AusCERT

Senate Standing Committees on Community Affairs

Inquiry into Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011 and the Personally Controlled Electronic Health Records Bill 2011

AusCERT Submission
January 2012

Table of Contents

Background

1. The following is AusCERT's submission to the Senate Standing Committees on Community Affairs inquiry into the Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011 and the Personally Controlled Electronic Health Records Bill 2011.

2. AusCERT is committed to protecting the privacy and security of Australian Internet users and has been active in identifying threats to Internet connected computers, online information, transactions and accounts and explaining how the online environment has can be used for malicious and illicit use. This extends to the compromise of Personally Controlled Electronic Health Records (PCEHR) by miscreants for identify theft and fraud. This submission draws primarily on three previous AusCERT submissions:

   - 2007 Electronic Funds Transfer submission to ASIC (attached)
   - 2007 AusCERT submission to the Australian Law Reform Commission - Inquiry (ALRC) into Privacy (attached).
   - 2009 AusCERT submission to The House of Representatives Standing Committee on Communications – Inquiry into Cyber Crime (attached)

3. These submissions also contain relevant background on AusCERT including its function and capabilities and this information is not duplicated in this submission.

Executive summary

4. The issues and concerns raised by AusCERT in the 2007 ALRC submission are as relevant, and in some cases more, in the current online environment given that the threats posed have increased over time as the capabilities of attacker and the richness and size of the target environments have also increased.

5. The inclusion of personal identifying information (PII) in the form of PCEHR to be accessible from personal computers over the Internet which are easily compromised, is compounding a problem that has been progressively getting worse over several years and will expose more Australians to fraud and identity theft.

6. The 2009 AusCERT Cyber Crime submission outlines the nature of the threat. Since 2009 the situation has continued to worsen and now include a range of new and highly sophisticated threats emerging that specifically target Internet infrastructure and enterprise and government networks.

7. In this submission, the focus is exclusively on the use of untrusted end point computers and mobile devices and how when compromised, they will enable

attackers full control over the PCEHR to view or modify its contents with the same privileges as the owner or particular authorised user. This is not to say that the other parts of the system are secure or will not be attacked but the mitigations and approaches for these systems differ significantly and are beyond the scope of this submission.

PCEHR over the Internet

8. The current proposal by the Australian Government to provide PCEHR over the Internet, presumably via a standard Internet connection and browser software, will allow for the exposure of these records to theft and compromise. However, the Commonwealth Department of Health and Aging (DHA) is promoting the benefits of PCEHR over the internet on the basis that it will be secure. Specifically it claims that:

> *A personally controlled electronic health record (PCEHR) will be a secure, electronic record of your important health information.* [1]*; and*
>
> *The Security and Access Framework for the PCEHR System will ensure that the confidentiality, integrity and availability of information within the PCEHR System are not compromised.*[2]

9. These statements cannot be assured and are misleading, particularly if any client, end-user computer, used to access to the PCEHR, is already compromised by malicious software – that means the confidentiality of the PCEHR may also be easily compromised. It also means that there is the potential to compromise the integrity of the record, depending on the user's modification privileges.

10. These statements above appear to focus on the security of the back end systems and not the end point systems from which people will connect to this system. At best this is misleading and at worst it is a misrepresentation of the level of risk.

11. The threats to PCEHR are expected to be broad and extensive and fall into four main categories:

- The back end central infrastructure – includes server databases and data processing systems

[1] http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr#.TyIWC7J15oY

[2] http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/PCEHRS-Intro-toc~ch5~5_3#.TyIRvbJ15oY

- Intermediate data storage and processing systems – either at a practice or intermediate level. Examples include General Practice and specialist surgeries, pathologists, imaging centres, radiography etc.

- The data transport and communications – both protocols and channels used for end to end or server to server communication.

- The end point devices and software used by users. Users include the individuals whose personal information is contained in the electronic health record, who will seek to have electronic access to the information from time to time; health professionals, who need to access and update the information as required, and IT or administrative staff who may have to access the records or data as required. All these users will operate a client PC, or other device. – which include PCs and smart devices in homes, offices, surgeries etc. Potentially some individuals may access this information from public computers such as in Internet cafes.

12. The importance and significance of end point devices for security and privacy in terms of providing confidentiality (and integrity) for system transactions is explained in detail in the AusCERT 2007 submission to the ALRC. As outlined in the ALRC submission, the security of any transaction done over a public Internet is ultimately dependent on the security of each of the systems involved in the transaction as mentioned above.

13. In the case of the Internet, the computer used to connect to the system can be anything from a mobile device such as a smartphone, a home PC or laptop, a enterprise PC on a public or private network to a publicly used PC located in places such as Internet kiosks and business lounges.

14. Since 2003 these 'consumer' devices have been effectively targeted for compromise typically by criminals for the purpose of identity theft and fraud. The success of this approach using techniques such as 'phishing' and 'malware', have been well established and documented with the end result being access to PII and access credentials stored or processed on these compromised computers.

15. At a basic level, information security includes the primary security goals to provide:

    - Confidentiality of the information stored. That is to ensure that only authorised personnel have access to the information in accordance with their roles/functions.

    - Integrity. That is to ensure that only authorised personnel, including the person whose PII is contained in the electronic health record, are able to modify the data.

    - Availability of information stored or processed on a computer or communicated over a computer network to ensure that it is available to the health professionals when required for them to provide health services, as required.

16. If the computer has been compromised then it is impossible to protect the confidentiality of information.

17. A former Minister for Health, Tony Abbott, stated that:

> *If people can access their bank account details via the Internet, there's no reason why they shouldn't be able to view their health records in much the same way.*[3]

18. What this approach does not recognise is that the business model for the Australian banks is fundamentally different from the DHA. For the Australian banks, while they cannot ensure the confidentiality of the online transaction there are ways to ensure that the transaction has not been modified or changed from its original form (integrity). Also, in the vast majority of attacks against online banking system, the attacker's objective is through a variety of means involving phishing or malware attacks, to obtain unauthorised access to the online banking account to transfer money from the account to another account in control of the criminal. Hence, for banks, their primary concern is to ensure that the integrity of the transaction is protected. There are various methods they use to detect potentially fraudulent transactions. While none are without their weaknesses and some are better than others, in general, the risk can be mitigated and managed, and there are ways to detect fraudulent transactions. In the worst case scenario, when a fraudulent transaction occurs, which the bank failed to prevent, the ultimate response of the bank is to reimburse the lost funds to the banking customer. Hence, in most cases the risk is managed and mitigated to protect the interests of the online banking customer/user.

19. For the online health record it is both the confidentiality and the integrity of the transaction that must be preserved. Hence detecting unauthorised access from a client computer or unauthorised changes from a client computer, will be difficult. When a client computer is compromised, the attacker operates with the privileges of the person who has authorised access and uses their compromised computer to facilitate the access; hence the use of audit trails and access monitoring is unlikely to detect unauthorised access or modifications, as the audit trail will point back to the particular authorised user and their computer.

20. As outlined in both the EFT Submission and the ALRC submission, online security, and hence the security of online transactions such as e-government, online banking and e-health (including PCEHRs), depends, inter alia, on end users being aware of the risks and having the knowledge, skills and resources to adequately manage those risks. It is AusCERT's assessment that the vast majority of end users do not have sufficient knowledge or skills to manage the risks in general. This is evident by the fact that in 2010 ACMA reported that about 25,000 – 30,000 computers are

---

3 http://www.tonyabbott.com.au/LatestNews/Speeches/tabid/88/articleType/ArticleView/articleId/3597/BETTER-RECORDS-MAKE-BETTER-DOCTORS.aspx

compromised in Australia every day and annually that equates to about 4 million PCs.[4] Considering that recovering from a computer compromises is a non-trivial exercise, it is likely that these compromises persist for days or weeks, and some may remain compromised; in many cases the compromises will not be detected by the user, or anti-virus software. Imagine if each of these computers had at least one user who used that computer to access their PCEHR. That represents potentially millions of records compromised by online criminals. It is apparent that if the owners/users had the skills to protect these computers, they would not have been compromised in the first place.

21. In the case of individuals who wish to access or modify their PCEHRs, a lack of knowledge and understanding of how to effectively manage those risks, means that the individual who opts in to PCEHRs, are at a greater risk of inadvertently compromising the confidentiality and integrity of that health record by using a compromised PC to do so. Unlike the banks, the compromise of this data is not easily detected; and even if it was detected, it is not possible to recover the loss of confidential information or unauthorised modification of PCEHRs, in the same way it is possible for a bank to reset a customer's password, or refund money stolen through a fraudulent transaction.

Privacy Impact Assessment on the PCEHR system

22. In November 2011 the Department of Health and Aging released a Privacy Impact Report (PIA) on the PCEHR system undertaken by Minter Ellison Lawyers and Salinger Privacy. The PIA report was over 150 pages and made 112 recommendations. However, on the critical matter of the security of the system, the report simply stated that this was not in scope for the PIA ie:

    1.1.2 What is not in scope for this PIA?

    This PIA report:

    (ii) is not an assessment of the adequacy of information security arrangements for the proposed PCEHR System. While ensuring appropriate data security is a critical privacy principle, expert assessment of the adequacy of information security arrangements will be required as the project moves towards a more detailed, operational level of design;

23. **While the PIA report acknowledges that data security is a critical privacy principle it is astonishing that this critical aspect is summarily dismissed and left to a later stage as the project moves on. This goes against one of the most basic information security tenants that effective security needs to be included in the**

[4] http://www.itnews.com.au/News/239580,acma-30000-australian-pcs-infected-every-day.aspx

design and architecture of the system and not done 'on the fly' or bolted on at the end. This approach does not bode well for the PCEHR system and shows an inadequate understanding of the risks posed to the security of the PCEHR, a lack of recognition of:

- the weaknesses in current approaches to protecting data confidentiality and integrity accessed via personal computers and devices; and
- the importance of ensuring all end user access points have a certain level of security standards and controls, as well as back-end databases and servers and data in transit over the Internet.

PECHR and Pharmaceutical fraud

24. A significant driver for the rise of online fraud and ID theft has been illicit financial gain. A key question relating to the PECHR is the ultimate value of these records. Certainly the PII information contained in the PECHR will have value to criminal enterprises for identity theft and fraud. Details such as full name, date of birth, current address and Medicare number are likely to be high on the list of useful PII credentials harvested by the criminals.

25. Additionally, there is legitimate concern in the health arena that the PECHR will deliver information to criminals which could be used to fraudulently obtain pharmaceutical drugs under prescription. Apparently criminals are realising that the purity of pharmaceutical quality drugs is worth pursuing rather than trying to 'cook' these drugs themselves. While it may be premature to predict the eventual outcome, this trend needs to be considered carefully with the possibility that the PECHR could be a catalyst to launch wholesale access to these drugs. This could have adverse implications for individuals, doctors and pharmacists, whose e-health records are manipulated in order to facilitate criminal endeavours, where the audit trail will lead back to those legitimate users who had access to these records, but who were in no way responsible for their fraudulent manipulation.

Conclusion

26. Ultimately, the PCEHR is meant to primarily serve the interests of the individuals whose medical information is contained in the health record. The emphasis on the records being "personally-controlled" is misleading as it implies the individual has full control over the record. This is not the case if individuals do not understand the risks to their EHR online when using a home PC, a work PC or other PC which may not be properly secured.

27. The focus on the security of the back-end systems and various data repositories is important, but is not by itself sufficient to mitigate this threat. Online criminals have

for many years been attacking PCs at work[5] and home in order to gain access to the systems and data they desire. There is no reason to think that once PCEHR goes live, criminals won't actively target these computers specifically for the benefits they may provide.

[5] In 2011, AusCERT advised of over 1,700 compromises to business and organisational computers. Therefore, it is not just home PCs which are being compromised.

APPENDIX A – List of Attachments

2007 Electronic Funds Transfer submission to ASIC (attached)

2007 AusCERT submission to the Australian Law Reform Commission - Inquiry (ALRC) into Privacy (attached).

2009 AusCERT submission to The House of Representatives Standing Committee on Communications – Inquiry into Cyber Crime (attached)