Protected Disclosure of Security Vulnerabilities in the PCEHR

A submission in response to
Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper

June 23, 2015

Summary

Following the *Review of the Personally Controlled Electronic Health Record*[1], the Department of Health has solicited public comment[2] in response to proposed legislative changes. This submission regards the potential inclusion of provisions aimed at facilitating the disclosure of security vulnerabilities without fear of prosecution under the new legislation.

Disclaimer

The opinions expressed herein are those of the author, and do not necessarily reflect the views of any institution with which they are affiliated.

Introduction

Existing legislation regarding the Personally Controlled Electronic Health Record (PCEHR[1]) includes provisions for civil penalty of up to 120 units with regards to the "unauthorised collection, use and disclosure of health information included in a consumer's PCEHR"[3] (Section 59), or up to 120 units *and* 2 years imprisonment for "unauthorised use and disclosure of healthcare identifiers"[4] (Section 26). Although exemptions to such penalties are included in Part 4, Division 2 of the PCEHR Act, there are no explicit protections for the disclosure of security vulnerabilities pertaining to (i) the PCEHR system, nor (ii) associated architecture such as health-software integrations.

[1] In keeping with the Discussion Paper, the existing nomenclature will be utilised instead of the proposed *My Health Record*.

A security vulnerability is a "flaw within a software system that can cause it to work contrary to its documented design and could be exploited to cause the system to violate its documented security policy"[5]. Responsible disclosure (RD) is a framework within which those who discover such a vulnerability can report it such that it may be corrected. This notion is based in a context of social responsibility whereby *finders*[2] make an active decision to protect the privacy rights of stakeholders rather than (i) leaving the system vulnerable for fear of litigation brought on by *vendor*[3] response, or (ii) maliciously benefiting from their discovery.

RD[4] has been embraced by many major software vendors including, amongst others, Google[6], Microsoft[7], Facebook[8], and Symantec[9]. The *Organization for Internet Safety* (OIS) has published guidelines[5] for such disclosure, and the reward of financial 'bounties' is commonplace[5].

The PCEHR Review stated that "privacy and security of records remain a priority for all users", and recommended the establishment of a *Privacy and Security Committee* (Committee). One proposed role of the Committee is to "facilitate protected reporting of privacy & security issues by users of eHealth systems". Subsection 64(2) of the PCEHR Act exempts penalty under Section 59 in order to "lessen or prevent a serious threat to public health or public safety", and it is under the proposed purview of the Committee that I wish to recommend the consideration of similar exemptions for RD.

Details

The discovery of a security vulnerability by a socially-minded individual does not preclude similar discovery by a nefarious party. The disclosure of such vulnerabilities may be considered as analogous to secondary prevention in healthcare. Disclosure (akin to the detection of early disease signs) allows for active protection against a data breach—or, more plainly, prevention is better than cure.

A move away from litigiously-minded responses to vulnerability discovery creates an environment in keeping with the recommendations of the PCEHR Review. The Review's recommendation for the adoption of an opt-out model is premised on evidence that it is well received "provided

[2]Security researchers, individual PCEHR users, etc.

[3]Software developers, the Government, individual stakeholders, etc.

[4]The specific term *responsible disclosure* has, in some cases, been abandoned due to historical connotations. Microsoft in particular refers to Coordinated Vulnerability Disclosure. I have, however, avoided the abbreviation VD lest I be accused of suggesting that we embrace venereal disease.

[5]See Google's *Vulnerability Reward Program*[6] which offers, at the time of writing, up to US$20,000.

safety and security issues are addressed". In light of their statement that "the Privacy and Security committee will... transparently report to the Minister", I believe that it is reasonable to extend such an approach across the full gamut of privacy and security.

That is not to say that specifics regarding vulnerabilities should be made publicly available—an approach known as *full disclosure*. RD allows for time during which the vendor can investigate, correct, and resolve vulnerabilities. Given the history of delays in *scheduled* development of PCEHR elements, it is my belief that the full disclosure model is not appropriate. The Committee should produce a publicly-accessible *disclosure policy* which allows—in consultation with an independent expert—for agreement upon a reasonable time frame for full resolution of vulnerabilities after which the finder can, without penalty, release details publicly.

Given the sensitive nature of PCEHR data, it is reasonable to believe that alternate courses of action exist. A malicious finder may, despite threat of prosecution, utilise said vulnerability to extort at-risk individuals. RD aims to realign incentives. Professional security researchers may consider public recognition as sufficient incentive, whilst other individuals might only respond to more tangible rewards. The time limit for resolution of vulnerabilities prior to full disclosure acts as an incentive on the part of the software vendor.

The discovery of a security vulnerability must, in certain circumstances, by its very definition, result in the "unauthorised... disclosure of health information included in a consumer's PCEHR"[3] to the finder. I am by no means suggesting that unfettered access to such data be allowed under the guise of security research, but rather that it not be subject to prosecution in the event that it is limited to that which is reasonably necessary. Furthermore any research or accidental discovery involving active disruption of services and data should be held to more stringent controls.

In the event of the discovery of a vulnerability that may lead to (i) tampering with data, (ii) reduced availability of data, or (iii) any other scenario that may endanger the health or safety of exposed patients, the vulnerability should not be explored further by the finder. A vendor, however, should not be allowed to offhandedly deny the existence of such a vulnerability, and processes should be in place to allow for controlled testing thereof or, failing this, full public disclosure. The availability of vendor-specific disclosure policies could be mandated under the auspices of the Committee.

Conclusion

The value of a national eHealth record relies on sufficient uptake by relevant parties, but it has been found that "practitioners and practices are fearful of becoming involved because of the significant fines and penalties for privacy breaches"[1]. A framework that allows for active mitigation of such breaches will buoy participation rates through improved stakeholder confidence. The adoption of a security-minded environment is clearly a priority of the proposed Australian Commission for Electronic Health, and the inclusion of legislative provisions allowing for protection of vulnerability finders, under a transparent disclosure policy, is a prudent measure for achieving such an outcome.

Further Reading

A full treatment of the benefits, implications, and caveats of vulnerability disclosure is beyond the scope of this document. Such exploration should fall under the auspices of the Committee following its establishment. Interested readers are, however, directed to the OIS guidelines[5] along with existing policies[6, 7, 8, 9].

References

[1] Australian Government Department of Health. *Review of the Personally Controlled Electronic Health Record*. 2013. URL: http://www.health.gov.au/internet/main/publishing.nsf/Content/46FEA5D1ED0660F2CA257CE40017FF7B/$File/FINAL-Review-of-PCEHR-December-2013.pdf (Accessed 2015-05-31).

[2] Australian Government Department of Health. *Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper*. 2015. URL: https://consultations.health.gov.au/ehealth/ehr-and-hi-legislation-discussion-paper-1/supporting_documents/PCEHR%20and%20HI%20Legislation%20Discussion%20Paper%202015%20D15537948.DOCX (Accessed 2015-05-31).

[3] *Personally Controlled Electronic Health Records Act (Commonwealth)*. 2012.

[4] *Healthcare Identifiers Act (Commonwealth)*. 2010.

[5] Organization for Internet Safety. *Guidelines for Security Vulnerability Reporting and Response (Version 2.0)*. 2004. URL: https://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf (Accessed 2015-05-31).

[6] Google. *Google Vulnerability Reward Program (VRP) Rules*. URL: https://www.google.com/about/appsecurity/reward-program/ (Accessed 2015-05-31).

[7] Microsoft. *Coordinated Vulnerability Disclosure*. URL: https://technet.microsoft.com/en-us/security/dn467923.aspx (Accessed 2015-05-31).

[8] Facebook. *Responsible Disclosure Policy*. URL: https://www.facebook.com/whitehat (Accessed 2015-05-31).

[9] Symantec. *Vulnerability Management Commitment and Disclosure Policy*. URL: https://www.symantec.com/en/au/security/ (Accessed 2015-05-31).