Electronic Health Records: Convenience Vs Potential Security Vulnerability

Roshan Hewapathiranae MBBS, MSc (IT), MIEEE
Executive Editor, Sri Lanka Journal of Bio-medical Informatics
Department of Informatics, Faculty of Mathematics and Natural Sciences, University of Oslo, Norway.
Visiting lecturer, Postgraduate Institute of medicine, University of Colombo, Sri Lanka
E-Mail address: roshanhewapathirana@gmail.com

Sri Lanka Journal of Bio-Medical Informatics 2011;2(2):38-40
DOI: http://dx.doi.org/10.4038/sljbmi.v2i2.3858

Information Technology is reaching all corners of the health care domain in the form of electronic health and medical records. Storage of personal information for remote access is now on the increase[(1)]. Computerisation of personal health records increase the portability and accessibility of data and at the same time it makes information more vulnerable to unauthorised and unscrupulous access[(2)].

In addition to the massive security and privacy issues that can arise if medical records reach an unauthorised person, electronic personal health records may also be targeted by the life insurance companies as a means of verifying the accuracy of the information provided by clients. According to Hoffman and Podgurski[(3)], electronic medical record systems need constant monitoring for unauthorised access and alternation of information including unusual updates of personal and clinical data. They further point out that the security of health information is, in fact, compromised with alarming frequency as a result of computer theft, sale of used computers without removal of data from hard drives, hacking, inadvertent disclosures and deliberate misuse of information.

An analysis performed by Pricewaterhouse Coopers LLP, USA based on the health information breaches reported to the US Federal Government over a 18 month period from September 2009, revealed that large scale breaches of personal health data happened on average every other day[(4)], It also revealed that 54% of health organisations reported at least one issue regarding information privacy and security over the past two years and out of all reported incidents, 73% involved electronic data.

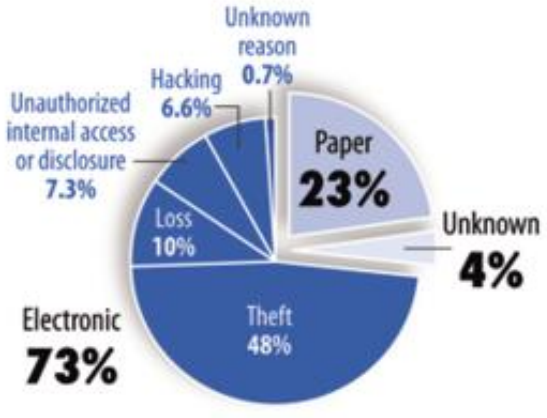

Figure 1: Electronic versus paper record breaches impacting over 500 individuals.

According to a US based leading provider of HIPAA risk analysis and IT security assessment services, Redspin, not only hackers, even authorised users with the intention of deliberate misuse of information, steal a surprising amount of personal health data by breaching computer security. It was mentioned in the Redspin *Breach Report 2010 - Protected Health Information*[5] that within the period of August 2009 to December 2010, the electronic health records of more than six million individuals were compromised and 61% of those security breaches were the result of malicious intent. However, the Redspin report focuses only on breaches involving more than 500 people which must be reported to the US Department of Health and Human Services under the breach notification provision of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Therefore, it is likely that more than six million people actually had their personal health information compromised in USA alone during the study period of 14 months.

Findings from the report, Protected Health Information include:

43	US states, D.C. and Puerto Rico have suffered at least one breach affecting *over 500 individuals*.
~27,000	individuals, on average, are affected by a breach.
78%	of all records breached are the result of 10 incidents, five of which are the result of theft of common storage media e.g. desktop computers, network servers, and portable devices.
61%	of breaches are a result of malicious intent.
~66,000	individuals, on average, are affected by a single breach of *portable media.*
40%	of records breached involved business associates.

According to the survey, it is clear that protected health information is actively targeted and has successfully been compromised by a malicious threat source. Unfortunately, it is expected that this trend will increase as healthcare informatics initiatives are deployed across the industry as a result of financial incentives associated with 'meaningful use' of objectives. Further, it was evident that locations that cannot rely on physical controls (laptops, mobile devices and portable storage devices) resulted in affecting the highest number of breaches.

Even though laptop breaches are more frequent, 39% of all records breached are a result of other portable media, including hard drives and backup tapes. This emphasises the need for adequate physical security controls for portable media devices, indicating that 246% more individuals are impacted as a result of a hard drive, backup tape, or other portable media device breach than an average data breach across all other locations.

Out of all health information breaches, medical identity theft is on the rise because it is profitable, and the increasing use of electronic health records makes more data accessible. Whereas stolen credit card numbers and other forms of financial data are losing their market value, medical insurance account information is becoming an expensive merchandise. A study conducted by the Ponemon Institute PLC, revealed that the average cost to resolve a case of medical identity theft is US $ 20,663, up from US $ 20,160 in 2010. Further in this

report, the Second Annual Survey on Medical Identity Theft[6], it is reported that roughly 1.5 million Americans are victims of medical identity theft. Technically, medical identity theft is an easier crime to commit, ranging from stealing the victim's name to obtain healthcare services or treatment to access or modify patient record where in most cases, the victim is either completely unaware of it (22%) or is too late in noticing (98%, after one month or never).

Even though electronic health records offer great opportunities in terms of interoperability and portability of health information, significant challenges also remain over balancing security and usefulness, standardising existing systems and managing changes to accommodate the rapidly advancing technologies. To reduce the likelihood and impact of a breach of information security, experts suggest implementing a proper incident detection and response programme, business associate oversight and formulating a portable media policy. More importantly, it is strongly recommended to develop a security plan that documents each component of the new system, including external connections, where sensitive data is stored and data encryption, access control, and assessment of vulnerabilities are in place.

Reference

1. Kalra D, Ingram D (2006). Electronic health records. In Zielinski K, Duplaga M, Ingram D (Ed.), *Information Technology Solutions for Healthcare* (pp. 135 - 181). : Springer-Verlag London Ltd.

2. Thomas C. Rindfleisch. 1997. Privacy, information technology, and health care. *Commun. ACM* 40, 8 (August 1997), 92-100.

3. Hoffman S, Podgurski A., Finding a cure: The case for regulation and oversight of electronic health record systems. Harvard Journal of Law & Technology 2008;**22**(1).

4. PwC Health Research Institute, Old data learns new tricks: Managing patient security and privacy on a new data-sharing playground, PricewaterhouseCoopers LLP, USA, 2011.

5. RedSpin Inc., Breach Report 2010, Protected Health Information, Redspin Inc , USA. 2010. Available from http://www.redspin.com/docs/WP_Redspin_2010_Protected_Health_Information_Breach_Report.pdf (Accessed on 10 December 2011)

6. Second Annual Survey of Medical Identity Theft. Ponemon Institute LLC, 2011.