Australian Government
Australian Digital Health Agency

28 August 2017

Senate Standing Committee on Finance and Public Administration Inquiry into the Circumstances in which Australians' Medicare Information has been made Available on the 'Dark Web'

This submission is made by the Australian Digital Health Agency to the Senate Standing Committee on Finance and Public Administration inquiry into the circumstances in which Australians' Medicare Information has been made available on the 'Dark Web'. This submission focusses on clause c of the Inquiry's Terms of Reference 'the implications of this breach for the roll out of the opt-out My Health Record system'.

As the System Operator of the My Health Record System, the Australian Digital Health Agency welcomes opportunities for improvement to the security and operation of the System which can be learnt from this event. This submission addresses:

- the security practices in the My Health Record system which protect against the unauthorised disclosure of health information including Medicare information;
- access to the My Health Record system; and
- the roll out of opt-out participation in the My Health Record system.

1. About the Australian Digital Health Agency

Tasked with improving health outcomes for Australians through the delivery of digital healthcare systems for Australia, the Australian Digital Health Agency (the Agency) commenced operations on 1 July 2016. The Agency leads the coordination, implementation and ongoing development of the National Digital Health Strategy - *Safe, seamless and secure: evolving health and care to meet the needs of modern Australia* - which was approved by the Council of Australian Governments in August 2017 (The Strategy is available online at http://digitalhealth.gov.au/about-the-agency/publications/australias-national-digital-health-strategy).

The Agency is responsible for all national digital health services and systems, with a focus on engagement, innovation and clinical quality and safety. Our focus is on putting data and technology safely to work for patients, consumers and the healthcare professionals who look after them. The Agency is the System Operator of the My Health Record system and has responsibility for the effective and secure operation of the My Health Record system.

What is My Health Record?

My Health Record is a secure online summary of an individual's health information. An individual can control what goes into their record, and who is allowed access the record. Individuals can choose to share their health information with their doctors, hospitals and other healthcare providers and can authorise others, such as carers, to access and manage their record.

Currently there are over 5.1 million individuals registered for a My Health Record, around 21 % of Australia's population. Nearly 10,000 healthcare provider organisations are currently participating in the System with over 2,750,000 clinical documents uploaded to the system including shared health summaries, discharge summaries and pathology reports.

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 56 Pitt Street, Sydney, NSW 2000
Phone +61 2 8298 2600 Facsimile +61 2 8298 2666
www.digitalhealth.gov.au

Why is there a need for a digital record system?

One in three general practitioners (GPs) will see a patient for whom they have little or no health information. Many patient records are created as paper files which are regularly transmitted between healthcare providers using unsecure email, fax machines and by post. The My Health Record offers health professionals secure digital access to a patient's record at the point of care, wherever that may be.

The My Health Record system provides significant benefits to Australians. Benefits include avoided hospital admissions, fewer adverse drug events, reduced duplication in diagnostic tests, better coordination of care for people seeing multiple healthcare providers, and better informed treatment decisions.

The My Health Record system has been supported by a range of healthcare provider leaders including the Australian Medical Association (AMA), the Royal Australian College of General Practitioners (RACGP) and the Pharmacy Guild of Australia. These peak bodies have entered into compacts with Government on behalf of the healthcare providers they represent recognising that electronic health records can play a crucial role in supporting healthcare outcomes. These organisations are committed to the system and are encouraging healthcare providers to adopt use of the My Health Record system into daily practice.

The implementation and development of digital health activities are supported by consumers.
The Consumers Health Forum values the importance of empowering Australians to be makers and shapers of the health system and recognises that digital health developments, including the My Health Record system, can support individuals to better manage and coordinate healthcare leading to better patient experiences, quality care and better health outcomes.

2. Access to the My Health Record system

An individual's Medicare card number does not allow My Health Record information to be accessed. Additional information is required to authenticate consumers and healthcare provider identity.

A healthcare provider can access the My Health Record system through the National Provider Portal, operated by the Agency, or through a local clinical information system. Both processes require the healthcare provider to be an employee of a registered healthcare provider organisation.

Healthcare Provider Access to the System through the National Provider Portal

In order for an individual healthcare provider to access the My Health Record system through the National Provider Portal:

- the healthcare provider's organisation must be registered to participate;
- a 'Responsible Officer' or 'Organisational Maintenance Officer' for the organisation must link the individual healthcare provider to the organisation and authorise their access to the National Provider Portal. This can be done online using the Health Professionals Online Service (HPOS), over the phone or through a written application form;
- the individual healthcare provider must apply for a National Authentication Service for Health Public Key Infrastructure (NASH PKI_ certificate, this certificate is linked to their Healthcare Provider Identifier for Individuals (HPI-I) so they must also be registered with the Healthcare Identifiers Service.

Organisation Maintenance Officers and Responsible Officers are the individuals responsible for acting on behalf of a healthcare provider organisation in relation to their participation in the My Health Record system. The identity of these individuals is verified at the time a healthcare provider organisation is registered.

The identity of individual healthcare practitioners accessing the My Health Record National Provider Portal is verified either:

- by the Healthcare Identifiers Service when the practitioner requests a HPI-I be assigned by the Department of Human Services;
- by the Australian Health Practitioner Regulation Agency (AHPRA) when the practitioner registers;

- by the Department of Human Services when the practitioners register for Provider Digital Access (PRODA).

Healthcare Provider Access to the System through their Clinical Information System

To get access to the My Health Record System through a clinical information system a health practitioner is required to:

- install conformant clinical software on a participating organisation's IT system;
- apply for a NASH PKI certificate for healthcare provider organisations;
- install the NASH PKI;
- begin accessing the system using local log on details.

Some, but not all clinical information systems record and use the HPI-I of the healthcare provider accessing the system. Participating healthcare provider organisations may choose to provide access to the My Health Record system for staff who are not healthcare providers. For example, administrative staff may be provided access to the My Health Record system for the purposes of retrieving information from the system for use by healthcare provider or uploading documents to the system. Provided these individuals are authorised to access the system by the participating healthcare provider organisation, and the patient would reasonably expect this activity to occur, this access is authorised under legislation.

Once a healthcare provider or other authorised employee of a healthcare provider organisation has access to the My Health Record system, they can view information in the individual's My Health Record if they know:

- name;
- gender;
- date of birth; and
- one of the following identifiers:
    - Medicare Card number & Individual Reference Number (IRN); or
    - DVA Card number; or
    - the IHI of the individual.

However, it should be noted that in order for it to be a lawful activity, the health practitioner needs to have a legitimate reason for accessing the record. Healthcare providers are also bound by their broader obligations as registered healthcare providers and as entities within the remit of the *Privacy Act 1988*.

Options are provided to enable healthcare providers without all this information to access the system through the use of other demographic information, such as address details as they are recorded in the Medicare database. The intention of this is to enable healthcare providers to access records where local records differ from the Healthcare Identifiers (HI) Service (the HI Service leverage Medicare enrolment data). Differences in data can occur through name spelling differences, name changes and differences in information provided by the individual to different healthcare providers.

Consumer access

To create a record a consumer must provide their Medicare card number and their address as recorded by Medicare, along with additional verification details such as their bank account number and information about their last doctor's visit for which a Medicare claim was made.

3. Security and privacy practices in the My Health Record system which protect against the unauthorised disclosure of health information

As the System Operator, the Australian Digital Health Agency is responsible for the security and privacy of the My Health Record system. The system complies with the Australian Government requirements for

storing and processing protected information and is regularly tested and audited to confirm that these requirements are met.

Security

The Agency has a comprehensive set of processes and technology controls in place to protect health and personal information in place. The system has strong security which ensures information is only stored and accessed by trusted connected health systems and users such as healthcare providers and consumer.

The Agency's Cyber Security Centre continually monitors the system for evidence of unauthorised access. This includes utilising specialist security real-time monitoring tools that are configured and tuned to automatically detect events of interest or notable events. Examples of this include:

- overseas access by consumers and healthcare providers;
- multiple failed logins from the same computer or device;
- multiple logins within a short period of time;
- logins to the same record from multiple computers and devices at the same time;
- high transaction rate for a given healthcare provider;
- certain instances of after business hours access and all instances of emergency access.

The Cyber Security Centre regularly reviews the events of interest based on its knowledge of the likely threats to the My Health Record.

Privacy

Demonstrating a commitment to protecting individuals' privacy is essential for establishing and maintaining the positive and trusted reputation of the Agency and the Government more broadly. The Agency takes a proactive approach to considering and managing its privacy obligations under the *Privacy Act 1988* (the Privacy Act), *My Health Records Act 2012* and the *Healthcare Identifiers Act 2010*. In managing its privacy obligations the Agency aligns itself to the Australian Privacy Principles outlined in the Privacy Act. Managing privacy goes across the full range of Agency activities including:

- design and operation of the My Health Record and supporting systems;
- communication with, and service delivery to, all Australians; and
- interactions with other organisations such as contractors and government agencies.

The Agency also works closely with the Office of the Australian Information Commissioner (OAIC) which has a regulatory oversight role administered under a Memorandum of Understanding with the Agency.

The Agency takes a proactive, privacy by design approach to managing the development and operation of the My Health Record system.

How does the My Health Record system ensure healthcare providers only access the information they should access?

Healthcare providers can only access an individual's My Health Record if they have:

- a healthcare provider or organisational certificate installed (either with NASH HPI-I or HPI-O certificate) on the device or network that they are using to access the record; and
- valid log on details for accessing the National Provider Portal or their local clinical information system; and
- the Record Access Code (RAC) or Limited Document Access Code (LDAC), if an individual has enabled restrictions on their My Health Record.

Healthcare provider organisations are only authorised to access the My Health Record system if they are providing healthcare to that individual. Criminal and civil penalties apply to healthcare providers that deliberately access an individual's My Health Record without authorisation. Penalties include up to two years in jail and significant fines.

As participants in the My Health Record system, healthcare provider organisations are obliged to have a policy in place covering issues of security, authorisation and training. This policy must be communicated to staff and enforced by the healthcare provider organisation. These obligations are outlined in the My Health Records Rule 2016.

Any software that connects to the system undergoes ongoing checks to ensure that it conforms to the system requirements and has authority to access the information. The ability to include information in the My Health Record system is only available to healthcare provider organisations via clinical software that has undergone a rigorous approval process.

What controls do individuals have?

Individuals can control what information is in their My Health Record, and which healthcare provider organisations can access their record. A range of privacy controls are available including:

- Setting a Record Access Code (RAC) which the individual can give to their healthcare provider organisation to allow access to their record, and prevent other healthcare provider organisations from access unless in an emergency;
- Flagging specific documents in their record as 'restricted access', and controlling who can view those documents using a Limited Document Access Code (LDAC) or specifically granted an organisation the ability to view these documents;
- Removing documents from view within their record;
- Asking healthcare providers not to upload information, which must be complied with under the *My Health Records Act 2012*.

An individual can also configure automatic notification via email or SMS when a healthcare provider organisation:

- accesses their record for the first time, or
- uploads certain types of information to their record, or
- views their record in an emergency situation which overrides the access controls in place.

An individual can view a real time log of every access to their My Health Record by a healthcare provider organisation.

4. The Roll out of Opt-Out Participation in the My Health Record system

As part of the 2017-18 Budget, following unanimous support by all State and Territory Governments, the Australian Government announced the creation of a My Health Record for Every Australian, unless they choose not to have one, to be implemented by December 2018.

This decision follows trials of different participation models in 2016. An evaluation of these trials found that an opt-out approach increased both individual and healthcare provider participation and achieved better outcomes in terms of understanding and use of the system. Individuals interviewed as part of the evaluation trials supported an opt-out participation model, particularly when they understood the protections and privacy controls available to them. The evaluation report can be accessed at (http://www.health.gov.au/internet/main/publishing.nsf/content/ehealth-evaluation-trials).

In preparing to implement opt-out participation the Agency is undertaking activities such as:

- developing a communication strategy to effectively communicate with the Australian community:
    - how their information will be collected, used and disclosed;

  - the privacy settings and controls available to them; and
  - how to tell us if they do not want a My Health Record.

- implementing an opt-out service to allow individuals to withdraw from participation of the My Health Record system;
- enhancing the core infrastructure and operations of the system to ensure it can accommodate increased service demand; and
- working with healthcare provider organisations and peak bodies to support increased use of the system once opt-out is implemented.

A number of independent Privacy Impact Assessments (PIAs) have been commissioned to understand and respond to the impacts of moving to an opt-out participation model. A PIA was conducted prior to the 2016 opt-out trials (https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/faq-security-410/$file/PCEHR%20Opt%20Out%20PIA%20-%202015.pdf).

The Agency is using the PIA undertaken by the Department of Health before the trials, but is also conducting a PIA on the national opt out arrangements prior to the national rollout. The Agency will publish the PIA on the My Health Record website.

Conclusion

The Australian Digital Health Agency thanks the Senate Standing Committee on Finance and Public Administration for the opportunity to input into the inquiry into the implications of the Medicare information breach for the roll out of the opt-out My Health Record system'.

An individual's Medicare card number alone does not allow My Health Record information to be accessed. Additional information is required to authenticate consumers and healthcare providers. As we have described above, the security and operation of the system protects against the unauthorised disclosure of health information from the My Health Record for individuals with access to Medicare numbers.

The Australian Digital Health Agency is happy to provide any additional information required to support the inquiry.