Australian Privacy Foundation

https://www.privacy.org.au

Secretary@privacy.org.au

1 April 2021

APF media briefing:
Federal Government quietly reward GPs for patient health data without getting informed consent

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation.

Background

The Federal Department of Health has a dubious record when it comes to developing and implementing information systems that acquire and manage the sensitive health data of Australians. After over ten years effort the controversial and largely unused My Health Record system (MHR) is still doing very little other than gathering existing government data and a few random test results, with random extracts of some past clinical records in some files. The Commonwealth government has never shown that the promises it made when it created the system, that it would enable patients to take charge of their own healthcare and that it would save the Federal budget billions of dollars, have been delivered.

It had abandoned the “informed consent” model for creating such a federal government controlled record, which was originally called the ‘Personally Controlled Electronic Health Record’, because few Australians were willing to give consent in trials.

The recent debacle with the launch of the Covid Vaccines booking system has probably further undermined trust in the Department's ability to develop large scale IT systems that actually work as intended.

Meanwhile the Department has been quietly working away to extract patient data from GPs’ clinical management systems, supposedly so that the Department can ‘improve the quality of healthcare delivery’. Patients are not aware that this is going on, they have not been informed about its nature and possible benefits and risks, and, as with the MHR, they have not been asked for their consent.

This may be because health authorities fear that given a choice, patients may refuse, so as to protect traditional doctor-patient confidentiality on which medical treatment, the therapeutic relationship and many public health implementations, are based.

What the Department will actually do with the data they quietly scrape up from the clinical management systems is also unclear – this is the advantage of not having to tell anyone about it, and not having to credibly respond to obvious concerns in order to obtain consent.

There are a number of 'data-sharing' and 'linking' projects across multiple government agencies which are generally based on non-consensual disclosure of data drawn from sensitive personal information to a third party. As far as we know, this data may be included in these projects.

The data collection processes

Two key data collection processes currently occur with patient health data stored by general practices based on the ostensible de-identification of related data streams.

1. The first collection process concerns the use of patient information drawn from a federated system of General Practice data bases to Primary Health Networks (PHNs), designated by the Federal Government as '**regional data custodians'**, around the country.
2. The second process awards eligible Australian General Practices up to $50 k annually each, as a key element of the *Practice Incentive Payments – Quality Improvement* (PIP-QI) program. The PIP-QI program extracts data from the PHNs and ports this to the Australian Institute of Health and Welfare (AIHW), designated by the Federal Government as **the 'national data custodian'**, to aggregate, control, use, access, secure and control individual patient's privacy of the 'PIP Eligible Data Set'. Theoretically at least, it commenced in August 2020.[1.]

Finally, the ostensible de-identification of patient information, where these individuals have supposedly provided consent for the data collection, is claimed to ensure both processes are legally justified 'secondary uses' of health information.

Data "de-identification" for secondary use of health data.

Patient data extracted from general practices, designated by the Federal Government as **local data custodians**, is claimed to be de-identified if obvious **direct identifiers**, such as a person's name, address, email contacts, telephone number and date of birth, are removed before use. Once direct identifiers are detached, organisations using and controlling the collected information are required to

eliminate or alter any other information that can identify a patient, in addition to controlling and safeguarding the data adopted, held, used, disclosed, refreshed or controlled in the data access environment to avoid reidentification.[2-3]

Ostensibly de-identified information capture processes are implemented by commercial data extraction software applications retrofitted to the eHealth clinical practice management system used by each general practice, and the data collated by the PHNs for communication to PIP-QI authorities. Anecdotal evidence suggests the scale of the data extraction process is immense, with more than 25 million records collected Australia-wide by this type of data extraction software. Yet most Australians are completely unaware of the data collection occurring, or that they may be able to have a say in whether this occurs to their sensitive medical data.

Ostensibly de-identified personal information is often in reality not permanently and reliably de-identified. From the moment of extraction it may be at risk of partial or complete re-identification, and this risk is likely to increase over time. Up to 400 data points are collected for each patient by the information capture applications linked to general practice eHealth systems, providing a rich and comprehensive baseline for automated or AI-based re-identification or reversible pseudonymisation efforts, so genuine de-identification of the collected records is simply not possible.[4-5] These substantial data points include medications such as opioids, antidepressants; alcohol consumption; smoking; and diagnoses such as cancer, chlamydia and anxiety. Prescribing dates are included in the data points, as are pathology results, and all the recorded information that patients confidentially shared with their General Practitioners to receive health care. There is a rich literature explaining how easy it can be to re-identify such rich data sets; one of those contributing to this literature after demonstrating a trivial effort was enough to re-identify doctors from a supposedly de-identified 'Open Data' dump from a sample of the Medicare database believes "detailed individual records cannot be securely de-identified while retaining their information, and should not be shared without the person's [informed] consent".[6.]

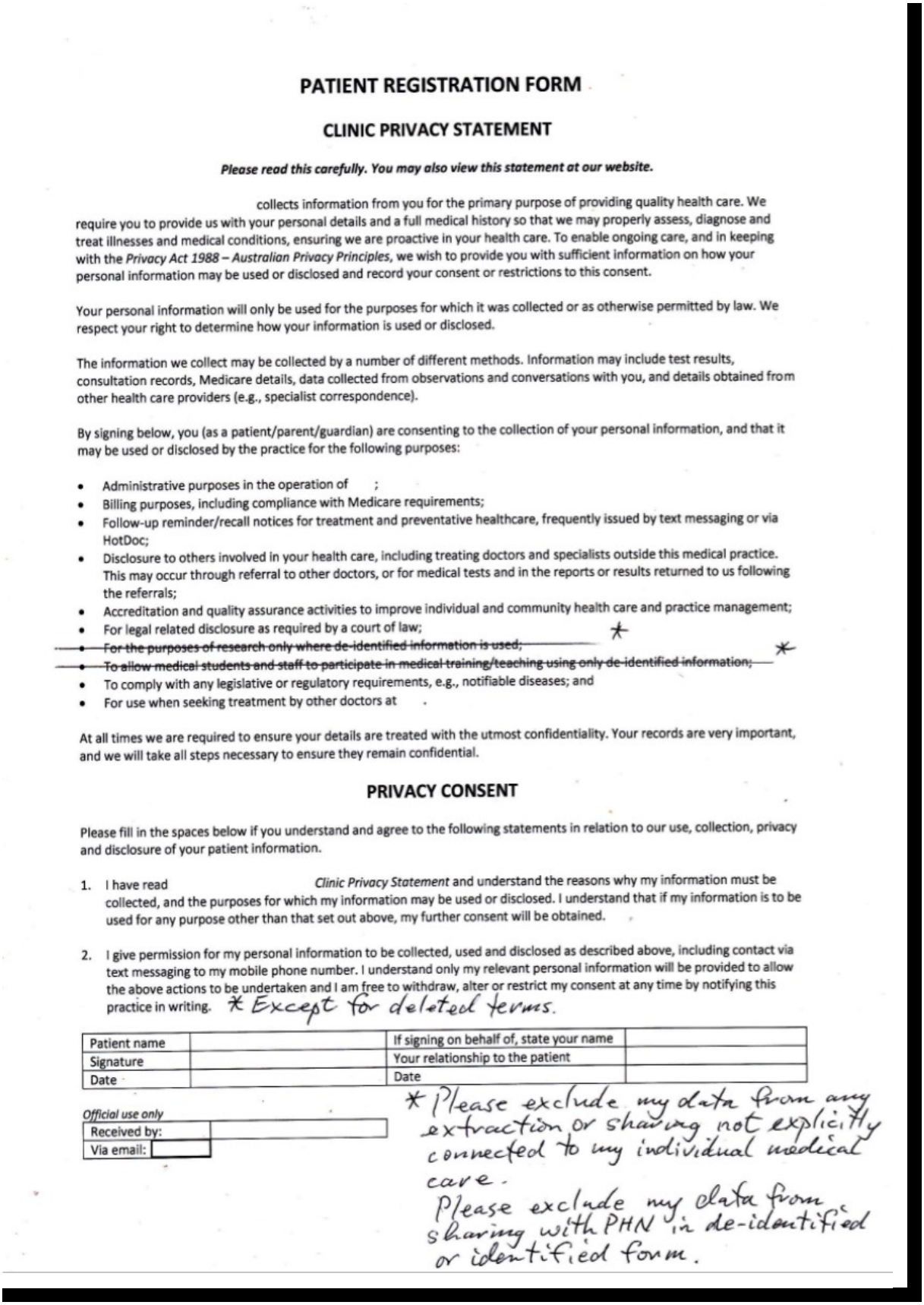
A suitably resourced and motivated entity can readily identify many forms of ostensibly de-identified records.[7-9] Consequently, Australian Privacy Principles (APPs) indicate that individual patient consent is a key foundation of the data collection processes used by general practices.[10-11] The APPs underpin advice offered by the Office of the Australian Information Commissioner (OAIC), the *OAIC/Data 61 guidelines*, which are published on the Internet.[11] The Australian Medical Association (AMA) and the Royal Australian College of General Practitioners (RACGP) formally support the de-identification advice.[3, 12-13] Associate Professor Teague from the University of Melbourne, renowned

cyber security expert, maintains the advice offered in the OAIC/Data 61 guidelines are poorly specified and generally reliant on techniques that are known to fail and keep on changing.[6] There is no evidence that the level of local engagement with ongoing international critiques of the effectiveness of existing de-identification methods and protocols, and the wide professional education necessary for clinical records custodians, clinicians, patients and professional disciplinary or research ethics bodies to understand and act on these risks, is occuring in Australia. In addition, evidence suggests general practice do not even comply with these limited and probably ineffective guidelines.[14] Instead, as shown in Figures 1 and 2, general practices obtain consent for the data collection project by posting a generic, 'bundled consent' privacy statement on waiting room walls, on request, Internet sites and then in effect rely on using implied consent. The latter means that individuals are claimed to consent merely by continuing to use a service. Not only are they not asked for explicit consent to allow the disclosure of their sensitive medical record data in weakly or ineffectively de-identified form to unspecified third parties, the level of concrete information on these ambiguous and cryptic generic privacy statements is almost univerally inadequate to draw a patient's attention to this practice, or to fairly explain how it works, how it may fail, and the risks and implications of consenting to this aspect, which is outside the normal realm of clinical records and practice management.

Withdrawal of consent

Importantly then, consent underpinning the data linking implementation is typically not an "informed consent process" as required by the APPs and the current OAIC/Data 61 guidelines. As Figure 1 illustrates, individual patients may try to deny consent for the data collection process once they become aware that it actually occurs. It is the consumer-hostile nature of 'bundled consent' to try to link one's consent for a wide range of non-essential, often incompletely-specified provisions to the offer of any services. The intention is for the data subject, if they bother to read it all, to think they have to agree to everything or be refused service; but contracts can be revised by either party, and consent can be conditional or partial.

While this may be a challenging process for anyone to confront, it can be particularly difficult individuals from CALD communities, despite the availability of translated documents in some instances. Individuals from CALD communities will be interacting with practice employees who may not speak the same language, and who themselves may not understand either the process of extraction and disclosure to multiple other (often un-named) third parties, or the nature and risks of particular de-identification methods when data is used by other entities with access to advanced analytics and other



PATIENT REGISTRATION FORM

CLINIC PRIVACY STATEMENT

Please read this carefully. You may also view this statement at our website.

collects information from you for the primary purpose of providing quality health care. We require you to provide us with your personal details and a full medical history so that we may properly assess, diagnose and treat illnesses and medical conditions, ensuring we are proactive in your health care. To enable ongoing care, and in keeping with the *Privacy Act 1988 – Australian Privacy Principles*, we wish to provide you with sufficient information on how your personal information may be used or disclosed and record your consent or restrictions to this consent.

Your personal information will only be used for the purposes for which it was collected or as otherwise permitted by law. We respect your right to determine how your information is used or disclosed.

The information we collect may be collected by a number of different methods. Information may include test results, consultation records, Medicare details, data collected from observations and conversations with you, and details obtained from other health care providers (e.g., specialist correspondence).

By signing below, you (as a patient/parent/guardian) are consenting to the collection of your personal information, and that it may be used or disclosed by the practice for the following purposes:

- Administrative purposes in the operation of ;
- Billing purposes, including compliance with Medicare requirements;
- Follow-up reminder/recall notices for treatment and preventative healthcare, frequently issued by text messaging or via HotDoc;
- Disclosure to others involved in your health care, including treating doctors and specialists outside this medical practice. This may occur through referral to other doctors, or for medical tests and in the reports or results returned to us following the referrals;
- Accreditation and quality assurance activities to improve individual and community health care and practice management;
- For legal related disclosure as required by a court of law; *
- ~~For the purposes of research only where de-identified information is used;~~ *
- ~~To allow medical students and staff to participate in medical training/teaching using only de-identified information;~~
- To comply with any legislative or regulatory requirements, e.g., notifiable diseases; and
- For use when seeking treatment by other doctors at .

At all times we are required to ensure your details are treated with the utmost confidentiality. Your records are very important, and we will take all steps necessary to ensure they remain confidential.

PRIVACY CONSENT

Please fill in the spaces below if you understand and agree to the following statements in relation to our use, collection, privacy and disclosure of your patient information.

1. I have read *Clinic Privacy Statement* and understand the reasons why my information must be collected, and the purposes for which my information may be used or disclosed. I understand that if my information is to be used for any purpose other than that set out above, my further consent will be obtained.

2. I give permission for my personal information to be collected, used and disclosed as described above, including contact via text messaging to my mobile phone number. I understand only my relevant personal information will be provided to allow the above actions to be undertaken and I am free to withdraw, alter or restrict my consent at any time by notifying this practice in writing. * Except for deleted terms.

Patient name		If signing on behalf of, state your name	
Signature		Your relationship to the patient	
Date		Date	

Official use only

Received by:	
Via email:	

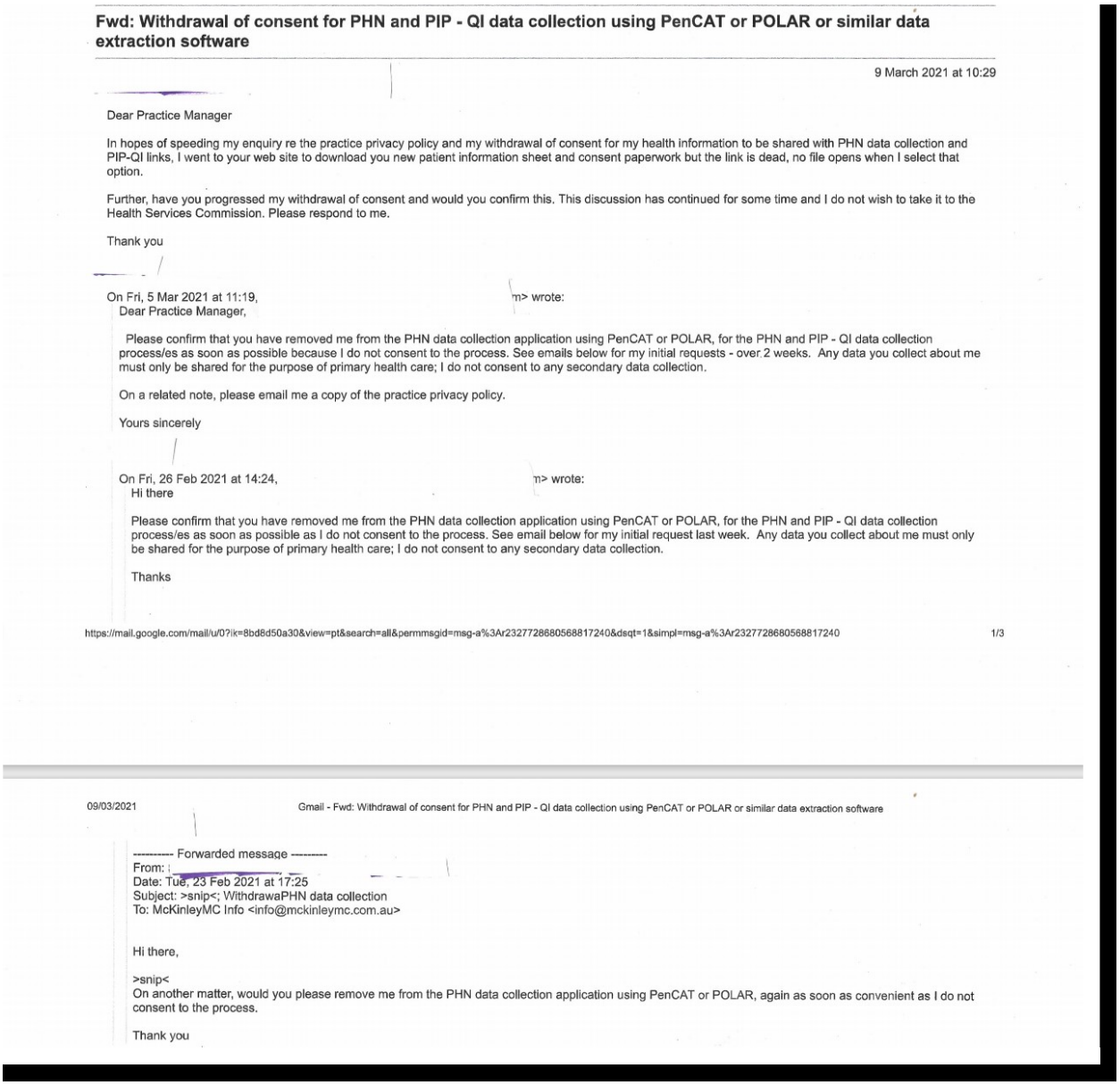
* Please exclude my data from any extraction or sharing not explicitly connected to my individual medical care.
Please exclude my data from sharing with PHN in de-identified or identified form.

Figure 1: Case 1. New patient withdrawal of consent for secondary health data collection

big data tools. It is vital that all patients, but particularly those from CALD backgrounds, are formally offered access to others who can explain the data manipulation, disclosure and consent process, and are supported to withdraw from this aspect of general practice data collection should they so decide.

Despite a legal right to refuse, withdraw or limit consent, it can prove extremely challenging even for those culturally Australian 'born and raised', as Figure 2 shows. The saga illustrated there continues, despite the APPs; it is expected to conclude with a legalistic State government complaints process upholding the effectiveness of the inadquate bundled consent and over-ruling the individual's refusal to agree to some elements, on the basis that it would be too complicated for everyone else to recognise and respect those limitations. At minimum individuals choose to withhold information from their MHR .[15] But the evidence suggests no body or person seems to have effective oversight over the data collection, sharing and informed consent processes used by local health data custodians, and general practice organisations. (This is one of the signal failiings of the billions spent over the last decade and a half on electronic health records and the MyHR: the "personally controlled" aspect, its key selling point enshrined in the title of original law, was quickly slipped into the too-hard basket and abandoned -- so the most important question remains unresolved, and systems around EHRs in Australia do not support a simple, interoperable, transparent method of describing patient choices or recording and auditing compliance with these choices.

To secure public trust and confidence, these exceptional and intrusive actions taken under the justification of collecting patient health data for secondary use by third parties need to be accompanied with measures at the local general practice level so that individuals can become informed about the process, about all the entities who may get access to data derived from their record, and about the limits and risks of current methods to ostensibly de-identify unit medical record data; and can then exercise informed consent about participating in these nation-wide data disclosure processes . Transparency and explicit notification measures, and an emphasis on responding to increased information security threats in an environment of constantly escalating methods for bypassing traditional data protection techniques is, in the context of the community trust required to progress pervasive health implementations across Australia, vital.



Fwd: Withdrawal of consent for PHN and PIP - QI data collection using PenCAT or POLAR or similar data extraction software

9 March 2021 at 10:29

Dear Practice Manager

In hopes of speeding my enquiry re the practice privacy policy and my withdrawal of consent for my health information to be shared with PHN data collection and PIP-QI links, I went to your web site to download you new patient information sheet and consent paperwork but the link is dead, no file opens when I select that option.

Further, have you progressed my withdrawal of consent and would you confirm this. This discussion has continued for some time and I do not wish to take it to the Health Services Commission. Please respond to me.

Thank you

On Fri, 5 Mar 2021 at 11:19, m> wrote:

Dear Practice Manager,

Please confirm that you have removed me from the PHN data collection application using PenCAT or POLAR, for the PHN and PIP - QI data collection process/es as soon as possible because I do not consent to the process. See emails below for my initial requests - over 2 weeks. Any data you collect about me must only be shared for the purpose of primary health care; I do not consent to any secondary data collection.

On a related note, please email me a copy of the practice privacy policy.

Yours sincerely

On Fri, 26 Feb 2021 at 14:24, m> wrote:

Hi there

Please confirm that you have removed me from the PHN data collection application using PenCAT or POLAR, for the PHN and PIP - QI data collection process/es as soon as possible as I do not consent to the process. See email below for my initial request last week. Any data you collect about me must only be shared for the purpose of primary health care; I do not consent to any secondary data collection.

Thanks

https://mail.google.com/mail/u/0?ik=8bd8d50a30&view=pt&search=all&permmsgid=msg-a%3Ar2327728680568817240&dsqt=1&simpl=msg-a%3Ar2327728680568817240 1/3

09/03/2021 Gmail - Fwd: Withdrawal of consent for PHN and PIP - QI data collection using PenCAT or POLAR or similar data extraction software

---------- Forwarded message ---------

From:

Date: Tue, 23 Feb 2021 at 17:25

Subject: >snip<; WithdrawaPHN data collection

To: McKinleyMC Info <info@mckinleymc.com.au>

Hi there,

>snip<

On another matter, would you please remove me from the PHN data collection application using PenCAT or POLAR, again as soon as convenient as I do not consent to the process.

Thank you

Figure 2: Case 2 Challenges for existing patient trying to withdraw consent for secondary health data collection

ACKNOWLEDGEMENTS

1. Honorary Associate Professor Virginia Teague, Computing & Information Systems, University of Melbourne. https://findanexpert.unimelb.edu.au/profile/34563-vanessa-teague

2. I acknowledge and thank the members of the APF Health Committee for their guidance herein.

REFERENCES

1. Central and Eastern Sydney PHN. Frequently Asked Questions: PIP QI and Data Sharing. November 2019. https://www.cesphn.com.au/
2. OAIC. De-identification and the Privacy Act, 21 March 2018. https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/
3. De-identification Decision-Making Framework, OAIC /Data 61 framework. 18 September 2017. https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decsion-making-framework/
4. de Montjoye, Y.A., Hidalgo, C.A., Verleysen, M.& Blondel, V. D. Unique in the Crowd: The privacy bounds of human mobility. Nature, 3: 1376. 25 March 2013. DOI:10.1038/srep01376 Available from: https://www.nature.com/articles/srep01376.pdf
5. PENCat. Cat4 De-Identified Extract Data Entry. 8 October 2019. Available from https://www.pencs.com.au/wp-content/uploads/2019/12/PenCS-CAT4-Deidentified-Data-Dictionary.pdf
6. Teague, V. Closed social media conversation with author, Topic- PIP-QI & PHN data de-identification process. 20 January 2021)
7. Teague, V., Culnane, C., & Rubinstein, B. The simple process of re-identifying patients in public health records, Pursuit. University of Melbourne, 18 December, 2017. Available from https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records
8. Culnane, C., & Rubinstein, B. & Teague, Submission 5 to the Senate Inquiry into circumstances in which Australians' personal Medicare Information has been compromised and made available for sale illegally on the dark web. Available from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/medicareinformation/Submissions)
9. Salas, J. & Domingo-Ferrer, J. Some basics on privacy techniques, anonymization and their Big Data challenges. Mathematics in Computer Science. 2018, 12:263-274. https://doi.org/10.1007/s11786-018-0344-6
10. OAIC. New Guides Paves the Way for better data privacy management. Office of the Australian Information Commissioner.. 17 September, 2017. https://www.oaic.gov.au/updates/news-and-media/new-guide-paves-way-for-better-data-privacy-management/

11. CSIRO. A framework for data de-identification, CSIRO Data 61- https://data61.csiro.au/en/Our-Research/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework
12. Australian Medical Association (AMA). Practice Incentive Payment Quality Improvement begins, media release. August 1 2019. Available from https://ama.com.au/gp-network-news/practice-incentive-payment-quality-improvement-begins/
13. Royal Australian College of General Practitioners (RACGP). Practice Incentives Program Quality Improvement Incentive (PIP QI) fact sheet. 2020. Available from https://www.racgp.org.au/running-a-practice/security/managing-practice-information/secondary-use-of-general-practice-data/pip-qi-factsheet
14. Kruys, E. Lets not fool ourselves about the PIP – QI, Doctor's Bag. 19 August 2019 https://doctorsbag.net/?blogsub=subscribed#blog_subscription-3
15. Barnett, C. Opinion: Is the new PIP QI a back door to your personal health data? Pulse IT. 5 August 2019. https://www.pulseitmagazine.com.au/news/australian-ehealth/5055-opinion-is-the-new-pip-qi-a-back-door-to-your-personal-health-data.