Summer 8-2011

IMPLEMENTING ELECTRONIC MEDICAL RECORD SYSTEMS: PRIVACY VS. SECURITY

Ryne Grotts
rygrotts@gmail.com

IMPLEMENTING ELECTRONIC MEDICAL RECORD SYSTEMS: PRIVACY VS. SECURITY

by

Ryne Grotts

B.S., Southern Illinois University Carbondale, 2009

A Research Paper
Submitted in Partial Fulfillment of the Requirements for the
Masters of Public Administration

Department of Political Science
in the Graduate School
Southern Illinois University Carbondale
August, 2011

RESEARCH PAPER APPROVAL

IMPLEMENTING ELECTRONIC MEDICAL RECORD SYSTEMS: PRIVACY VS. SECURITY

By

Ryne Grotts

A Research Paper Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Public Administration

in the field of Political Science

Approved by:

John Hamman Chair

James Sissom

Charles Leonard

Graduate School
Southern Illinois University Carbondale
5/13/2011

ACKNOWLEDGMENTS

I would like to thank Dr. John Hamman, Dr. Charles Leonard, and James Sissom for their assistance, guidance and direction throughout this paper. In particular I would like to thank Dr. Hamman for his recommendations on how to improve the flow and content of this paper.

I would also like to thank the professors from both my undergraduate and graduate instruction that gave me the knowledge of both technology and public administration.

A special thanks is also in order to my fellow students who have helped me throughout this journey in many ways. I also would like to thank Melissa whose help and support made this all possible. Finally, I cannot express my gratitude to my friends and family. Without them I would not have been able to accomplish what I have to date.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Societies increasing reliance on technology has created new headaches for medical personnel. Doctors now identify patients as suffering from 'nomophobia' (anxiety stemming from not having ones mobile phone), and 'mousewrist' (strain injury caused by prolonged use of a computer mouse) (Rauhofer, 2008). Along with this trend in lifestyle changes has been the collection of data about every aspect of our lives now kept in online databases (Rauhofer, 2008). These databases keep track of activities, purchases, and many other things. With technology people can buy anything they need online, order a pizza, and even do their taxes.

While people may seem to have lost the idea of what it is like to have something be kept private, health care is the one place where most still want privacy. So this raises an important question. Why are people so concerned with their medical records or other patient data when they otherwise expose private information routinely when they make purchases on eBay and participate on other social networking sites daily? In most other instances, most people don't think twice about their personal information. "In a 2005 CHCF(California Health Care Foundation) national consumer survey, 67 percent of respondents said they were "very concerned" or "somewhat concerned" about the privacy of their health information; in 2010, 68 percent expressed the same level of concern" (California Health Care Foundation survey, 2010).

Health care administrators have always been keen to keep patient information confidential. Indeed, an important part of the physician's code of conduct is privacy which dates back to about 400 B.C. with the creation of the Hippocratic Oath (Maria &

Paul, 2009). A single trip to the doctor can generate an abundance of personal data. Important identity information such as a Social Security numbers, insurance information, pharmacy records and medical test results are cause for concern when dealing with patient records.

> "Medical records kept by physicians and hospitals about patients may include identifying information, X-ray films, EKG and lab test results, daily observations by nurses, physical examination results, diagnoses, drug and treatment orders, progress notes and postoperative reports from physicians, medical history secured from the patient, consent forms authorizing treatment or the release of information, summaries from the medical records of other institutions, and copies or forms shared with outside institutions for insurance purposes" (Wen &Tarn, 2001, p.19).

The process of making health care records electronic is difficult. Organizations must decide what their specific needs are in order to determine an EMR vendor that fits those needs. There is a variety of equipment, staff, training, and costs that contribute to the success or failure of one's implementation. Health care and technical administrators must also deal with a variety of privacy issues and find a way of keep patient data secure. Currently, technical administrators utilize a number of techniques in an attempt to keep patient data secure. In addition, for health care administrators to successfully implement an electronic medical record (EMR) system they must follow legislation and guidelines laid forth by HIPAA, and the Privacy Act of 1974 (Social Security Administration, 2011, Rudloff & Jabouri, 1999). Today, health care administrators must grapple with utilizing modern information technology in order to improve the efficiency and effectiveness of

health care while at the same time maintaining the practice of doctor patient confidentiality, individual rights to privacy, and the integrity and security of the technology itself to avoid the system and personal privacy of patients from being compromised. Will this new technology improve or maintain patient confidentiality, and what does this mean for the security of health care information?

CHAPTER 2
BACKGROUND

Privacy Law and Legislation

The privacy act of 1974 laid the foundation for dealing with personal information (Rudloff & Jabouri, 1999). "The Privacy Act of 1974, as amended at 5 U.S.C. 552a, protects records that can be retrieved from a system of records by personal identifiers such as a name, social security number, or other identifying number or symbol" (Social Security Administration, 2011).

Congress subsequently passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 and set the standard for much of the statutes and legislation having to do with data privacy today. The act has two main objectives: "(1) to improve the efficiency and effectiveness of the health care system by standardizing the electronic exchange of certain administrative and financial transactions (focusing on EDI) and (2) to protect the security and privacy of transmitted information" (Rudloff & Jabouri, 1999, p.33). HIPAA also puts constraints on data privacy for the good of patients. The courts of the United States have found that physicians are liable for releasing doctor patient privileged information (Maria & Paul, 2009). Not only is this protected under law but doctors who reveal a patient's private medical information to anyone without consent is accountable for any damages that the patient might have as a result of such disclosure (Maria & Paul, 2009). Breach of confidentiality is also considered malpractice because it violates a standard of care to which the doctors agree (Maria & Paul, 2009). Many statutes are for the protection of the patient. Some protect from a broad standpoint where others protect a specific type of patient data. Some other statutes for example create

protections for specific conditions such as HIV/AIDS, and alcohol and drug abuse (Maria & Paul, 2009).

In addition to personal information such as specific medical conditions federal statutes give protection for health care information held by federal agencies, information held by health care organizations operated by the government, and organizations that participate in Medicaid, Medicare, and other federal health care programs (Maria & Paul, 2009). HIPAA makes sure that no one person or organization has access to a patient's health records without that patient's permission.

HIPAA was also the first legislation passed that protected not only a patient's personal data and medical records, but also their insurance information. HIPAA states that insurance information must only be used for treatment, getting payment or for improving care (Maria & Paul, 2009). HIPAA also "established standards and requirements for the electronic transmission of certain health information (eligibility requirements, referrals to other physicians, and health claims" (Maria & Paul, 2009, p.143). Along with doing all of these things and protecting a patient's confidentiality they also laid forth certain civil and criminal penalties for giving out information without permission and breaking the patient doctor confidentiality (Maria & Paul, 2009).

HIPAA requires any agencies they do business with to have a contract. Health care providers, who use electronic or paper records, are required to have a contract to make sure that they are following the policies and procedures set forth by HIPAA (Maria & Paul, 2009). These organizations include hospitals, physicians offices, health care plans, employers, public health authorities, life insurers, clearinghouses, billing agencies,

information systems, and “any person or organization who furnishes, bills, or is paid for health care in the normal course of business”” (Maria & Paul, 2009, p.144).

HIPAA has four general issues that their policies and procedures should address when dealing with data privacy and the patient’s well-being: 1. the policies and procedures to oversee issues of confidentially, data integrity, and data access. 2. Physical boundaries that limit access and protect computer systems from disasters such as fire or flood. 3. Technical security techniques to protect data which is stored in information systems such as an EMR system. 4. Technical measures that prevent information sent over the network from being intercepted (Maria & Paul, 2009). All of their policies are in place to make sure that patient data is kept safe and private and does not fall into the wrong hands and is not used to exclude someone from a group or job consideration (Maria & Paul, 2009).

HIPAA requires providers to safeguard the integrity and confidentiality of all written, electronic and oral personal information (Maria & Paul, 2009). The case of *Bagent v. Blessing Care Corporation* (2006) illustrates a blatant HIPAA violation by a hospital employee. Misty Young (defendant) a phlebotomist employed by Illini Hospital divulged confidential patient information to Suzanne Bagent’s twin sister at a public tavern. Suzanne Bagent (plaintiff) had blood drawn and the results sent to Illini Hospital earlier that month. The defendant cited in testimony, that she completed the required HIPAA privacy training, and understood the implications if the rules were violated. The case is currently in the trial stage.

There are also groups intending to help ensure that data is secure and does not fall into the wrong hands. The International Medical Informatics Association (IMIA) is an

independent organization established under Swiss law in 1989 (International Medical Informatics, 2011). IMIA provides leadership and expertise to the health focused community and policy makers to allow health care to improve worldwide (International Medical Informatics, 2011). In 1979 the Swiss put in a bid to establish the IMIA in order to meet specific needs in the application of information science and technology in the fields of medicine, health-care and biomedical research (Smith & Eloff, 1999). One of the fifteen groups that make up the IMIA deals specifically with data protection and established the initial approaches for securing hospital information systems (Smith & Eloff, 1999).

The second Bush Administration called for a nationwide implementation of EMR systems by 2014 (Vinsion et.al., 2008). To assist Bush's effort Congress approved a health IT bill in 2008 which would provide nearly $560 million dollars in loans and grants to health care providers and physicians (Vinison et al., 2008). This is an idea that the Obama administration has vowed to see implemented. "President Obama and his administration have agreed to fulfill Bush's vision of full implementation of EMRs. President Obama has promised to spend $50 billion over five years on Health care Information Technology and fulfilled more than one-third of the pledge with $17.2 billion in the economic stimulus package to help health care organizations with adopting electronic record systems" (Brown, 2009, Brooks & Grotz, 2010, p.75). Even with the money given to have these systems implemented, there are a number of hurdles that have made this more tedious than many anticipated.

The Need for Economy in Health care

Electronic Medical Records (EMRs) are the latest way of documenting a patient's medical information. If the implementation of Electronic Medical Records is achieved, administrators and doctors will improve the quality of health care while at the same time lowering the cost. This has been a difficult road however (Brooks & Grotz, 2010). Deploying any large system is complicated and costly and this is true in the health care industry. If done correctly this new type of system will be greatly beneficial but there are also many challenges that make the implementation and success difficult and slow. With HIPAA and other privacy legislation setting the standard for health care privacy, the next major hurdle administrators face is cost. The continual rise in cost for health care leaves administrators attempting to balance the justification of implementing an EMR while still trying to provide treatment at an affordable rate (Brooks & Grotz, 2010).

Probably the most talked about challenge is financial. It is not cheap to go from a paper system to an electronic one. Change is required in areas such as storage media, network infrastructure, and training of employees (Brooks & Grotz, 2010). “One northern Kentucky provider with 1,000 physicians and six hospitals is spending $40 million on an EMR deployment” (Brooks & Grotz, 2010, p.79). This is a major deterrent for physicians and clinics. Many providers see the high price tag and a lack of investors and decide that they do not want to implement such a system (Anderson, 2007).

EMRs are supposed to save a lot of money in the long run but can also be costly to start up. There have been several estimates of how much it will cost to implement such a system dating back to the second Bush Administration. Some say that such a system “can cost hospitals $20 million to $200 million due to implementation, vendor and

hardware costs, staff training and upkeep" (Leo, 2009, p.16). Estimates put the initial cost of an EMR in a range from $16,000 to $36,000 per physician (Anderson, 2007).

Maintenance of the system and decreased revenue from patients during the transition from the paper chart to the EMR require additional costs (Anderson, 2007). The cost however is not limited to just hardware and software (Brooks & Grotz, 2010). The cost must include, consulting, training, additional software such as billing software and many other unforeseen expenses (Brooks & Grotz, 2010). Many experts also say to include glitches in software or hardware that cause loss of productivity and slow billing processes (Brooks & Grotz, 2010). This is very common in new systems and in return costs more money (Brooks & Grotz, 2010). It is important to overestimate cost when implementing a new EMR system because an organization will always spend more than they originally estimate (Brooks & Grotz, 2010). One executive director at a medical facility in North Carolina recommends adding 50 percent to the cost of an EMR system for lost productivity, training, and other unforeseen problems during the early implementation stages (Brooks & Grotz, 2010).

It is also important to understand that these new systems can exclude certain groups because of the cost. Some of the smaller organizations will not be able to afford to implement such a system. Larger hospitals and health organizations might be able to afford the cost of implementing an EMR but to smaller organizations such as individual physicians or a small group the cost presents a problem (Funke, 2008). Physicians argue that the patients have everything to gain at this point when compared to the practitioners. The practitioners have to absorb a lot of cost as well. Physicians participating in an EMR system have no direct financial benefit but absorb participation costs such as, lost time

and productivity due to learning new processes, training of staff, and risks that come with system failure or data loss (Funke, 2008).

Even some of the larger groups may not be able to afford such a system without subsides from government organizations or private donors. Some of the larger health care organizations have had to use federal and state funds along with subsidies from the government in order to implement and EMR system (Joch, 2008, Funke, 2008). Companies such as Kaiser Permanente and Blue Cross and Blue Shield have also helped subsidize some systems (Joch, 2008, Funke, 2008). The only way it seems plausible for the doctors and physicians to implement such a system is if the patients are willing to pay for such services (Funke, 2008). Figure 3 represents a sample cost benefit analysis of a single doctor medical office conducted by EMR experts, a web based company that organizes, and improves medical office workflow by choosing a system that fits ones practice.

Cost-Benefit Analysis Example (Single Provider Office)	Initial Costs	Year 1	Year 2	Year 3	Year 4	Year 5	5 Year Total
Costs (Per Provider)							
Software License	$10,000						
Implementation – Software Customization ($100/hr x 10 hrs)	$1,000						
Implementation – Training ($100/hr x 25 hrs)	$2,500						
Implementation – Travel Expenses	$1,500						
Implementation – Computer & Network Setup	$1,000				$1,000		
Hardware – 1 x Tablet PC	$2,500				$2,000		
Hardware – 3 x Workstations	$3,000				$2,500		
Hardware – Network/Server	$2,000				$1,000		
Support & Maintenance – Software		$2,000	$2,000	$2,000	$2,000	$2,000	
Support & Maintenance – Computer		$1,000	$1,000	$1,000	$1,000	$1,000	
Induced Costs – Productivity Loss (40 hrs)	$10,000						
Gross Annual Costs	**$33,500**	**$3,000**	**$3,000**	**$3,000**	**$9,500**	**$3,000**	**$55,000**
Additional Physician Adjustment (10%-30%)							
Net Annual Costs							
Benefits (Per Provider)							
Improved Coding		$12,500	$25,000	$25,000	$25,000	$25,000	
Transcription Savings		$3,000	$6,000	$6,000	$6,000	$6,000	
Chart Management		$2,400	$4,800	$4,800	$4,800	$4,800	
Searching for Charts		$1,000	$2,000	$2,000	$2,000	$2,000	
Prescription Refills		$3,250	$6,500	$6,500	$6,500	$6,500	
Capitated Benefits (If applicable)			$29,000	$29,000	$29,000	$29,000	
Total Annual Benefits		**22,150**	**$44,300**	**$44,300**	**$44,300**	**$44,300**	**$199,350**
Net Benefit (cost)	**$(33,500)**	**$19,150**	**$41,300**	**$41,300**	**$34,800**	**$41,300**	**$144,350**

Figure 1: Cost-Benefit Analysis Example on hypothetical single doctor medical office (EMR Experts, 2010).

Cutting Costs

Although implementing an EMR can be costly initially, the long term benefits of the implementation outweigh the expensive startup. Implementation of an electronic system would help cut down on the high cost of health care due to a number of reasons. "Electronic records, according to proponents, will reduce inappropriate treatment, duplication, fraud and errors" (Funke, 2008, p.6). This would make it much easier for insurance companies to find fraud within health care systems which in return would lower the overall cost (Funke, 2008). It is a well known fact that patients might "doctor shop" to receive more of a restricted prescription (Funke, 2008). With an electronic system in place the pharmacy could monitor it continuously and therefore prevent things of this nature from happening. Not only do patients try to 'game' the system, providers have been known to do it as well. "Studies have found bills for patient visits or treatment and in office tests that are not needed, or for services that were not provided, sometimes based on billing for numbers of patient visits that are not feasible" (Funke, 2008, p.6). Implementing these systems could keep patients as well as providers from committing fraud, therefore cutting costs. Doctors understand that health care costs are astronomical and EMR systems provide a more efficient and effective way of providing patient care, therefore lowering costs in the long run.

Effective and Efficient Treatment

When disasters such as Hurricane Katrina hit many people all of a sudden had no medical records. People working in relief areas had a very hard time treating these people (Brooks & Grotz, 2010). It became evident that doctors and physicians did not want to repeat this nightmare. Having EMRs allows medical organizations to avoid this type of

situation. People's entire medical records along with test results and medications are available with just the click of a mouse (Funke, 2008). It can be very dangerous to rely on memory of previous tests, diagnoses, and medications. Patients are not doctors and they simply cannot remember everything (Funke, 2008).

Caring for U.S. soldiers provides another example. Being able to treat wounded soldiers quickly and have follow-up treatment as they are moved to and from different hospitals and places of treatment requires reliability and continuity of records (Funke, 2008). It is important for a physician to know everything about that solider including treatments, and prescriptions that they have received because they have most likely seen different doctors in different medical facilities (Funke, 2008) Although the case of war and soldiers seems a bit extreme it also plays a factor in every day civilian life (Funke, 2008).

The thought behind implementing such a system is to have complete and accurate data no matter where a patient is located. Such a system will save lives and decrease the amount of time it takes to diagnose an illness or determine a person's medical history (Simmons, 2009).

> "The 'theory' is such that when a new patient presents to your office you can access that patient's database and pull in as much of that patient's medical record as is necessary. This will allow all health care providers, hospitals, pharmacies, etc., instant information on patients. It would behoove everyone to understand why anything short of an EMR is essentially a waste of your time and money" (Simmons, 2009, p.10).

Such a system would make sure to eliminate such errors and more spend more time on what really matters, providing effective and efficient care to patients.

CHAPTER 3:
ELECTRIFYING PATIENT RECORDS

The Conversion Process

Making the switch from paper records to electronic records is not without its challenges. Going paperless requires a number of things including vendor choices, equipment, training of staff, and cost.

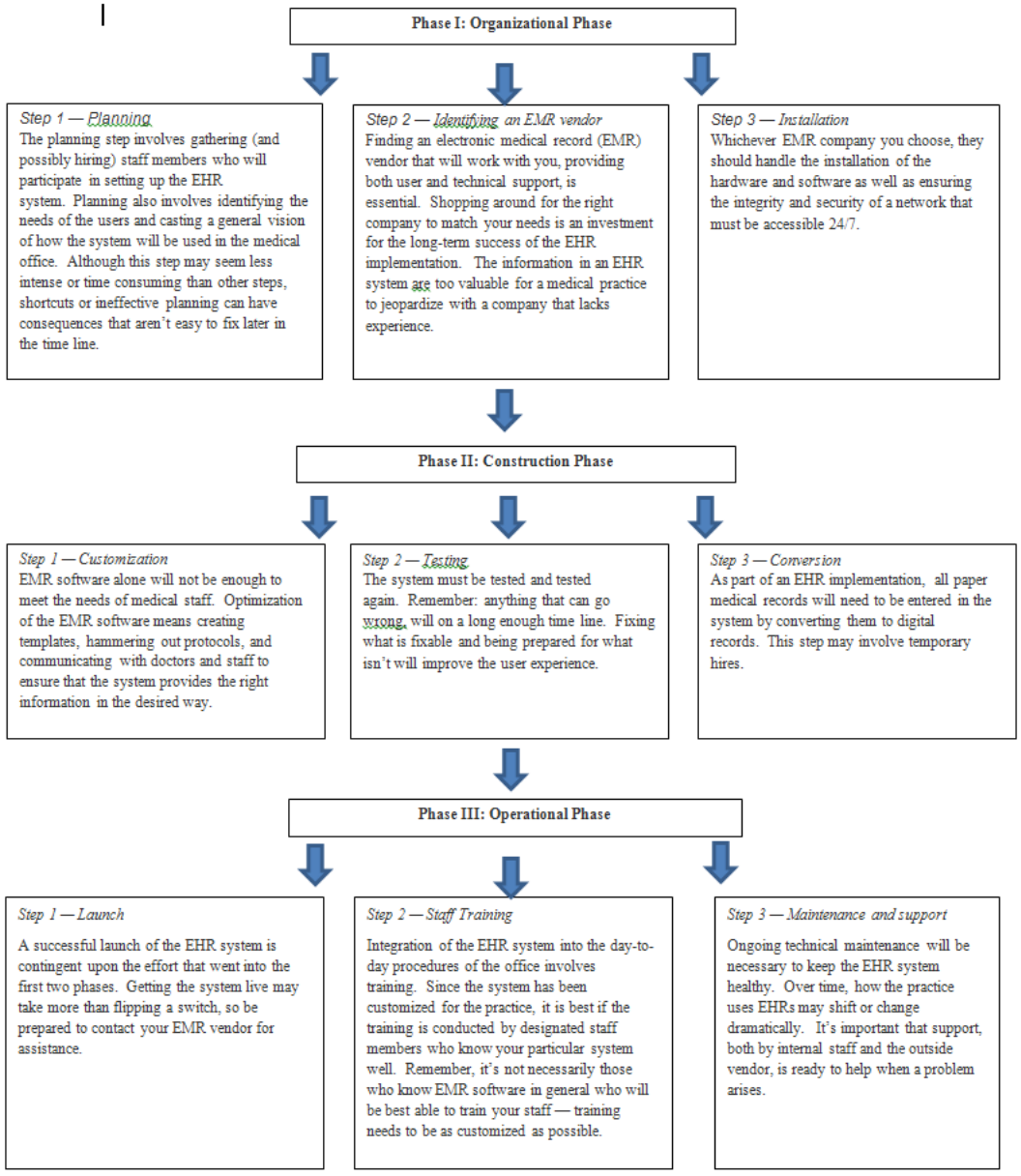

Figure 2: Phases of EMR Implementation (Hill, 2009)

Figure 2 shows a sample of the various phases of implementation for an EMR system. Each phase contains a number of steps that health care organizations must take when looking to implement an EMR. Health care administrators must consider a number of measures when dealing with patient data and the implementation of an EMR. Complex networks accompany complex problems. With over 400 vendors being available it is important for administrators to choose the one that best suits the needs of their company (Renner, 2009).

Once the administrators choose a vendor who can customize to the company's needs it is ready for the construction phase (See figure 2). Computers and networking equipment are the backbone of an EMR system. Vendors can provide computers or the organization can purchase them on their own. Either way the system access must be the same for all employees (Terry, 2008). Limiting access can cause major problems. Often organizations limit the purchases of desktop computers for the staff and doctors end up completing the work that data entry staff should be doing, therefore decreasing productivity (Terry, 2008).

Organizations have many choices when choosing what equipment to use for implementing their EMR system. Desktops, laptops, tablet PC's, cables, and networking devices (routers, switches) are all needed in order to set ones network up properly (Terry, 2008). Each organization must consider cost when implementing such a system. Such a system "can cost hospitals $20 million to $200 million due to implementation, vendor and hardware costs, staff training and upkeep" (Leo, 2009, p.16). Installing wired desktop computers is often cheaper and preferred over laptop computer because of the

cost (Terry, 2008). Laptop computers require additional battery packs and secure wireless network to fully utilize its portability which in return means more money spent on equipment (Terry, 2008). In addition laptop computers can die when not plugged in often leaving staff members in an awkward position trying to care for patients and input information (Terry, 2008). Ron Sterling, an IT consultant, even recommends that health care organizations invest the extra money in tablet PC's because it eliminates the staff having to run around looking for a computer that is not in use (Terry, 2008).

Once the network is set up and tested operational the shift focuses to the staff (See figure 2). Data entry staff is perhaps the most important when making the transition from paper records to electronic. It can be very difficult when a current patient comes in for a visit, and their record is opened there is nothing listed about that patient (Terry, 2008). To avoid this data entry staff needs to enter information on active patients at least three months before the 'go live' date of the system (Terry, 2008). In addition to the data entry staff, IT staff is perhaps equally as important. It is very important that health care administrators hire a computer technician that can keep the computers and the network running as needed (Terry, 2008). Many vendors who set up networks offer technical support but often the staff will end up on the phone for hours with offsite support trying to fix a problem that a local technician can fix easily (Terry, 2008).

After the shift from paper to electronic records and the implementation of the EMR including, equipment, software and staff, the issues of confidentiality integrity and availability are beginning to come to light. An EMR system increases the reliability of patient records by making the records confidential and readily available (Wen & Tarn, 2001). Confidentiality is increased because patient's records are now stored in a secure

database. It is very important that when transmitting data between networks that records are being protected from unauthorized access (Wen & Tarn, 2001). The implementation of an EMR eliminates the loss of paper files. An EMR allows multiple health care organizations to share patient data without concern for error (Wen & Tarn, 2001). Availability is based on the fact that people who should have access to records cannot be denied access for any reason (Wen & Tarn, 2001). This can often been seen during peak usage hours when networks might be slowed down and access not granted to those who are authorized (Wen & Tarn, 2001). This is just the beginning of the implementation process; health care administrators must now address privacy concerns, threats to security and the need to protect data from unauthorized use.

Security Issues

Transferring health records from paper to electronic form does not eliminate the need for the securing of health care data and their networks. If anything more security must be put in place to keep records secure especially in a business environment that is becoming electronically driven. Lost, stolen, and abused data are privacy issues that health care administrators must address (EHR Scope, 2009). When dealing with an information system, security professionals must face a changing array of threats. Greenmeier (2005) notes that many companies spend money to stop outside threats such as hackers or identity thieves, but what they should be worried about their own employees. Figure 3 shows a list of security threats, including internal and external threats ranked according to seriousness.

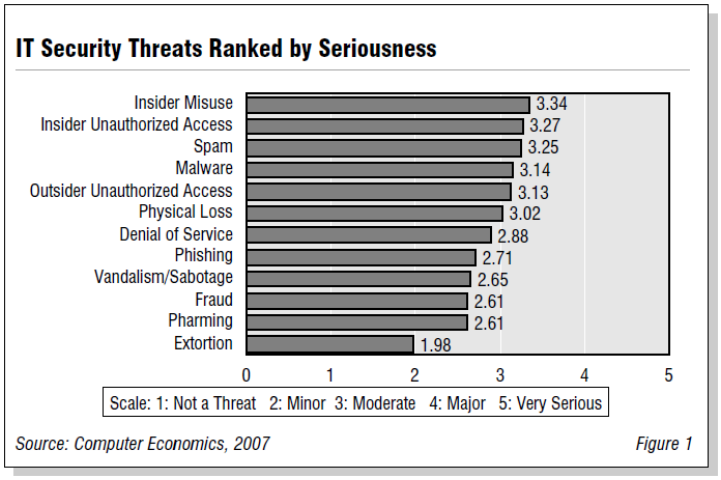

Figure 3: Security threats ranked by seriousness (Computer Economics, 2007, p.1).

Health care organizations would like to think that the people they hire are trustworthy and do not pose a threat. The fact is however that more often than not the biggest threats the organizations face are internal. Keith Jones, a computer forensics expert notes that all organizations face threats from two main sources- internal and external (Wolfe, 2007). Wolfe goes on to state that the most devastating type are internal attacks (Wolfe, 2007).

Figure 4: Percentage of espionage suspected by IT professionals (Greenemeier, 2005)

Figure 4 shows the percentage of malicious activities that IT professionals say is the work of internal threats. There are two reasons why internal threats are far more dangerous than external threats. Internal threats have two critical elements that can make a successful attack, 1) the ability to bypass security measures and 2) prior knowledge of the organizations business and networking infrastructure (Wolfe, 2007).

When threats are not taken seriously or networks are not adequately secured, bad things can happen such as security breaches leading to misuse or destruction of patient data. Health care administrators have dealt with problems of data privacy often. For example, there are many instances in which personal information and medical records were lost, stolen or made public. In March 2008, UCLA Medical Center took disciplinary action against a dozen employees for violating patient's rights and viewing their personal medical records (Raths, 2008). Hospital employees improperly viewed records on celebrities such as Britney Spears, and Maria Schriver along with thirty one other celebrities, and the information later appeared in tabloid newspapers (Furillo, 2008).

Another instance of a data privacy breach occurred in 2009 when hackers demanded a $10 million dollar ransom for approximately 8.3 million patient records they had stolen from a Virginia government website that tracks prescription drug abuse (EHR Scope, 2009). The Virginia Department of Public Health confirmed that the information stolen included social security numbers and other information valuable to identity thieves (EHR Scope, 2009). Authorities are not sure if the hackers compromised data or used it maliciously (EHR Scope, 2009). Many government agencies do not have a budget that will allow them to take the best security measures in order to prevent future attacks (EHR Scope, 2009)

External threats are not as common as internal threats but still occur because the people within an organization allow them access to the network. The most common external threats are malicious email, and websites (Wolfe, 2007). Email phishing marks a target through email to gain unauthorized access to confidential data (Waxer, 2007). Some of these attacks can be very sophisticated and will appear as if though they are from a bank or credit card company (Waxer, 2007). This results in employees giving confidential information such as passwords, or financial data to intruders (Waxer, 2007). Dangerous web sites operate in almost the same way. These websites contain a tool of exploit (Trojan virus) that will allow an attacker to gain access to a person's computer (Waxer, 2007). From there the intruder can help themselves to any data available on ones computer (Wolfe, 2007). The motivation of most computer attackers is usually financial in type and consists of credit card numbers, social security numbers, and account information (Wolfe, 2007).

Methods to Secure Patient Information

Many security professionals would strongly advise against using the Internet to transmit important information because it may not be as secure as we give it credit for. There are however, some solutions for making a network more secure. The technical solutions to secure a network are in three categories: 1) cryptography applications for encrypting and decrypting, access authorization, and secure network protocols (Smith & Eloff, 1999). With the sharing of information over the internet organizations must be sure to make sure that not just anyone can view this information.

"Encryption is the chief technology by which third parties may be prevented from reading confidential patient information" (Smith and Eloff, 1999, p.44). This

encryption takes the information that you are transmitting and scrambles it so people with malicious intentions may not read it. This way if someone is stealing information as it transmits, they cannot decipher what the information is without an extreme level of expertise (Smith & Eloff, 1999).

There are two different approaches to encryption, symmetric and asymmetric. The symmetric approach has a key or algorithm that encrypts or decrypts the information (Smith & Eloff, 1999). The same key works for both encryption and decryption in the symmetric approach (Smith & Eloff, 1999). This can be beneficial and dangerous at the same time. The technician must protect the key for the approach to work. People can steal transmitted information, but unless they have the key they will not be able to decode the encrypted file and see the original information (Smith & Eloff, 1999). The asymmetrical way of encrypting is a little bit different. In the asymmetric approach each person involved in secure messaging has a set of two unique keys (Smith & Eloff, 1999). One of the keys (public key) in the pair is made public, but the other key (private key) is kept absolutely private" (Smith & Eloff, 1999, p.44).

Along with encrypting data there are a number of other ways to keep both the patient data safe and to keep the health care providers safe from leaking information. Some of these solutions would seem to be common sense. The first is simply to limit the access that people have to such information. One can achieve this using a variety of methods. Some of the methods are using passwords, biometrics, smart cards and the use of firewalls within a network (Smith & Eloff, 1999).

Passwords might be the simplest approach. Passwords can work well if used correctly. A strong password is unrecognizable to anyone except its owner (Fordham,

2008). The more complex the password, the better because this makes the password harder to guess. Strong passwords combine a mixture of letters, numbers, and special characters or punctuation (Fordham, 2008). Passwords should not be something like a favorite pet, birthday, or the street that you live on (Fordham, 2008). A password must be unique, so using the same password for multiple accounts decreases the strength of the password (Fordham, 2008). Bad or weak passwords can compromise the integrity and security of a system.

The problem with passwords and Personal Identification Numbers (PINs) in health care is that physicians need to be mobile. Doctors need to access data from different terminals at different locations. The nature of the tasks that doctors and medical staff perform requires them to have mobility and access to multiple terminals within their organization (Zuniga & Susilo, 2009). They may even need remote access if they are using a web based clinic type site (Zuniga & Susilo, 2009).

Smart cards are another option that some health care organizations might consider using to protect data. Smart cards are a physical card that is usually associated with a PIN. One might be able to tell the problem with using this type of security already. Smart cards present many disadvantages including deterioration, accidental loss, and forgotten PINs (Zuniga & Susilo, 2009). In addition if any of these events happen another card must be issued which is costly and time consuming (Zuniga & Susilo, 2009). Many people write down their passwords and PINs and put them on a sticky note on their desk of computer monitor, by doing this the owner of the computer is giving anyone that sits at their computer access to their protected information. . This is one of the unsolvable security problems.

It can also be very costly to use a password, or smart card. The Gartner group estimates that password maintenance costs around two-hundred dollars per user per year (Gates, 2007). This cost can be reduced drastically by using biometrics authentication technology, especially the cost related reissuing of forgotten access credentials such as PIN and passwords (Gates, 2007, Zuniga & Susilo, 2009).The only way to try and deter this type of problem is through the use of biometrics.

Biometrics is something that has become more popular recently. Biometrics make it so that people do not need a password or a PIN to access data instead it uses what cannot be duplicated and that is features that are unique to an individual.

> "Unlike the usual identification methods centered on what the person has (card, token, key) or what the person knows (password, PIN), biometrics allows the identification of an individual based on who the person is. Biometric recognition is based on pattern-recognition technique that distinguishes a person based on a feature vector which is derived from physiologic or behavioral characteristics such as fingerprint, face, retina, gait, odor, hand geometry, iris, palm print, or voice. Nowadays, biometric is used as a method for identification or confirmation of a person's identity" (Zuniga & Susilo, 2009, p.975).

This is relatively new technology but the health care field is slowly implementing the use of it to protect data. In the health care field doctors use biometrics as a method for securing and restricting access to facilities, protecting private patient information, and reducing fraud in health care facilities (Zuniga & Susilo, 2009). Biometrics is a great way to create access barriers among users because it is almost impossible to fake a retinal scan

or a fingerprint. This makes it so that only the people who are supposed to have access can see people's personal patient data.

While it would seem that biometrics would save on costs considering the cost of password maintenance and the replacing of lost or stolen smart cards biometrics is not without its downfalls. It is possible to trick a biometric system into providing unauthorized access. It also can be very costly to implement and maintain as well. "On the other hand, the high level of initial investment required in the implementation of biometric is a downsized in the implementation of this technology" (Reynolds, 2004; Zuniga & Suslio, 2009, p. 978). For example, fingerprint scanners vary between $200 and $1500 per unit. Also, the integration and maintenance of this technology would also be costly and need to be considered (Zuniga & Susilo, 2009). Many believe that the high startup cost would eventually pay itself off by securing information better and the maintenance being less. Table 1 provides a broad overview of the techniques used to secure data.

Table 1: Data Securing Techniques

Technique	**Example**	**Security Problem**	**Effectiveness**	**Cost**
Password	Polly123	Using easy to guess passwords such as birthday, or pets name	Varies	$
PIN	1234	Easy to guess, people share PINs and often write them down	High (if done correctly)	$
Smart Card	ID Badge	Theft, deterioration, and misplacement	High (if done correctly)	$$
Biometrics	Retina Scan	Almost none, however biometric measures are costly	Very High	$$$

Implementation Success and Failure: Lessons Learned

Because of incentives for physicians, along with a push from government officials including President Barack Obama, health care organizations are increasingly implementing more EMR systems. Some health care organizations have had some success but very few have been able to implement a fully integrated EMR system. One such success story takes place in California. Long Beach Memorial which is part of MemorialCare Medical Centers is one of the few hospitals with a fully integrated EMR system (Leo, 2009). Like all other health care organizations Long Beach Memorial had to deal with the same challenges and concerns such as cost, and resistance of employees (Leo, 2009). Dr. James Leo, associate chief medical officer at Long Beach Memorial, states that no matter how large or small the organization it is important to take the time necessary to create a system that will meet ones needs (Leo, 2009). Long Beach Memorial was lucky because Leo notes they had a relatively smooth transition, and a high acceptance rate among the physicians (Leo, 2009). Several strategies were critical to the success of their EMR system.

Taking time to determine the needs of a system for ones organization was very important. The search for a vendor started in 2003 for Long Beach Memorial (Leo, 2009). They were able to slowly narrow their choices to a final three based on their criteria of compatibility with current IT systems and cost effectiveness (Leo, 2009) Next they had each finalist come to their site for a week-long visit to demonstrate their product (Leo, 2009). Making sure that choosing the right vendor for ones needs is a critical phase of implementation. One strategy that helped in the success was involving the staff of the hospital in this phase (Leo, 2009). They were able to show the vendor the types of activities they would need to use. They also were able to provide feedback on how to

better the system to fit their needs (Leo, 2009). Finally, after almost a year of research and evaluation Long Beach Memorial selected Epic Systems to be their vendor (Leo, 2009). Taking their time was an element they consider integral in the success of their EMR system (Leo, 2009).

Training is another area where their implementation was a success. Even in a technological era there are still people who do not have a firm understanding of technology or they do not grasp the computer skills needed to implement such a system (Leo, 2009). The vendor, Epic Systems, provided training and as a result "the percentage of physicians now utilizing computerized physician order entry [CPOE) at MemorialCare increased to nearly 75 percent within the first 48 to 72 hours of 'go-live'" (Leo, 2009, p.17). Since then, other physicians who were unsure at first were now embracing the new system and its capabilities (Leo, 2009). In addition, Long Beach Memorial has also designated and trained 400 additional staff to be "super users" (Leo, 2009). These staff completed a more expansive training from Epic Systems (Leo, 2009). The purpose was so that in the future when people have questions or need assistance they can approach one of these super users for help (Leo, 2009). This also helps cut back on the cost of additional technical support (Leo, 2009).

Security is another area that they greatly improved. "Long Beach Memorial has invested in security features to make electronic patient information more secure and private so only those authorized can access a patient's medical record" (Leo, 2009, p.17). In addition to limiting access in order to better protect patient data they also implemented a new level of security. This additional measure requires users to state why he or she

needs to access this data (Leo, 2009). It also alerts additional staff that people are viewing these records in order to keep track of who is viewing this information (Leo, 2009).

The way that Long Beach Memorial implemented their "go live" date was the final element of success. They used a 'rip and replace' approach where they switched their records from paper to electronic records all at once (Leo, 2009). They also did their major change in the middle of the night so they did not affect their daily business hours (Leo, 2009). With all of the changes that made this successful they have see many benefits. "Leo cites several benefits to EMR adoption, including a reduction in operating costs and an increase in efficiency and productivity among hospital staff" (Leo, 2009, p.17). For most medical organizations the biggest benefit is an improvement in patient safety (Leo, 2009).

Failure

Although many will have success when implementing EMR systems a large percentage will also fail. Patti Renner, a professional marketing copyrighter, states that "roughly 73% of all EMR implementations fail" (Renner, 2009, p.3). There are a number of reasons why EMR implementations fail. AC Group CEO Mark Anderson has identified many issues linked with the failure of EMR implementations (Renner, 2009). Software issues are a major source of failure. There are many options out there ranging from simple word-document styles to advanced applications with advanced prompts, system alerts, and are fully customizable (Renner, 2009). Also, much of the software is not certified which is required if attempting to get health care stimulus money (Renner, 2009).

Slow documentation often makes implementation difficult. When implementing a new system there are certain tasks that are going to take longer than before. There will always be a learning curve (Renner, 2009). Anderson "believes that some EMR systems can take physicians up to nine times longer to document a patient visit when compared to dictation or hand-written charts" (Renner, 2009, p.5) A study done by the Medical Group Management Association (MGMA) showed a decrease in physician productivity of around 15% during the first year of implementation (Renner, 2009). Initially EMR systems can take longer than paper records and written charts (Renner, 2009). Often physicians get discouraged and give up using the EMR because they believe they can do it faster the other way (Renner, 2009). "According to Anderson, when a doctor is frustrated or slowed down by an EMR system, there is a good likelihood that he or she will simply stop using it (Renner, 2009, p.5). This will end up wasting thousands of dollars invested in the system and will cause physicians to miss out on potential gains in efficiency in the future (Renner, 2009).

Bad vendors are another reason to do a good job picking for one's system. There are approximately 400 EMR vendors currently doing business (Renner, 2009). Of those almost 50 go out of business every year (Renner, 2009). When a system has problems or an error messages appears in ones system there is a major problem (Renner, 2009). If there is no one to support the system then often times it is abandoned completely (Renner, 2009). It is essential to pick a vendor that is reputable and has a good track record of provided support (Renner, 2009). Some even compare such implementation to childbirth (Renner, 2009). There are going to be pains and problems but the end result will be state of the art and efficient (Renner, 2009).

First year pains are a major reason implementations often fail. Transitioning is not an easy task and will not happen overnight (Renner, 2009). Ebrahim Randeree conducted a case analysis in which he compared three health care practices (case 1, case 2 and case 3) to determine their success or failure. While each of these is a work in progress, none of them were able to successfully implement a fully integrated EMR system (Randeree, 2007). Case 3 provides a good example of the problems that can arise during implementation. Case 3 is a practice consisting of three physicians, one physician's assistant, two nurse practitioners, twenty-four office staff and three locations (Randeree, 2007). After the attempted implementation of their EMR system many problems have surfaced. So far only the new patient's records are in the EMR system. They are running two different systems for the past two years or operation. They have a paper system and a wireless EMR (Randeree, 2007). They are not yet paperless, and have numerous redundant work flows because of the two systems (Randeree, 2007). They have numerous vendor issues and have issues staffing because of the time that it takes to train the staff (Randeree, 2007). In addition, records have been lost, and wireless security issues have led to attacks from their web interface (Randeree, 2007). This case is a failure because of the lack of an integrated system, and the failure to address key issues that will lead the system to success.

Administrators can learn a great deal from the organizations that have succeeded and failed while trying to implement EMR systems. The successful cases took their time in the planning phase and made sure that they chose a vendor who truly fit their needs. They made sure that their security was acceptable in order not to lose, or misplace

records. Training was probably the most important factor. Success was often dependent on the fact that all staff received adequate training (Leo, 2009).

The ones who failed often did not meet these criteria. They were often hasty when choosing a vendor by thinking that "one size fits all". They also rarely provided good training. Security is often a problem because they are not prepared to implement such a system. The lessons that can be taken from these individual cases are: 1.) Be patient 2.) Choose a vendor that suits you 3.) Train all employees, and 4). Security is a must.

EMR Implementation Recommendations

It is evident there are a number of factors that can have an effect on the success of an EMR system. Health care providers must consider each factor carefully in order to implement a system that works and does not waste money. Many health care organizations have implemented ERM systems or some variation of one. They have all had various experiences and all give different advice as to how to improve upon what they have done.

In order to have a successful EMR implementation administrators should do the following. First, it is important to be patient. It might seem attractive to implement a system quickly because of the positive outcomes that such a system can promise. It is important to do a thorough investigation of what each specific organizations needs are before choosing to implement an EMR system. Second, it is crucial that a vendor is chosen that suits the needs of the organization. Not all health care organizations are the same and therefore they will have different needs from the EMR system. Some organizations might focus more on data entry where others such as a pharmacy need to do more prescription tracking. Third, training of employees is vital. Employees need to

be on board with the change and they need to be trained in a manner where they feel comfortable and at ease with the transition. Training also ensures that fewer mistakes are made which saves money. Finally, security is a must. Any system that is using sensitive health care information needs to be properly secured. Money should be spent on security because it will cost far less to secure a system than it will if information falls into the wrong hands. If these steps are followed the implementation of an EMR system should face fewer problems and have greater success.

CHAPTER 4
CONCLUSION

In a day and age when everyone relies on electronic devices it is important to understand that there are benefits and challenges associated with any type of new technology. The field of health care will not exclude EMRs and Healthcare Information Systems from such a group. Along with the implementation of many new technologies is also the collection of data from everyone on a daily basis. The days of paper records and personalized doctor visits are behind us. Even ones favorite clothing store and grocery store have some sort of information about you and your purchase activities (Collett, 2004). Retail businesses are trying to go back to the ways of older days when the owner of the grocery store knew everyone by first name and knew their buying habits (Collett, 2004). So essentially, when you enter a store they will already know what you are going to buy based on past purchases. Much like retail, the health care industry is trying to improve their systems worldwide by implementing EMR systems that store patient data. With the storing of data in massive online databases there are many challenges associated with such activities.

When collecting personal information the challenges only grow. People do not want to have their Social Security numbers floating around the internet. With identity theft almost a common day occurrence one can see why it is so important to keep people's personal and medical data secure. "According to the Federal Trade Commission, medical identity theft accounts for 3 percent of identity theft crimes, or 249,000 of the estimated 8.3 million people who had their identities stolen in 2005" (AHIMA, 2008). There are a number of things to implement including network security, passwords, ID cards, and even biometric procedures. Other challenges include cost, organizational

culture, and professional concerns. Along with the many challenges such a system faces there are also numerous benefits such as speed, quality, and completeness of care (Funke, 2008).

Affordable health care is a subject that has been at the forefront of American policy for years. It was started decades ago and just recently was brought to focus. EMR systems can make affordable health care possible by making health care more efficient, accurate and in the long run actually decreasing cost by eliminating the need for repetitive labor such as data entry (Funke, 2008). Patients do not see many of the important administrative benefits (Miller & Sim, 2004). However, these benefits make the lives of the physicians easier. Therefore, this makes the patient care better. Some of these benefits include viewing capabilities, communication benefits, billing capabilities, and a more patient directed system using websites to health care organizations benefit (Miller & Sim, 2004).

There are current incentives for hospitals and clinics to implement these new systems. Currently only a small percentage of hospitals and clinics have actually implemented full scale or basic EMR systems. However, "The U.S. Congressional Budget Office (CBO) estimates these incentives will persuade nearly 90 percent of U.S. physicians to use EMRs over the next 10 years" (Leo, 2009, p.16). Implementing EMR will take time and will face adversity. However, these new systems will revolutionize the way that the health care business operates.

REFERENCES

AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft."*Journal of AHIMA* 79, no.7 (July 2008): 63-69.

Anderson, J.G. (2007). Social, ethical and legal barriers to E-health. *International journal of medical informatics,* 76, 480-483.

Bagent v Blessing Care Corporation, 4-05-0495 (5th Appellate 2006)

Brooks, R., & Grotz, C. (2010). Implementation of electronic medical records: how healthcare providers are managing the challenges of going digital. *Journal of Business & Economic Research*, *8*(6), 73-84.

Brown, M. H. (2009, March 23). Computerized records giving doctors new tool. But some fear loss of privacy with U.S. Health Information Network. Retrieved June 8, 2009, from www.chicagotribune.com/news/health

California Healthcare Foundation. (2010). New National Survey Finds Personal Health Records Motivate Consumers to Improve Their Health [Press Release]. Retrieved from http://www.chcf.org/media/press-releases/2010/new-national-survey-finds-personal-health-records-motivate-consumers-to-improve-their-health

Collett, S. (2004). Turning data into dollars.*Computerworld*, *38*(38), 36-37.

Computer Economics. (2007). Computer economics report. *Computer Economics*, *29*(4), 1-5

EHR Scope, . (2009, May 7). *Virginia public health organization reports emr security breach*. Retrieved from http://www.ehrscope.com/virginia-public-health-organization-reports-emr-security-breach

EMR Experts. (2010) EMR ROI (Return on Investment). Retrieved from http://www.emrexperts.com/emr-roi/index.php

Fordham, D. (2008). How strong are your passwords?.*Strategic Finance*, 42-47.

Funke, O. Environmental Protection Agency, Association for Politics and the Life Sciences Biopolicy Panel. (2008). *Electronic medical records and privacy: purpose, benefits and problems.*

Furillo, A. (2008, April 8). Governor addresses ucla medical leaks. *The Sacramento Bee*,

Gates, M. A., Biometrics—passing on using passwords. Radiol. Today. 8 (17)28–31, 2007.

Greenemeier, L. (2005, October 31). You know these security threats--you hired them. *InformationWeek*,

Hill, D. (2009, October 26). Phases of an EHR Implementation: Steps to Building Success [Web log comment]. Retrieved from http://blog.pchealthstop.com/?p=68. (2011, April 20).

International Medical Informatics Association (2011). About IMIA. Retrieved from http://www.imia.org.

Joch, A. (2008). Broadband flows to rural cities. *Government Health IT,* 3(5), 16.

Leo, J. (2009). One hospital that got it right. *Health Management Technology,* 14-17

Maria, M., & Paul, S. (2009). Legislative issues in the processing of sensitive personal data in the electronic patient record. *Health Science Journal,* 3(3), 139-148.

Miller R.H., & Sim, I. (2004). Physicians' use of electronic medical records: barriers and solutions. *Health Affairs,* 23(2), 116-126.

Randeree, E. (2007). Exploring physician adoption of emrs: a multi-case analysis. *Journal of Medical Systems*, *31*(6), 489-496.

Raths, D. (2008, May). Stay out of my emr. *Healthcare Informatics*,

Rauhofer, J. (2008). Privacy is dead, get over it! Information privacy and the dream of a risk-free society. *Information and Communications Technology Law,* 17(3), 185-197.

Renner, P. (2009). *Why Most EMR Implementations Fail: How to Protect Your Practice and Enjoy Successful Implementation* [White paper]. Retrieved from http://www.streamlinemd.com/Data/Sites/58/assets/StreamlineMD_WhitePaper_1B.pdf

Reynolds, P., The keys to identity: as healthcare organizations strive for greater security, some are using a very personal approach in the form of biometrics.(Security/Authentication) (Cover Story). Health Management. Technol. 25(12):12(14), 2004.

Rudloff, R., & Jabouri, J. (1999). Preparing for electronic medical records legislation. *Information Systems Security*, *8*(1), 33-38.

Smith, E., & Eloff, J.H.P. (1998). Security in health-care information systems- current trends. *International Journal of Medical Informatics,54, 39-54.*

Simmons, R.A., (2009). Letters to the Editor. *Podiatry Management*, 10.

Social Security Administration. (2011, February 09). *The privacy act and the freedom of information act*. Retrieved from http://www.socialsecurity.gov/privacyact.htm

Terry, K. (2008). Technology: emr success in 8 easy steps. *Physicians Practice*, *18*(13), 1-3.

Vinson, R.K., Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan. (2008). E-Health: Electronic records and e-discovery in the digial age. *ABA Health eSource, 5(1).*

Waxer, C. (2007, April 12). *The top 5 internal security threats*. Retrieved from http://www.itsecurity.com/features/the-top-5-internal-security-threats-041207/

Wen, J., & Tarn, M. (2001). Privacy and security in e-healthcare information management. *Security Management Practices*, 19-34.

Wolfe, M. (2007) Facing down security threats. *New York Law Journal.*

Zungia, A., Win, K.T., and Susilo, W. (2010) Biometrics for electronic health records. *Journal of Medical Systems,* 34, 975-983.

VITA

Graduate School
Southern Illinois University

Ryne M. Grotts Date of Birth: March 29, 1986

912 Tippit Street Apt. 6 , Carterville, Illinois, 62918

350 Oak Grove Road, Makanda, Illinois, 62958

rygrotts@gmail.com

Southern Illinois University Carbondale
Bachelor of Science, Information Systems and Applied Technologies, 2009

Research Paper Title:
Implementing Electronic Medical Record Systems: Privacy vs. Security

Major Professor: John Hamman