Some Notes on the implications of Medicare numbers being sold online

A person's Medicare number isn't an inherently sensitive piece of information. The concern is whether that information could be used by a criminal to impersonate the person and hence extract sensitive information or perform other kinds of fraud.

The HPOS system is used by a very large number of providers – it is probably impossible to guarantee that nobody ever misuses their access or leaves security holes in their system.

Attention should focus on minimizing the damage that occurs if someone learns someone else's Medicare number.

This shows that cybersecurity issues have to be thought of in the full context of all the other protocols running at once. Although no immediate harm is caused to a person through exposure of their Medicare number, there may be significant harm from the combination of that breach with other breaches, weaknesses, or design choices.

Note 1: Using a purchased Medicare number, along with address and date of birth, to access a MyHealth Record.

This is a speculative effort to understand whether a Medicare number could be used to access a person's MyHealth record. We have (obviously) not attempted to use these steps to access any medical records. The purpose of this section is to illustrate the sort of steps that a malicious attacker might use, and to raise a specific sequence of possible steps that warrant careful checking by the inquiry.

The attack requires knowledge of the target person's date of birth and address. The idea would be roughly like this:

1. The attacker buys the Medicare card number of someone who doesn't already have either a myGov account or an online Medicare account.
2. The attacker makes up a new myGov account with a plausible name and their own email address (e.g. XXXX123@yahoo.co.uk.) No authentication (other than an email address) is required to create a new MyGov account.
3. The attacker then logs into the newly-created fraudulent MyGov account and attempts to link the target's Medicare billing account with it. If we understand rightly, this requires the Medicare card details and the person's name, address and date of birth. See the screenshot on p.3. It seems that an attacker who bought the Medicare card details from the criminal would have enough information to fill this in.

   This is where it might not succeed – we don't know whether this screen then leads on to a screen that asks for more information that the attacker wouldn't have. We didn't try, obviously.

   This would require guessing the person's individual reference number on the Medicare card (we don't recall that being part of the data offered for sale), but that wouldn't be hard in most cases – most people who live alone are number 1; most eldest children who live with both parents are number 3. If the first guess was wrong, the attacker could try again.

4. If it does succeed, it seems that that would then furnish the information required to complete the MyHealth record registration, *i.e.* the "Information about your last doctor's visit for which a Medicare claim was made" described at https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/before_you_register

   This too may be mistaken, and the attack may fail at this point if the acquired information is not enough. The site also requires the BSB and account number for automated Medicare payments, if they have been set up. So the attacker might need to target people who have not set up automatic payments, or find the target's BSB and account number.

Note 2: Increasing confidence in re-identifications in the MBS-PBS 10% sample.

The MBS-PBS 10% sample was determined by taking all people with the same last digit of their Medicare number. The actual number chosen was not made public (indeed, we are not entirely sure that this method of selection was public). If an attacker managed to re-identify some patients in the published MBS-PBS open dataset, there would probably be some uncertainty about whether those re-identifications were accurate. Mistaken re-identifications could occur if there was a coincidental resemblance and the target person was not in the 10% sample. However, if the attacker could also purchase Medicare card numbers for all the re-identified people, it would be fairly easy to infer what the selection digit was and hence be very confident that an individual who could be uniquely identified in the sample was a correct re-identification.

Note 3: Medicare card number as proof of identity

Given that the Medicare card is worth 25 points in the 100 point identity check,[1] the widescale availability to look up Medicare card numbers via HPOS raises concerns. When combined with other breaches, for example, the recent breach of passport details by Flight Centre,[2] the ability to buy targeted card numbers could enable identity theft. Many other 25-point options are not very secure either.

Conclusion:

The underlying issue of widespread access to a system that allows the lookup of an identity document is difficult to address. The vulnerability is in the widespread access, yet the widespread access is at the heart of the HPOS system. It may not be possible to secure access without undermining the very service the HPOS system is intended to provide.

We recommend not using Medicare number as partial proof of identity. The way to address the real problem is to work towards better alternatives for secure online authentication.

[1] https://www.border.gov.au/Licensing/Documents/100-points-identification-guidelines.pdf
[2] http://www.abc.net.au/news/2017-07-13/personal-information-leaked-third-party-suppliers-flight-centre/8706422

Your details - myGov - Mozilla Firefox (Private Browsing)

details - myGov

ail Files - ownCloud Calendar - ownCloud NetBank - Log on to Ne...

Your member service reference number

Medicare Card Number (no spaces) Help

Require a value

Your Individual Reference Number on your Medicare Card Help

Require a value

Your personal details

Given name (first only) Help

Require a value

Family/Surname Help

Require a value

Date of birth (dd/mm/yyyy) Help

DD MM YYYY

Your address

Unit/Flat number Help

Street number Help

Street name Help

Suburb/Town Help

Postcode Help

State Help

Select an Option

Country Help

Australia

Cancel Next