Submission to the Review of Pharmacy Remuneration and Regulation

Dr Chris Culnane, Dr Ben Rubinstein, Dr Vanessa Teague

Our submission focusses solely on the areas around electronic health records and the associated security and privacy risks.

The benefits of deploying electronic health records and prescriptions are clear, both in terms of reduced risk of error and improved information at the point of care. However, any digitisation of records presents increased security and privacy risks. Such risks are inherent in even well designed and secure systems, since they originate not from implementation, but from the inherent centralisation and scale associated with such systems. For example, the impact from a rogue employee is proportional to the amount of data they have access to–in a paper-based system there is an implicit limit to the amount and scope of the data that they can access and easily copy. Conversely, a digitised system of records will provide much broader access to data, about a much larger number of people. This cannot be avoided, since it is this broader access to more information that delivers the very benefits being pursued. To prevent such access, or to make such access cumbersome, negates the very reason for pursuing electronic records.

The presence of such risks does not preclude the use of electronic records, it does however impact on the design, deployment and oversight of such systems. Patient privacy and data security must be protected from misuse with a combination of technical protections and appropriate legislation & regulation. Current privacy legislation in Australia lags behind parts of the rest of the world, in particular the European Union, which is following a path of ever-stronger privacy legislation. Such legislation recognises the importance of the social license to centralise information management and care. The development of such legislation must precede the broadening of access to data, otherwise both the data and public trust in the system could be lost.

This submission does not attempt to describe a complete solution to the design problem. We simply list three important factors that need to be considered in any solution considered feasible.

Individuals may misuse legitimate access

The recent discovery of online sales of Medicare numbers focused attention on possible misuse of the HPOS system. Whether the criminal who sold the numbers was an individual with legitimate access, or whether they had compromised the system of a person with legitimate access, this sort of leak is probably inevitable in any large system. The best way to minimise impact of future breaches is to control access carefully: medical professionals should have access only to the record attributes they need in order to treat their patients. Community pharmacists very rarely need to read a patient's information in an emergency without their consent, so permissions should be restricted unless explicitly granted by the patient. Logs of who accesses which records should be kept to enable periodic auditing, and independent oversight.

"De-identified" data may be easily re-identifiable

The protection of patient data currently held by pharmacies, in particular large pharmacy chains, is inadequate. This is not just a problem that will be faced if option 2-8 is pursued–the problem exists today. Vast datasets of individual prescribing histories are being constructed and held by

pharmacy networks. One analytics company "*captures every script from over 3000 pharmacies.*"[1]. Such information is claimed to be de-identified, and not re-identifiable[2]. Unfortunately many, if not all, de-identification methods have consistently been shown to be ineffective in protecting against re-identification[3] of complex unit-record level data.

A subset of the data was used for the 2017 Melbourne Datathon. We did not partake in the datathon, since entry required the signing of a restrictive non-disclosure agreement, which contained a number of liability clauses. However, information about the data could be gleaned from various public sources. It appears that it consists of detailed transactional information, including drug codes, prescriber IDs, store IDs, store postcodes, and repeating prescription data. Additionally, it appears that gender, year of birth and postcode of the patient is included. This is more detailed than anything that was released as part of the government MBS/PBS 10% longitudinal open-data release, which could be re-identified. Without seeing the data, it is not possible to determine what, if any, perturbation has been applied to those fields.

It is our conjecture that such data would be readily re-identifiable.

It should be fairly obvious that an individual's prescribing history alone is highly identifiable, even if the name and other identifying fields have been removed or perturbed. Removal of explicit personally-identifying attributes rarely prevents identification of some individuals. There is a significant risk that these vast datasets are being made available for commercial exploitation, with little oversight of the privacy impact on patients.

Data integrity matters too

The Interim Report describes risks to patient health associated with errors in the prescribing and dispensing of medications. Automating the process could certainly reduce the rate of errors. However, it is critical to defend the system against deliberate manipulation of prescriptions–a malicious party who deliberately introduced a change into a prescription could do the recipient great harm. Similarly, criminals who tried to access medications for the illicit drug trade could benefit from deliberate manipulation of prescription data. A well-designed and secure system could be better at detecting them than the present system, but a weak or poorly-structured one would be more vulnerable.

Conclusion

Failure to adequately protect patient data risks jeopardising public trust in the pharmacy network. This could result in patients failing to engage with the health network for sensitive medical conditions, which would have a detrimental impact on the health of society as a whole.

Our concerns with electronic health records and prescriptions are not with the concept in itself, rather the track record of the existing providers and the apparent lack of necessary safeguards to protect existing data. Prior to expanding access to patient data it is essential that current deficiencies in privacy protection are addressed. Appropriate privacy protections will serve as an

1 https://www.pharmacynews.com.au/news/latest-news/dispensing-deficit
2 https://www.nostradata.com.au/Public/Home/Privacy
3 Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: https://ssrn.com/abstract=1450006

enabler for the safe deployment of electronic health records. Failure to protect privacy will expose patients to an unacceptable risk of exploitation, irrespective of whether electronic health records are pursued.

The great benefits of electronic pharmaceutical and health records can only be realised given successful protection of privacy and data security. This requires a combination of good engineering for cybersecurity and good legislation for privacy.