Submission

Independent Review of Health Providers' Access to Medicare Card Numbers

3. security risks and controls surrounding the provision of Medicare numbers across the telephone channel, and the online connection between external medical software providers and HPOS

6. any other identified area of potential weakness associated with policy, process, procedures and systems in relation to accessibility of Medicare numbers

First and foremost, the primary security weakness in the Medicare system is that it by design collects too much medical information unnecessarily. Medicare numbers are just the gatekeeper to the richly detailed set of health data that lies behind them. It's the richness of that data that's the real problem, as it's the potential release of that health data that matters to victims when a Medicare number is compromised, not so much the number itself.

When Medicare was first created, it was created in an offline world of paper records stored in filing cabinets. This paper-based system was then gradually adapted to an online world in a sloppy, piecemeal manner with insufficient regard paid to patient privacy and consent rights. The Medicare database in its original incarnation was never designed to make the information it contained as widely available, with as many access points, as is the case today. If it had been, more attention would have been paid to the amount and type of information being collected and whether it was really necessary to collect so much given the risk of a data breach.

It would be perfectly possible to design a system which stores only a minimal amount of medical information, if any, or which allows patients to set the detail of logging (with some possible exceptions for addictive substances). If multiple billing items cost the same amount, does Medicare really need to record which item specifically the patient was billed for, rather than just the amount? Or if a patient sees a specialist, does Medicare really need to record the name and specialty of that specialist in the patient's record? Does Medicare really need to store that much detailed medical information just for billing purposes, and for as long as it does? Do they really need to keep billing data for longer than one to two financial years for auditing purposes?

The biggest security flaw in the Medicare system is how much detailed data is kept needlessly, for longer periods than necessary, and importantly, without patient consent or control. Why was this data available online without patient consent?

1. the type of identifying information that a person should be required to produce to access Medicare treatment in both urgent and non-urgent medical situations

Q2. What identifying information should patients have to produce to access health services?

How does this fit in with anonymous and pseudonymous healthcare? Is that no longer available? I was under the impression, as I'm sure many other Australians are, that we could seek treatment under a false name for anything we consider too sensitive to have recorded under our real name and that we wouldn't be denied treatment (just billed the full amount upfront). Have you considered the effect on the numbers of patients accessing sexual health clinics and phone counselling services if they had to prove their identity in order to access treatment? How would this affect celebrities and domestic violence victims who have

higher than average privacy needs and would prefer to access pseudonymous healthcare by default? There needs to be some understanding of the negative effect that record-keeping has on patient willingness to share information. There are some things you just wouldn't want written down as a patient, but we still don't have the right to control our records like that.

I also think many people might find it a little confronting to be asked for ID, that it will catch them off-guard. Just on the level that it feels a little cattle class, that it doesn't convey the message that we're the ones in control. It might not get a strong community backlash, but it could still add to the general perception that we're slowly, gradually losing our patient rights and slipping back to the days when doctors were in charge.

Why is there any need to show ID in most cases? And would the very small number of fraudulent transactions that may be detected really justify the imposition on the great majority of the Australian public who are lodging honest claims? Is the potential loss of goodwill worth that?

4. the sufficiency of control by patients and the appropriateness of patient notification regarding access to their Medicare number

Q1. Do patients have sufficient control and awareness of access to their Medicare card details?

It doesn't appear that we have any control at all as patients, so no, that's not sufficient. When it comes to putting our data online in particular, that shouldn't be happening without our consent. Health data is too sensitive and the risk of a breach too great, that any claimed benefit could possibly outweigh that negative. Even more than that, it goes against our rightful data ownership rights for doctors to be making that decision for us, against our will. It should be our decision as patients how much, if any, of our medical information gets uploaded to the internet.

This goes to the broader issue of health records not being under patient control. These records are about our bodies, and yet we are not recognised as the rightful owners of them, just as we are over our bodies. It is part of our bodily autonomy rights that we should be able to control the length, breadth and format of any data storage pertaining to those bodies, including whether or not it is available online. This data breach would not have occurred if the data was not online. Why was it online without consent?

Q8. In what circumstances do health professionals require access to Medicare card numbers through the provider enquiries line? Could the provider enquiries line be made available in more limited circumstances?

While better access logging is needed for the telephone enquiries line, it should still be retained as an option for patients who don't want their personal information sent online, and this decision should belong with the patient. Why is confidential patient information being shared online without patient consent?

Q11. How can Government build public awareness of why it is important for individuals to protect their Medicare card information?

I think you have to be careful with this one that it doesn't sound like you're blaming us for Medicare's failure to protect our data. This breach wasn't the fault of any one individual who didn't protect their card enough, it was a system breach. So while this suggestion is harmless enough in itself, if it is seen as being a response to this breach, it could come across as Medicare trying to shift blame off of themselves and onto the victims of the breach.

Q12. Do you have any other comments about the Review Panel's possible responses or any other matters relating to the Terms of Reference?

At the heart of this matter is that patients have been stripped of our decision-making powers on various data access and control issues which should rightfully have been under our control. Our Medicare data should never have been available online in the first place without our consent. Nor should any other of our health information be online without our consent. That doctors are allowed to keep detailed records about our bodies at all, often including photographs and scans, is in itself in conflict with our ownership rights as patients over our bodily data. That we have no avenue of accessing healthcare without being subjected to that record-keeping is emotional blackmail and swings the power balance away from the patient where it should rightfully be.

Please restore our data control rights so that at a minimum we can request that no data be shared online. Where are our patient rights?