Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Information Security Foundations for Electronic Medical Records

William Arthur Conklin
University of Houston, waconklin@uh.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2009

Recommended Citation
Conklin, William Arthur, "Information Security Foundations for Electronic Medical Records" (2009). *AMCIS 2009 Proceedings*. 407.
http://aisel.aisnet.org/amcis2009/407

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Information Security Foundations for Electronic Medical Records

Wm. Arthur Conklin
University of Houston
waconklin@uh.edu

ABSTRACT

Electronic medical records are clearly in the future and should provide benefits to all parties. Trust in the information is dependent upon the security of the system and the history of security associated with distributed electronic record systems should initiate many questions for such a critical system. The current methodology of broad regulatory guidance and letting industry "do its best" has failed in the financial sector with identity theft becoming a significant crime. Allowing the same outcome to occur in electronic medical records will both limit the efficiencies and imperil lives. The solution is to enjoin security from the ground up in a tight knit method similar to national security systems, and to do that across the myriad of players will require regulation. This paper explores the basis for the regulation of technical solutions and proposes a form in which they can be employed.

KEYWORDS
Electronic medical records, information security, regulation

INTRODUCTION

There is little debate over whether or not we will be moving to electronic medical records, the debate primarily centers over the when this transition will occur. The US Government has issued a Presidential Executive Order directing health care organizations to implement electronic medical records for most Americans by 2014 (Bush 2004). The Health Insurance Portability and Accountability Act was passed in 1996 and anticipated the movement to electronic medical records and included provisions for protecting this form of medical record (HIPAA 1996). For purposes of this article, the term electronic medical record is used for both electronic medical record and electronic health record, for with respect to the material in this article, they are essentially identical. There is also little doubt that all forms of electronic records suffer from security issues as indicated by the 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 policies needed for this type of electronic record.

Electronic medical records represent a treasure trove of opportunity for data and identity thieves. An electronic medical record is comprised of many elements, each with value to a criminal. The demographic and identity information present are valuable to criminals; social security number, date of birth, address, and phone number. The financial information, including medical account and credit card information for payments also are attractive targets to criminals. The medical portion of the record, including diagnoses and insurance information has become attractive to a new criminal element that trades in these items of information for 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).

The benefits of electronic medical records are numerous. There are many authorized users of the data, insurance companies, healthcare providers (including doctors and nurses), pharmacies and government entities. Some of these authorized users need immediate access to specific elements of a record related to medical care, as in the case of emergency room personnel treating urgent care victims. 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 emergency providers. The efficiencies afforded the system through the digital exchange of information is promoted as cost saving, with projected savings of over $80 billion annually system-wide (Hillestad et al. 2005). Coupling this level of

information in digital form, retrievable via computers over networks by a variety of parties represents a unique security challenge.

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 medical records on a large scale basis, the same issues that have been addressed in the personal financial records world appear. 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 broad based, non-proscriptive laws to regulate 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 proscriptive security standard to apply to everyone who handles 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.

INFORMATION SECURITY REQUIREMENTS

Information security is not a new topic in the industry or literature, with some of the seminal works dating back to the 1970's (Bell et al. 1976; Biba 1977; DoD various; Saltzer 1974). 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 needs for computer security, some of which did not translate to commercial systems in a useful fashion (Clark et al. 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. Further complicating the situation is the high level of interconnectivity across untrusted regions such as the Internet and the implications of the computer security intermediate value theorem (Bell 2005). The computer security intermediate value theorem states that the level of security is related to the levels of all the interconnected systems, in effect creating the value of the weakest link argument. This limits the security levels in highly distributed and Internet connected machines. Although trusted computing base machines exist for national security activities, the cost and flexibility prevented them from becoming relevant in today's commercial systems. This leaves commercial users with the aspect of having to apply external point defenses and architecting to mitigate risk.

A key principle in designing and building a secure system is the decision point of "What security means for this system". Two main elements comprise the knowledge 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 common attributes of confidentiality, integrity, and availability have been used to discuss the ramifications of threats. Three additional attribute also have a role in electronic medical record security; authentication, accountability (including Non-repudiation) and auditability. The key step is to examine an electronic medical record and make a series of determinations regarding these attributes. This will be examined from a use case scenario, where a user interacts with the system to achieve a specific outcome, the use-case.

EMR USE-CASES

An electronic medical record is really a large collection of elements related to a patient and the patient's medical experience. The experience element can be in a doctor's office, a clinic, a hospital, a pharmacy, or any other medical provider. To manage the financial aspect, there is also the series of third party groups, billing firms, insurance companies and government agencies. According to a report in the LA Times, an average of 150 people (nurses, doctors, technicians, etc) will have access to at least some elements of a patients record during a hospital stay (Foreman 2006). Privacy issues abound even among healthcare professionals as VIP records are frequent targets for snooping, leading to flagging systems to monitor access to specific records.

Examining a record and use for patient X we can investigate the relationships of the information and users with respect to the computer security attributes. When the patient is in the emergency room, medical providers are extremely reliant upon availability of the information and its integrity. Issues such as confidentiality (at the current moment) are less important. Authentication is needed to determine appropriate access, and accountability and auditability sets the stage for future reviews. For the medical insurance and billing firms, availability is much less

important as the financial functions are not as time sensitive. But these views are narrow and inaccurate, as they only represent the user's immediate needs. From patient X's point of view, the 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. (auditability)
- 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 user would apply and unfortunately has no advocate. Adding to this complexity is the naturally decentralized nature of the records. Patient X may have medical records at one or more doctor's offices, one or more pharmacies, one or more hospitals, and one or more insurance systems. As the LA Times article illustrates, the number of involved parties is large and diverse. A centralized database allowing all the records to be centrally located may make some aspects easier, but it would also add issues of data security, traffic management and other constraints. Although decentralized, many of the components can become very large repositories, as the number of large pharmacy chains, and insurance companies will represent large data stores (DHHS 2009).

HACKER METHODOLOGY

Criminals have been targeting electronic record for years to commit various forms of fraud. Medical records have been targeted as well, for they offer a treasure trove of information to sell (Andrews 2008). There is a pattern to most unauthorized computer accesses. The first step involves obtaining access in any form via stolen credentials. The credentials can be stolen via a wide range of methods which is not important in the big picture. Once the perpetrator obtains access to the system, they then can do a variety of methods to increase access to a privileged level to obtain access to the desired records. This is the challenge facing all computer system administrators. Software has all sorts of vulnerabilities. A talented hacker will be using credentials that legitimately allow access to systems under their protection. The system administrator must close or cover all the vulnerabilities, the hacker needs to only find a single unguarded point.

The greater the number of systems, the greater the attack surface area for the hacker to exploit and the greater the risk of compromise to the data. Also, with multiple independent systems, even if one organization has adequate security, the next one may not. Hackers are after information for many different reasons, but in most cases, the source is not as important as the fact that records are obtained. Hackers use the computer security intermediate value theorem to their advantage, leveraging their ability to gain access through the least protected point of entry.

From a records protection point of view, hackers may seem like an obscure entity that is not a threat to most people; "We are small, why would they attack us?" or "We are protected by our ISP." But what about already 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 system protect information from this type of abuse?

PROTECTION MECHANISMS

The current state-of-the-art in computer security involves each system taking care of its own security according to its own interpretation of appropriate level of risk management. One element that plays a role in the risk management decision process is the set of laws and regulations governing the system. The overarching sets of regulations to date are a combination of state privacy laws and HIPAA. These regulations specify responsibility for protecting the information, but do not specify how to achieve this protection. This leaves firms up to their own devices when making the operational decisions associated with protecting electronic medical record data. And history has not shown tremendous success in the distributed transaction environment of the financial credit card systems, necessitating the PCI DSS regulations.

The current state of security for electronic medical records is built around a risk analysis methodology and enforced via HIPAA mechanism (Centers for Medicare & Medicaid Services et al. 2007). These mechanisms are designed

primarily to combat issues such as fraud, and substantial penalties for health record fraud are provided (Hyman 2002). While the 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. Significant penalties associated with financial fraud have not stopped identity theft, for it is easy to steal and hide, avoiding prosecution. This same problem will occur with widespread adoption of electronic health care records – for penalties to work, they must be applied at a significant rate, and based on track records, the chance of prosecution appears slim. Widespread medical record identity theft will erode end user confidence and create significant additional burdens on several portions of the system, reducing the cost savings and value to users.

When market failures occur, one of the recourses available is government regulation. History has shown that distributed organizations with specialties other than computer security have a less than spectacular record protecting data (Prince 2008; Privacy Rights Clearinghouse 2009). The current HIPAA and state privacy laws do not close the security gap by providing appropriate levels of guidance. There are several systemic levels of protection that can be proscribed as minimum set of principles, including network based controls, authentication based controls and encryption to assist in properly securing sensitive data. Enacting these layer defenses, although frequently touted as proper in the literature, is seldom seen in reality. Reasons of technical difficulty, cost, convenience, and business necessity are given, yet when viewed in the whole, the current status quo approach for all industries is less than needed for something as critical as medical records. Fraudulent entries on a person's credit report may delay their ability to purchase a home or car. Fraudulent medical entries could cost them their life (Dixon 2006). The severity of loss to the third party in the information chain (the patient) coupled with the lack of that party's ability speak in the aggregate calls for intervention in the form of regulation.

To be effective, regulations must cover all aspects of the medical information privacy/integrity problem, including technical, social and procedural. This paper is only looking at technical aspects, just one part of the overall solution. There are three elements to the proposed solution; authentication, network segregation, and encryption. Each of these plays a role in securing part of the problem and together they resolve the issue of multi-level security and the computer security intermediate value theorem.

One aspect of the solution needs to be 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 digital realm the same levels of protection are needed. Use of a token, smartcard or token based, coupled with a biometric, prevents the sharing of credentials. Passwords alone fail because they can be shared without detection. Coupling a token with a biometric resolves the sharing issue. All activity will 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 will be restricted by the network through segmentation, regardless of credentials.

Network segregation of information by information criticality has an advantage over other security mechanisms by making the data unreachable by the network. The network itself can act as a security mechanism, dropping packets that are not from authorized addresses. Using the network layer as a segregation mechanism effectively breaks the network connectivity and can allow the firm to establish a break that isolates the records from outside access. This further restricts access, as an authorized user must also be in an authorized location to even have network connectivity to the records; a doctor will not be able to get to medical records from non-secure areas of the facility such as a receptionist in the lobby. An outside agent, even with stolen credentials cannot access the records because of this connectivity barrier. Wireless networks would be permitted, provided they are secured via VPN and NAC mechanisms. Business rules could also prevent multiple records to wireless connections as they are obviously there for patient level access interactions.

Encryption is not the be all and end all in security, but it does have its place. Using encryption of the data, one can affect the behavior of a VPN environment for the users accessing the data. All datastores of electronic medical record data need to be encrypted in stored form. All accesses to the datastores will require three conditions; authorized user per 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 will be further restricted to prevent data harvesting. And the scope of multiple record accesses will also be garnered in the business rules. All information in

transit will be encrypted to the accessing entities key that is tied to the credentials, so that the credentials will be needed to access any copy of the information once it leaves the datastore. At all times when in transit or storage, all electronic medical record data will be encrypted against the authorized user's key requiring credentials to re-access any information.

These levels of protection would need to be designed in, from the ground up for all aspects of the system. They are purposefully designed to completely encapsulate the data at all times. These technical methods would not be effective against users enacting fraud through billing of services not rendered, etc. and these would need to be covered by other mechanisms. In essence, what this solution attempts to create in effect 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. Just as a VPN creates a network within a network that is exclusive to users, this solution builds the equivalent around the information and further restricts it to specific networks.

CONCLUSIONS

Electronic medical records are needed for all the benefits that they can bring the system in terms of care and financial savings. But for those benefits to occur, the system must be trustworthy (Gates 2002; Gates 2006). Current protection mechanisms for electronic records of all sorts have shown to be less than desired and medical records could be even more of an issue. Not only are they much more sensitive from an impact to society perspective, but criminals already benefit from their skills developed against other enterprise network based record stores, making this more lopsided than previous situations. There are currently many separate point solutions, each attempting to mitigate a specific weakness. Solutions exist to monitor "VIP" records, as if their record is more valuable, and yet the very nature of the crime makes bulk records the currency of the crime. 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.

Enacting the technical security recommendations described will not totally resolve all security issues. There are still social and policy type issues that need to be resolved (Dixon 2006). But the technical basis will enable the rest of the security functionality a firm foundation from which to operate from, securing these records to the best available standard today. The party most in need of these protections is society, for if society is to gain from electronic medical records, society must be able to trust the records. The society at risk is the masses of patients, and errors will lead to damage to them, much greater than damages to the other parties, providers and payers. And yet this principal party does not have a seat at the decision making table when the appropriate level of protection decisions are resolved. Failure to regulate security will lead to failures resulting in lawsuits, which increase costs to the point that laws/regulations will become necessary to constrain liabilities, all still harming the victims.

There is an economic argument for regulation as well. If electronic medical records can save the system billions in efficiencies, then part of those savings should be redirected as an investment into enabling the implementation. As the Federal Government is the major player in the financial aspects of healthcare, it has a vested interest in the savings. Providers and payers have little financial incentive towards securing of the system, any gains they pocket, any losses can be pushed onto other parties. To correct these inequities requires regulation, and regulations stronger than current guidance.

REFERENCES

1. Andrews, M. (2008) "Medical identity theft turns patients into victims," *US News*), February 29 2008.
2. Bell, D.E. (2005) "Looking back at the Bell-La Padula model," in: *Computer Security Applications Conference, 21st Annual*, 2005.
3. Bell, D.E., and La Padula, L.J. (1976) "Secure Computer System:Unified Exposition and Multics Interpretation," ESD-TR-75-306, Mitre, Bedford, MA, p. 129.
4. Biba, K.J. (1977) "Integrity Considerations for Secure Computer Systems," Mitre, Bedford MA.
5. Bush, G. (2004) "Presidential Executive Order," Executive (ed.), Washington, DC, 2004.

6. Centers for Medicare & Medicaid Services, and Department of Health and Human Services (2007) "Security Standards: Technical Safeguards," in: *HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information*, 2007.
7. Clark, D., and Wilson, D. (1987) "A Comparison of Commercial and Military Computer Science Policies," 1987 IEEE Symposium on Security and Privacy, IEEE, Oakland, CA, 1987, pp. 184-194.
8. DHHS (2009) "Resolution Agreement CVS Consent order $2.25 Million in HIPAA Privacy Case," Department of Health and Human Services (ed.), Washington, DC, 2009.
9. Dixon, P. (2006) "MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You," World Privacy Forum, p. 56.
10. DoD (various) "Rainbow Series Library," N.C.S. Center (ed.), US Department of Defense, Washington, DC, various.
11. Foreman, J. (2006) "At Risk of Exposure," in: *LA Times*, LA Times, Los Angeles, CA, 2006.
12. Gates, B. (2002) "email Subject: Trustworthy Computing," M.a.S.A. FTE (ed.), Microsoft Corporation, Redmond, WA, 2002, p. 3.
13. Gates, B. (2006) "Keynote Address - "Microsoft's Security Vision and Strategy"," in: *RSA Security Conference 2006*, San Jose, CA, 2006.
14. Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., and Taylor, R. (2005) "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs " *Health Affairs* (24:5) 2005, p 14.
15. HIPAA (1996) "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," in: *Pub.L. 104-191, Aug. 21, 1996, 110 Stat. 1936*, 1996.
16. Hyman, D.A. (2002) "HIPAA and Health Care Fraud: An Empirical Perspective," *CATO Journal* (22:1) 2002, p 29.
17. Landwehr, C.E. (1981) "Formal Models for Computer Security," *ACM Comput. Surv.* (13:3) 1981, pp 247-278.
18. PCI Security Standards Council (2008) "Payment Card Industry Data Security Standard," 2008.
19. Prince, K. (2008) "A Comprehensive Study of Healthcare Data Security Breaches In the United States From 2000 - 2007," Perimeter eSecurity, Milford, Connecticut, 2008, p. 31.
20. Privacy Rights Clearinghouse (2009) "A Chronology of Data Breaches," Privacy Rights Clearinghouse / UCAN, 2009.
21. Saltzer, J.H. (1974) "Protection and the control of information sharing in multics," *Commun. ACM* (17:7) 1974, pp 388-402.