Senate Finance and Public Administration References Committee

Circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'

Dr David Glance
Director UWA Centre for Software Practice
The University of Western Australia

I am starting with the following assumptions:

[1] The committee is aware of the circumstances of the sale of Medicare identification information on the Dark Web.
[2] The committee will have been informed about the nature of the access of this information by the person selling these details and so are probably already aware of how this information was accessed. This is not obviously information that is available to me commenting on this breach and its consequences.
[3] Although there are a number of ways in which the vendor could have accessed the Medicare information, it is likely that this involved access to HPOS through stolen PRODA credentials or through a GP or other system capable of accessing Medicare information directly, rather than an actual "hack" of HPOS or the access to the entire Medicare database (see below for more detail of this)

The questions that have been raised about this incident are the following:

[1] How did the vendor get access to the Medicare information
[2] What could someone do with this information if they got it.
[3] Could they use this information to access My Health Record and why would anyone want to access My Health Record in this way and what could they do with this information if they got it?
[4] Are there steps that can be taken to mitigate the risk of illegal access and the downstream consequences of breaches of this information.

Dealing with these in turn

[1] How did the vendor get access to the Medicare information

The small number of sales of Medicare information indicated on the vendor's profile on the Dark Net Market AlphaBay suggests that access to this information would have been for targeted use in identity fraud and/or doctor shopping for scripts.

Due to the nature of the service, the fact that the vendor supplied a specific number on the supply of a full name and date of birth, the access was likely via direct lookup through HPOS using either compromised PRODA credentials and mobile account or through GP practice software or HPOS through remote access.

It is very unlikely that the vendor had access to large numbers of Medicare details, as might be the case if s/he had hacked the Medicare system and got access to the underlying database.

If that had been the case, Medicare details could have been sold in bulk which potentially would have been more useful to criminals wanting to use the information for purposes outlined below.

A significant issue with the Medicare card is that it is used as identification in situations that are unrelated to health care. The actions taken by Medicare in managing the access of this information are only related to its use within the context of healthcare and not necessarily cognisant of the impacts on its other use as form of identification.

The reliance on a Medicare card as a form of identification is not ideal given that Medicare itself is not charged with the explicit responsibility to deal with this secondary function. Given the massive number of people who have access to Medicare details would be like providing similar access to credit card numbers with the date of issue and the verification number as well. This is not the case for credit card information and shouldn't be the case for Medicare cards.

If Medicare cards are used for ID, there should always be some element that only the card holder knows – or there should be some sort of verification (chip, pin, secret number, etc). when it is used for this purpose.

It is worth stressing that even though this particular breach was highlighted by the media, that particular vendor seems to have been shut down for now – presumably after Medicare identified the compromised account that was being used.

[2] What could someone do with this information if they got it.

From a criminal perspective, obtaining Medicare identification information is valuable in the case of identity fraud for setting up or gaining access to a bank account using a stolen identity and for other situations where proof of identity is necessary – getting access to an anonymous cryptocurrency account for example.

The other major driver for obtaining Medicare identification information would also be for obtaining prescriptions to obtain painkillers and possibly S8 medications.

A final use for Medicare information would be to attempt to divert Medicare rebate payments from a legitimate account to a false one under the criminal's control.

Less likely would be getting these details for access to My Health Records or medical records of any kind.

[3] Could they use this information to access My Health Record and why would anyone want to access My Health Record in this way and what could they do with this information if they got it?

In terms of accessing My Health Record, although it is possible to obtain enough information from criminals operating on the Dark Web, it seems unlikely that this would be done for the purpose of gaining access to a My Health Record.

For a start, if the criminal already has significant information about a person, accessing My Health Record really doesn't add that much value.

The mechanism by which the Medicare numbers were being sold on the Dark Web and the cost associated with them would mean that access would need effort and there would have to be some degree of knowledge about what was on the record to make it worthwhile. It is hard to find any motivation to taking this path to gain access to a My Health Record which currently [a] is unlikely to exist and [b] is unlikely to have significant amounts of information in it.

Even when the system becomes opt out, the majority of records are not going to have information in it apart from PBS and MBS data and so will not represent a particularly valuable resource unless it was obtained on a large scale or it belonged to specific individuals where the information was of particular significance. Because of the protection around getting access to myGov, this is a great deal of effort for little potential reward.

[4] Are there steps that can be taken to mitigate the risk of illegal access and the downstream consequences of breaches of this information.

The level of risk presented by breaches of Medicare numbers to My Health Record is relatively low. It is easier to simply obtain access to a record through simple phishing of credentials to myGov and spoof the SMS code verification process.

The general means of initial verification used by Medicare in establishing access are adequate and the access control of myGov, generally at an industry standard in terms of its approach with 2 Factor Authentication through the use of a code sent to a mobile phone.

One step that would add an additional level of protection would be to have notification of access to the account by means of a text message or email set as a default for users (as it is with systems like Facebook that will alert you to new logins from different locations). Currently, it has to be selected as an option in settings by the user.