Information Security Foundations for the Interoperability of Electronic Health Records

Wm. Arthur Conklin*
College of Technology, University of Houston
312 Technology Bldg., Houston, TX 77204
E-mail: waconklin@uh.edu
*corresponding author

Alexander McLeod
Information Systems Department /026
University of Nevada, Reno, NV 89511
E-mail: amcleod@unr.edu

Abstract: Electronic health records are clearly in the future of medicine and will provide benefits to all parties. Accurate and timely health record information is essential and dependent upon the security of the system and the security of related, interconnected systems. The current methodology of broad regulatory guidance and letting industry "do its best" has failed in the financial sector where identity theft has become a significant crime. Allowing the same outcome to occur in electronic health records will both limit the efficiency, effectiveness and interoperability of systems. The solution is to incorporate security "from the ground up" in a fashion similar to national security systems. To do so across the myriad of players in healthcare will require regulation. This paper explores the foundation for technical solutions and proposes security mechanisms to protect electronic health records.

Author

Keywords: electronic health records, electronic healthcare systems, information security, regulation, healthcare security

1 Introduction

There is little doubt that Electronic Health Records (EHR) will play an important role in the future of medicine. There is debate over how and when this transition will occur. Leading this debate are the many political and legal forces driving EHR adoption. For example, the U.S. Government established a ten-year plan directing health care organizations to implement interoperable electronic health records for most Americans by 2014 (Bush 2004; Cronin 2004). Another legal driver is the Health Insurance Portability and Accountability Act, passed in 1996. This law anticipated the movement to electronic healthcare systems and included provisions for protecting personal medical information (HIPAA 1996). Recently, the American Recovery and Reinvestment Act (ARRA) allocated $19.2 billion for health IT investment providing seed funds for medical providers to advance their EHR capabilities (ARRA 2009). While these and other legal requirements mandate usage, there has been little consideration of how to implement adequate security policies and mechanisms to protect individual privacy (Dunlop 2007). There is little doubt that all forms of electronic records must be protected given the security issues revealed by numerous data disclosure incidents over the past several years (Prince 2008; Privacy Rights Clearinghouse 2009). The purpose of this paper is to explore the necessary information security foundations needed to protect electronic health records. The remainder of this work is organized as

follows: First we discuss important contextual issues related to information security and electronic health records. Next we look at information security requirements and protection mechanisms followed by the EHR use case and summary. We conclude with a discussion of how these foundational elements can support the use of interoperable electronic health records.

2 Contextual Issues of Electronic Health Records

There are fundamental differences between electronic health records and electronic medical records which require definition (Carets and Davis 2005). Electronic Medical Records (EMR) typically contain clinical data captured by a single healthcare provider. Depending on state law, private practitioners who have already adopted electronic records usually own and maintain EMR data independently. EHR are more complex and frequently combine patient demographic information, medical history, treatment history, and other patient details. EHRs represent an aggregation of data from EMRs into a comprehensive health care record. Thus, EHRs provide the ability to connect information from physicians, hospitals, pharmacies, and other clinical data. To achieve this aggregation, potentially reduce medical errors, and improve the overall quality of healthcare, EHRs must be interoperable (Dunlop 2007). Interoperability requires that standards be adopted to ensure that data may be consolidated seamlessly. Unfortunately, this is a more complex issue than it appears since most practitioner data is decentralized. Patient X may have medical records at one or more doctor's offices, pharmacies, hospitals, and insurance systems. A recent article in the LA Times (Foreman 2006) illustrates, the large number of data

collecting parties involved in EHR systems. Although decentralized, many of the information repositories can collect very large quantities of data. Hospital systems, pharmacy chains, and insurance companies represent huge decentralized data stores (DHHS 2009) challenging interoperability and raising security issues such as "attack surface." Security concerns are compounded by the number of points where a system may be compromised. EHR entities sharing medical information produce a greater number of opportunities for hackers. More interconnected systems increase vulnerability and more devices provide greater opportunity. With such large systems comes large diverse user sets, increasing the potential for criminals to exploit vulnerabilities. With multiple independent systems, even if one organization has adequate security, the next one may not. . These EHR differences equate to greater risk of compromise to the data – termed "attack surface."

The number of people capturing and maintaining electronic health records is great. There are many different types of users of EHR. Some users need immediate access to information, such as emergency room personnel treating urgent care patients. The ability to have rapid access to medical records across the system can assist in accuracy of care and provide key medical history information to healthcare providers. Some of the tools used to provide rapid access represent security weaknesses, such as multiple system sign-on. While these mechanisms improve data availability for practitioners, privacy risk must be assessed. An electronic health record is a large collection of elements related to a patient's medical experience occurring in a doctor's office, a clinic, a

hospital, a pharmacy, or with any other medical provider. An average of 150 people (nurses, doctors, technicians, etc) will have access to at least some elements of a patient's record during a hospital stay (Foreman 2006). Privacy issues abound even among healthcare professionals. Electronic health records are comprised of many elements representing a treasure trove of opportunity for data and identity thieves. Criminals value demographic and identity information such as social security number, date of birth, address, and phone number. The financial information, including medical account and credit card information also make attractive targets for criminals. A new form of identification thievery takes the form of medical identity theft for the purpose of using someone else's insurance. The medical portion of the record, including diagnoses and insurance information has become the target of a new criminal element trading in these items of information for the purpose of committing medical fraud (Andrews 2008). Cases have occurred where identities have been compromised and people's insurance benefits have been fraudulently used by criminals, including the obtaining of prescription drugs (Andrews 2008).

A centralized database allowing all health records to be centrally located may ease some of these contextual concerns, but it also adds issues of data security, traffic management and other constraints. Current state-of-the-art security requires individual systems managing their own security issues according to the individual system's interpretation of risk management. One downside to this approach is that each PC or system through which records flow becomes a vulnerability. This requires significant system administration to reduce inherent

risks at each machine in the data flow. The specific protection required at each point in a record's travel will depend upon many factors, including the system using the record and the data elements exposed. Managing this diverse set of requirements across a distributed enterprise comprised of many different organizations is a challenge that will require a national level driver. The problem is that in some cases even a high level driver is insufficient to ensure compliance. The same features of digital records that permit ease of use also facilitate ease of theft and corruption. When examining the security requirements for electronic health records on a large scale basis, similar issues have been addressed in the personal financial records arena. If one examines the parallels in the financial world and the current growing issue of identity theft, several items become clear. Expecting the industry to be self-policing would not be a prudent course of action as the personal financial record industry has shown. Nor would laws regulating highly distributed data stores be beneficial in any significant way. After years of increasing fraud and data losses, the credit card industry formed an alliance and developed their own prescriptive security standard which applies to all entities handling credit card data (PCI Security Standards Council 2008). This is a contractually enforced standard across the business model, from merchant to processor to bank. Medical records may not be as distributed as the credit card industry, but this is the best parallel example currently in the electronic marketplace.

The creation of an electronic health information exchange and interoperability (HIEI) between providers is one method of realizing the opportunities promised

by EHR. The efficiencies afforded the system through the digital exchange of information is promoted with projected savings of over $80 billion annually (Hillestad, Bigelow et al. 2005; Walker, Pan et al. 2005). While these studies have analyzed the utility and efficiencies of a HIEI, they have not taken into account the risks and associated information security requirements of EHRs. The information captured in EHR and HIEI systems provides easily retrievable data via networks and creates significant risks representing unique security challenges.

3 Information Security Requirements

Information security is not a new topic in the industry or literature, with some seminal works dating back to the 1970's (Saltzer 1974; Bell and La Padula 1976; Biba 1977; DoD various). A wide range of formal models have been developed with specific applicability to differing protection environments (Landwehr 1981). These early studies were centered around military computer security needs, some of which did not translate to commercial systems in a useful fashion (Clark and Wilson 1987). Commercial systems tend to be built around the concept of a transaction, with security questions relating to what transactions users are permitted to do. The actual implementation of security measures requires not just consideration of the previously described contextual issues, but a tacit acknowledgement of the importance and necessity of addressing these concerns. This is typically implemented through a series of policies and procedures. Business policies and procedures are the means by which actions are managed in

an enterprise. Implementing information security controls in an organization or enterprise, requires that security risks be properly acknowledged and addressed. A key principle in designing and building a secure system is the decision point - "What security means for this system." Two important elements are needed to make a good decision with regard to security. First is the concept of information criticality; how important is the information and under what circumstances. The second is closely related – "What are the threats to the system and the information?" The terms confidentiality, integrity, and availability have been used to discuss security concerns and information criticality. Three additional attributes play a role in electronic health record security - authentication, accountability (including non-repudiation) and audit-ability. The first step is to examine an electronic health record and make a series of determinations regarding these attributes. Can the data be adequately protected and confidentiality maintained? Will the quality of the data remain reliable without unauthorized modifications? Can the availability of needed information be assured? Can those accessing data be verified? Will changes to data be associated with the user making those changes? Finally, does the data structure support an audit trail for forensic purposes? The results of this step can be used to properly formulate the appropriate level of security controls for the information in electronic health records.

4 EHR Use-Case

Authentication is a foundational element of any security system. Most controls will rely upon proper authentication of a user to determine the level of access

afforded to the user. Authentication is used to determine appropriate access and accountability with audit-ability setting the stage for future review. Examining a record and its use for patient X, we can investigate the relationships between the information and users, with respect to the computer security attributes. When the patient is in the emergency room (ER), medical providers are extremely reliant upon availability of the information and its integrity. In the ER, during an emergency, issues such as confidentiality (at the current moment) are less important than issues such as integrity and availability. For medical insurance and billing firms, availability is much less important since financial issues are not as time sensitive. Each user of the record has a separate valuation of the attributes associated with security, and each is based on their assessment of threats and risks.

Many if not all security measures depend upon authentication. To prevent credential theft and impersonation, stronger measures than simple passwords are required in high security situations (NIST 1994; NIST 2006). One solution is to use multi-factor authentication. Just as a doctor needs to show credentials to get privileges at a hospital, get an ID, and then use that ID to gain access to buildings, patients, etc., in the electronic health record arena the same levels of protection are needed. Use of a second factor, smartcard or token based, coupled with a biometric, prevents the sharing of credentials. Passwords alone fail because they can be shared, or impersonated, without detection. Coupling a token with a biometric resolves the sharing issue. All activity should be logged for each user on the system. Assignment of access based on credentials will be

based on the credential holder's "need to know", i.e. a nurse will not need to see financial information. Within organizations that have credentialed users, access to information can be restricted by the network through segmentation, regardless of credentials. From a records protection point of view, hackers may seem like an obscure entity non-threatening to most people; "We are small, why would they attack us?" or "We are protected by our network." But what about authorized personnel exceeding their authority? What about a pharmacist using his access to check the medical history of his daughter's fiancé? Clearly this would be a case of overstepping authority and also would be nearly impossible to detect. Can the electronic health record system protect information from this type of abuse? A combination of logging all accesses and use of the "need to know" principle will assist in mitigating this form of security failure.

Data associated with EHRs should be encrypted at all times, whether in storage or transit, to prevent unauthorized access to the content. All access to EHR data stores should require three conditions; authorized user credentials, authorized endpoint per network, and authorized data quantity per business rules. The first two are fairly obvious restatements of previous restrictions, but the third is intended to restrict multiple record accesses. Two different forms of access will be common, a single record for patient interaction, and multiple record interactions for billing, reporting, etc. Multiple record accesses should be further restricted to prevent data harvesting. The scope of multiple record accesses will also be garnered via business rules. All information in network transit should be encrypted to the accessing entities key tied to credentials, so that the credentials

will be needed to access any copy of the information once it leaves the data store. At all times when being transmitted over the network, data should be encrypted against the authorized user's key requiring credentials to re-access any information. This network segregation of information has an advantage over other security mechanisms by making the data unreachable. The network itself can act as a security mechanism, dropping packets that are not from authorized network addresses. Using the network layer as a segregation mechanism effectively breaks network connectivity. This further restricts access, as an authorized user must also be in an authorized location to even have network connectivity to the records. For example, a doctor will not be able to get to medical records from non-secure areas of the facility such as a receptionist's PC in the lobby. An outside agent, even with stolen credentials cannot access the records because of this connectivity barrier.

5 Use Case Summary

From the patient's perspective, the needed security attributes are as follows:

- All users of the record must be authenticated. (authentication)
- All accesses will be according to defined business rules. (accountability)
- All accesses will be tracked and logged. (audit-ability)
- Only users with specific purpose will be allowed access. (confidentiality)
- Only users with specific purpose will be allowed to modify records. (integrity)
- When needed and authorized the records will be available. (availability)

This is a much higher level of protection than any specific end user would apply and unfortunately has no advocate. Enforcing this level of use requirements across the health care organizations will require an external mandate.

6 Regulation

One element that plays a role in the security management decisions is the set of laws and regulations governing the system. Regulations to date are a combination of state and federal privacy laws. Currently security for electronic health records is built around a risk analysis methodology and enforced via HIPAA legal requirements (Centers for Medicare & Medicaid Services and Department of Health and Human Services 2007). These mechanisms are designed primarily to combat issues such as fraud and carry substantial penalties (Hyman 2002). While these types of regulations and penalties are needed to combat fraud, the process of securing electronic health records from unauthorized access must be combated at the prevention level, rather than the detection and punishment level. Current laws specify responsibility for protecting the information, but do not delineate how to achieve adequate protection, leaving organizations to make the required operational decisions to protect electronic health record data. History has not shown tremendous success in the distributed transaction environment of the financial credit card systems, necessitating regulations in that venue. It is not reasonable to expect all health care providers to come together and create the web of protection necessary to ensure data security, thus it will be necessary for government regulation to drive security behaviors.

7 Discussion

EHR's are ultimately digital records like modern finance, e-commerce and other database records. What separates them from other forms of digital records is their potential impact to members of society. An EHR security failure impacts people both financially and medically. Financial impacts associated with EHR fraud are similar to financial record fraud. The results of most financial frauds are relatively temporary in nature, causing a lot of work on behalf of victims, and possibly causing issues with financing of large ticket items, but ultimately these issues can be cleared up. Medical issues may not be as time forgiving. Records that are incorrect could cause incorrect diagnosis and improper treatments. Insurance related fraud may end up causing a patient to be denied care until disease progresses beyond simple treatment options. Finance record failures cause inconvenience, but medical record failures can result in life altering, and possibly life threatening results.

8 Conclusions

To be effective, laws must cover all aspects of the medical information privacy and data integrity problems, including technical, social and procedural aspects and in addition be proscriptive and specific. Mandating protection has not worked in other industries, so the mandates must be more specific, and must include penalties for failures that will deter skirting of the regulations. Dictating the levels of protection is a direct finding that comes form the failures of the

financial records industry, and the record there shows how tough it is to capture once lost.

These levels of protection need to be “designed in” from the lowest level for all aspects of the system. They are purposefully intended to completely encapsulate the data at all times. Technical methods alone would not be effective against all threats. For instance, against users enacting fraud through billing of services not rendered would need to be covered by other mechanisms. The addition of people and process measures will be necessary to ensure complete protection, In essence, what this solution attempts to create is a multi-level security solution across the system, forcing all entities to authenticate before access to protected information, and to always keep the protected information in an encrypted domain accessible to appropriate authenticated users.

One obvious path to enacting these security measures would be to centralize the storage of all EHRs, removing the security issues of the multitude of PCs and other record keeping systems from the direct security equation. Using a cloud based, thin client model, a HIEI entity could assume the burden of security functionality. The same network based data controls and encryption methodologies would still be needed, but centralization would make them more manageable and lower the unit cost. All users of the information could then connect via secure portals isolating EHR data and transactions from end point machines and their inherent vulnerabilities. This model is similar to mainframe based data models providing many advantages in security, redundancy, accessibility and cost. Rather than letting each provider manage their own

records, providers would be forced to subscribe to a centralized system. Although ultimately this may lower total costs, individual firms will lose control over their costs and local inefficiencies will create resistance to such large scale systems.

Electronic health records are needed for all the benefits that they can bring the health care system in terms of care and financial savings, but for these benefits to be fully realized, the system must be trustworthy (Gates 2002; Gates 2006). The true solution is one based on security built in from the ground up. National security systems are designed and built this way, with security being a primary factor at every junction. Healthcare records for the nation deserve no less protection.

9 References

Andrews, M. (2008). "Medical identity theft turns patients into victims." US News.

ARRA (2009). American Recovery and Reinvestment Act. Pub.L. 111-5 123 Stat. 115, H.R. 1 , enacted February 17.

Bell, D. E. and L. J. La Padula (1976). Secure Computer System:Unified Exposition and Multics Interpretation. Bedford, MA, Mitre**:** 129.

Biba, K. J. (1977). Integrity Considerations for Secure Computer Systems. Bedford MA, Mitre. **I**.

Bush, G. (2004). Presidential Executive Order. Executive. Washington, DC.

Carets, D. and M. Davis (2005). "Electronic Patient Records: EMRs and EHRs." Healthcare Informatics Online.

Centers for Medicare & Medicaid Services and Department of Health and Human Services (2007). Security Standards: Technical Safeguards. HIPAA

Security Guidance for Remote Use of and Access to Electronic Protected Health Information. **2**.

Clark, D. and D. Wilson (1987). A Comparison of Commercial and Military Computer Science Policies. 1987 IEEE Symposium on Security and Privacy, Oakland, CA, IEEE.

Cronin, K. (2004). The Decade of Health Information Technology: Framework for Strategic Action. D. o. H. H. Services. Washington, D.C. **3**.

DHHS (2009). Resolution Agreement CVS Consent order $2.25 Million in HIPAA Privacy Case. Department of Health and Human Services. Washington, DC.

Dixon, P. (2006). MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You, World Privacy Forum**:** 56.

DoD (various). Rainbow Series Library. N. C. S. Center. Washington, DC, US Department of Defense.

Dunlop, L. (2007). "Electronic Health Records: Interoperability Challenes Patient's Right to Privacy." Journal of Law, Commerce & Technology **3**(16).

Foreman, J. (2006). At Risk of Exposure. LA Times. Los Angeles, CA, LA Times.

Gates, B. (2002). email Subject: Trustworthy Computing. M. a. S. A. FTE. Redmond, WA, Microsoft Corporation**:** 3.

Gates, B. (2006). Keynote Address - "Microsoft's Security Vision and Strategy". RSA Security Conference 2006. San Jose, CA.

Hillestad, R., J. Bigelow, et al. (2005). "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs " Health Affairs **24**(5): 14.

HIPAA (1996). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Pub.L. 104-191, Aug. 21, 1996, 110 Stat. 1936.

Hyman, D. A. (2002). "HIPAA and Health Care Fraud: An Empirical Perspective." CATO Journal **22**(1): 29.

Landwehr, C. E. (1981). "Formal Models for Computer Security." ACM Comput. Surv. **13**(3): 247-278.

NIST (1994). Federal Information Processing Standards Publication 190 - Guideline For The Use of Advanced Authentication Technology Alternatives. Guideline For The Use of Advanced Authentication Technology Alternatives. US Department of Commerce. Washington, DC, National Institute of Standards and Technology.

NIST (2006). Federal Information Processing Standards Publication 200 - Minimum Security Requirements for Federal Information and Information Systems. Minimum Security Requirements for Federal Information and Information Systems. US Department of Commerce. Washington, DC, National Institute of Standards and Technology.

NIST (2009). NIST Special Publication 800-53 Revision 3 - Recommended Security Controls for Federal Information Systems. Recommended Security Controls for Federal Information Systems. US Department of Commerce. Washington, DC, National Institute of Standards and Technology.

PCI Security Standards Council (2008). Payment Card Industry Data Security Standard.

Prince, K. (2008) A Comprehensive Study of Healthcare Data Security Breaches In the United States From 2000 - 2007. **Volume**, 31 DOI:

Privacy Rights Clearinghouse. (2009). "A Chronology of Data Breaches." Retrieved February 19, 2009, 2009, from http://www.privacyrights.org/ar/ChronDataBreaches.htm.

Saltzer, J. H. (1974). "Protection and the control of information sharing in multics." Commun. ACM **17**(7): 388-402.

Walker, J., E. Pan, et al. (2005). "The value of health care information exchange and interoperability." Health Affairs **19**: W5-10W5.