll on the AMA's doctors portal suggests 76% of respondents think the MHR will not improve patient outcomes while 12% think it will.

Notwithstanding this fundamental deficiency, the government is pushing ahead with an inherently risky scheme.

2. It creates a security risk

If you read the very long (7,800 words) privacy policy for MHR, you'll see that the Australian Digital Health Agency (ADHA) itself states there are risks from the online transmission and storage of our

personal information in this system.

Health data is prized by hackers

We have witnessed a stream of health data breaches in Australia and overseas, and the incentives for these breaches are only increasing.

Storing records digitally with online access greatly increases their accessibility for criminals, hackers and snoopers. Health records are valuable as a means of identity theft due to the wealth of personal information they contain. They are a huge prize for hackers, fetching a high price on the Dark Web.

Read more: After the Medicare breach, we should be cautious about moving our health records online

---

You won't know who has seen it

It won't just be your doctor who has access to this centralised digital record of your personal health information. The default position is that numerous people will have access – doctors, pharmacists, physiotherapists, nurses, and unidentified staff of various organisations.

MHR's access-logging system does not track which individuals are accessing records, only institutions, which means you won't be able to tell who has seen it. Even without a technical hack, that will make it almost impossible to keep your information secure in this system.

De-identification is risky

The government is also planning to allow access to your health information for research purposes by "de-identifying" your information. That means the data should not be able to be linked to a particular individual.

But the national government has a bad record for successfully de-identifying health information.

In 2016, the government released a data set that included information on a large number of patients spanning 30 years. It was meant to be de-identified.

IT researchers at Melbourne University quickly demonstrated it could be re-identified and linked to the individuals concerned. Such re-identification risk will only grow, as data sets proliferate and tools get smarter.

Third-party access jeopardises security

MHR also permits external health apps to access your records. According to the legislation, this should only be done with your consent.

Unfortunately, and predictably, health apps are already securing "consent" through obscure, standard form contracts so you might not be aware the app owner could sell your sensitive medical information to others.

Last month, the ABC revealed one such health app (HealthEngine) was selling patient information to law firms, so patients with serious conditions and injuries were contacted repeatedly by strangers pushing them to pursue legal claims. Many didn't know how their sensitive medical information was revealed.

The ADHA's website has published a report on the woefully inadequate privacy policies of mental health apps, and yet these apps might be authorised to access your MHR data with your supposed consent.

Read more: HealthEngine may be in breach of privacy law in sharing patient data

---

3. An 'opt-out' scheme goes against best practice

Critically, the opt-out consent mechanism for MHR flies in the face of global best practice for informed consent – and our own federal privacy regulator's guidelines on the sort of consent necessary for use of health information.

Consent for use of personal information should be express, fully informed, easy to understand, and should require action on the part of the individual.

MHR disregards all of those principles.

MHR does not seek your *express* consent. Instead, if you do not take the necessary steps before 15 October, your health records will automatically be copied, stored and shared.

You will also not be *fully informed*. There will be no national television, radio or print media campaign to advertise the MHR scheme, which many Australians have misunderstood in the past. The government will not even send you a letter to tell you about this scheme, let alone its very serious risks.

By contrast, the OAIC says organisations seeking individual consent to use personal information should generally:

> *… ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent.*

and:

> *… seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.*

Even if implied consent were acceptable (and it is not), the OAIC states further that an organisation:

> *… should not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. Nor can an entity establish implied consent by asserting that if the individual knew about the benefits of the collection, use or disclosure, they would probably consent to it.*

Read more:* *App technology can fix the e-health system if done right

The time to opt-out is now

MHR is likely to create very limited benefits for many, if not most, Australians. It creates unacceptable security risks for our most sensitive personal information. And the government's method of obtaining "consent" goes against international best practice.

If the MHR scheme were properly advertised, fully explained and Australians given a choice whether to opt-in, Australians could make an informed choice about whether the limited benefits justify the substantial risks to their sensitive information.

Those concerned about the security of their health information will need to take steps now to remove themselves from the MHR system.

This article has been updated to reflect that the ADHA report on the privacy policies of health apps focused on mental health apps.

Privacy **Data security** **Data privacy** **Medical records** **My Health Record** **Medical Information**