Professor Peter Shergold AC, Chair
Independent Review of Health Providers' Access to Medicare Card Numbers
Department of Human Services
18 Canberra Avenue
Forrest ACT 2603

Submission by Australian Privacy Foundation

This submission to the Independent Review of Health Providers' Access to Medicare Card Numbers is made by the Australian Privacy Foundation.

The Inquiry

The Australian Privacy Foundation (the "Foundation") is a non-partisan civil society organisation concerned with privacy. It brings together health specialists, lawyers, academics, information technology experts and non-specialists from across the community. More information about the Foundation and access to submissions over the past thirty tears regarding health privacy is available at privacy.org.au.

The Foundation welcomes the Inquiry. It has both specific concerns regarding unauthorised access/use of Medicare Numbers and broader concerns regarding the development of population-scale e-health systems such as the MyHR program.

This submission builds on comments made by Foundation representative Asst Professor Arnold in meeting with the members of the Inquiry last week. They address and contextualise particular concerns regarding policy review, systems development, health system administration and misplaced calls for a national identity card.

Trust as the foundation of health service delivery

At the outset the Foundation emphasises the fundamental importance of trust as a basis of the delivery of health services to all Australians, including in instances where a recipient may not hold a card or other token of entitlement to services. Respect for that trust through a coherent, principled and effective privacy regime is *not* antithetical to good governance, efficiency and responsiveness to individual needs.

Best practice privacy management does not preclude the collection, storage, processing and dissemination of data that uniquely identifies an individual – for example the Medicare Number – or that has a diagnostic and therapeutic nature. Best practice does however necessitate

- a coherent legal framework,
- effective supervision
- a proactive approach in discerning and then addressing potential harms such as data breaches and
- public engagement.

The Foundation recognises and strongly endorses efforts by health professionals to protect their patient's privacy, as reflected in professional codes rather than merely confidentiality and statutes such as the *Privacy Act 1988* (Cth), the *Health Identifiers Act 2010* (Cth) and the

Health Records and Information Privacy Act 2002 (NSW) and the *Health Records Act 2001* (Vic) .

The Foundation recognises inherent tensions in delivering health services on a timely and whole of population basis. It endorses efforts by the Department of Health and Department of Human Services to work with health professionals in providing those services effectively, for example the telephone channel highlighted in the Inquiry's discussion paper, where the card identifying a service recipient is not immediately available. It notes developments such as a mobile phone (or other networked device) schema – a 'digital card' – for the identification of recipients.

It is not surprising that health practitioners, information technology specialists, lawyers, project management analysts and consumers are concerned about reported data breaches involving Medicare Numbers (the "Numbers"). Those breaches erode trust in the overall handling of health data, i.e. beyond the Number as a discrete identifier. Consistent with a loss of trust in the proper handling and securing of personal information has been the growing concerns among health professionals and the wider community about the system design and implementation of the MyHR program. This has resulted in non-engagement on the part of both professionals and consumers. They are consistent with cautions made in a range of reports and should be addressed on a transparent, strategic basis.

This practitioner and community disquiet is consistent with public wariness about government data handling following the Centrelink and Census project management failures which were exacerbated by the reluctance of the Government to

- acknowledge substantive concerns expressed by a range of stakeholders and
- ensure that the foreseeable problems do not recur, through, for example, investment in system redesign/maintenance, adequate resourcing and enhanced accountability at the operational and ministerial levels.

Contextualising the Medicare Number Breach

The Foundation notes that the Inquiry discussion paper refers to MyHR rather than merely to Medicare Numbers. That reference is commendable, given concerns expressed by health professionals and consumers regarding the design, implementation and accountability framework for the MyHR program.

Those concerns are salient given deferral of the ANAO review of MyHR project management.

They are also salient given the problems – including delays, budget blowouts, confusion, disengagement by health practitioners and disregard of patient privacy – evident in the United Kingdom counterpart of MyHR.

These problems are not new. Concerns were raised in the 2014 ANAO report on Medicare data integrity. The Inquiry is a welcome opportunity for the Department to step back to gain a strategic perspective on Medicare (and MyHR) data handling rather than focusing narrowly on the breach of Medicare Numbers.

No support for an Australia Card

The Foundation is disquieted by suggestions that the Medicare card be replaced by a 'universal' multi-service card along the lines of India's Aadhaar card (used for a wide range of entitlements and private sector purposes) or the 'Australia Card'.

Development of such a card may be attractive to systems vendors but lacks community support. Importantly, it will not be an effective mechanism for substantially reducing identity offences (for example social service entitlement fraud or credit card fraud) in the public and private sectors. It is a fundamentally disproportionate mechanism. As was recognised when the Australia Card was proposed, the development and implementation costs outweigh the benefits to the taxpayer and the broader economy.

The Foundation considers that a shift to a multi-purpose national card will exacerbate community concerns regarding privacy, identity crime and the legitimacy of public sector bodies. That is particularly so if such a card is not embedded within both a coherent legal framework that is underpinned by meaningful accountability mechanisms.

The Foundation considers that the Medicare Number should be regarded as a weak rather than definitive signifier of identity. It supports suggestions that the Number be decoupled from the Card and that there be a statutory prohibition on use of the Card as a proof of identity in public/private sector transactions.

The Foundation cautions against ostensible remedies such as including biometric or other images on the Card, given the fact that:

- identity offenders currently fake driver licences and other photo identity cards in all jurisdictions (sometimes on a substantial scale)
- very few of the people who scrutinise photo identity cards in the public and private sectors have forensic skills sufficient to differentiate between genuine and non-genuine cards.

Policy development and review is imperative

While the Foundation welcomes the Inquiry as sign of the Department's engagement on matters of community concern it is disquieted by the apparent non-involvement of the national Privacy Commissioner and broader Office of the Australian Information Commissioner ("OAIC").

That non-involvement reinforces the incapacity of the OAIC. It is at odds with the objects of the *Privacy* Act 1988 (Cth)[1] and the Information Commissioner's oblications under it, with practice at the state level where Governments have provided public reassurance and agencies have received valuable input through involvement of their Privacy/Information Commissioners.

It is imperative that the OAIC be involved – and be seen to be involved – in inquiries dealing with privacy breaches, particularly where those breaches indicate a need for system redesign. Involvement necessitates properly resourcing the OAIC. It also necessary for the OAIC to adopt a proactive timely approach to breaches and investigations. It is insufficient and poor policy to rely on the Digital Transformation Agency, an entity that has a weak grasp of privacy principles and law.

The Foundation notes that use of the Medicare Card and Medicare Number occur in deteriorating external environment for IT and data security. If it was ever tenable to promise that government could guarantee to keep a 'motivated intruder' out of a digital honeypot, those days are over. The relentless litany of breaches shows the advantage is now firmly with the intruders. This is being made worse by current government efforts to compromise the 'last line of defence' offered by unbreakable encryption, rather than supporting and strengthening this essential foundation of information security.

[1] at Section 2A

In a world where breaches are almost inevitable, IT security expert Bruce Schneier's insight that 'data is a toxic asset' will increasingly lead to acceptance of 'data minimisation' as the necessary foundation of sensitive information security and privacy. The Medicare number needs to be protected and reserved for its special purpose, not exposed to further opportunistic attacks.

In responding to the Medicare Number breach and considering development of MyHR the Department must recognise the growing threat from an aggressive, carefree culture of so-called 'Open Data' (releasing sensitive data sets 'into the wild' with breakable de-identification and no long term protection), a culture that does not want to face up to the future hazards that machine learning and data proliferation pose to the long term effectiveness of even the best de-identification methods.

Responses

The Foundation recommends that problems evident in handling of Medicare numbers can be addressed at several levels.

Privacy Tort

A succession of Commonwealth and state/territory law reform commissions and parliamentary inquiries have recurrently called for establishment of a statutory cause of action regarding serious breaches of privacy (aka the Privacy Tort). That tort is not antithetical to public administration, the implied freedom of political communication (or more broadly a flourishing media sector) and vibrant commerce within/across Australia's national borders.

The tort provides an essential discipline for public and private sector data owners. It is also a mechanism for inducing awareness among those entities of the need to think in terms of curation rather than exclusive ownership, particularly regarding health data (which may be intimate, intergenerational and unlike an identity number not readily changed).

The resistance by Federal Governments of both hues to legislate for a Privacy Tort despite two major inquiries and the High Court's plea in 2001 for Parliament to step in[2] constitutes a significant and egregious failure of public polic.. The policy is especially egregious after India's highest court this month confirmed that a billion Indian citizens now have enforceable constitutional privacy rights, joining nearly a billion in the European and North American zones who can litigate to protect themselves. Australian citizens have no practical and effective way to enforce any legal rights they have to privacy. That should be remedied without delay.

Transparency

The Foundation encourages greater transparency on the part of the Department and private sector bodies regarding confirmed and perceived data breaches. That transparency requires timely disclosure by holders of data that a breach has occurred or is likely to have occurred. That disclosure is not antithetical to law enforcement and is consistent with research regarding overseas practice indicating that consumers value responsiveness rather than a perceived willingness to hide or ignore breaches. Heath service recipients do not need to know the details of how a breach has been detection and how holders are responding. They do however need to know that problems have been identified, that action is being taken and that the holder (such as the Department) has learned from mistakes in order to prevent/minimise future problems of the same type. The Foundation hopes that the current Inquiry is an example of that learning.

[2] *ABC v Lenah Game Meats* 208 CLR 199

The Foundation again joins with the legal, academic, business and information technology communities in expressing concern regarding major loopholes in a delayed, weak data breach notification regime. There is opportunity for regulatory capture and self-interested concealment of the true state of vulnerability and exposure to data breach risks; and for continuation of a culture which remains hostile to transparency, and still implicitly rewards rather than punishes successful concealment, minimisation or denial of risks and actual data breaches. Abuses of Medicare numbers may often remain undisclosed.

Monitoring

On the basis of the reported information, which may of course be inaccurate, the Department was alerted to the Medicare Number breach by a journalist. The Foundation considers that it is imperative that the Department establishes systems that assist detection of anomalies in the processing/sharing of health data – including Medicare Numbers – and that thereby address perceptions that it had to rely on *The Guardian* to identify the breach.

The Foundation recognises difficulties in monitoring given the nature and scale of transactions involving Medicare Numbers by phone and online. However, effective system design should enable monitoring without disproportionate cost or adverse outcomes such as delays in the processing of entitlements to people in remote Australia or who do not have English as a first language.

The Foundation thus commends a move to secure digital systems (including the mobile app noted above) and a strategy that emphasises process reengineering to quickly identify and respond to data breaches.

The Foundation considers that the Department should closely examine the instant breach of the de-identification of clinician identifiers in the 10% Medicare sample, released without appreciation of the danger in 2016. That is a harbinger of things to come. In future, most of the crackers will not be re-identifying out in the open for public interest purposes, but instead doing it secretly and for dubious purposes, almost certainly offshore and safely out of reach of the ineffective and misunderstood regime regarding re-identification. (The effect of the current re-identification law is likely to be to discourage frank research and future disclosure by Australian data scientists, pushing this re-identification problem under the rug).

The Medicare number is a key element in the illicit re-identification market that will spring up to exploit 'Open Data' dumps, and needs maximum protection. (The extensive third party access built in to the design of the MyHR government-controlled electronic medical record will only increase this risk.)

Enforcement

The Foundation recommends that the Inquiry consider the adequacy of penalties regarding

- intentional illicit exposure and use of data
- negligence leading to exposure of data

One rationale for strengthening penalties is to communicate to officials, health professionals and other entities that the data they own or for which they have custody is sensitive (eg substantive health records) or that might be used to build a false identity that affects a health service recipient outside the framework of that service. Put simply, a trivial penalty coupled with a culture in which 'we own the data about you' fosters carelessness.

This is salient in the ongoing development of MyHR.

A public education campaign

Active enforcement, through both prosecution of offences and publicity about that prosecution, is one aspect of a public education campaign. There is general acknowledgement in the information security community that cybersecurity involves a range of stakeholders, including consumers, rather than merely data owners/curators.

Enforcement would, we believe, foster trust by communicating that the Government is vigilant in data protection for all Australians. That is important given incidents such as the Census, Centrelink and DIBP failures that are perceived by many people across the community (and within government) as demonstrating that key public sector bodies are either indifferent or incapable of protecting the privacy of citizens.

A strategic education campaign would foster recognition that patients and health professionals use but do not 'own' Medicare identifiers. On that basis they should expect the formal owner to behave responsibly.

Australian Privacy Foundation
www.privacy.org.au

8 September 2017