Health IT Security: An Examination of Modern Challenges in Maintaining HIPAA and HITECH Compliance

Andrew S. Miller
University of North Georgia, asmill0296@ung.edu

Bryson R. Payne
University of North Georgia, bryson.payne@ung.edu

Abstract
This work describes an undergraduate honors research project into some of the challenges modern healthcare providers face in maintaining compliance with the Health Insurance Portability and Accountability Act (HIPAA) and HITECH (Health Information Technology for Economic and Clinical Health) Act. An overview of the pertinent sections of both the HIPAA and HITECH Acts regarding health information security is provided, along with a discussion of traditionally weak points in information security, including: people susceptible to social engineering, software that is not or cannot be regularly updated, and targeted attacks (including advanced persistent threats, or APTs). Further, the paper examines potential violations of HIPAA involving vulnerabilities in commonly-used enterprise health records systems. Finally, we compare these challenges to the challenges of the United States healthcare system prior to 1995, specifically looking at information handling procedures, how procedures have changed, and how effective those changes have been.

Disciplines
Health and Medical Administration | Health Information Technology | Health Law and Policy | Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Technology's use in the developed world has increased exponentially since the Industrial Revolution, especially so in health care. An early example of this technology is the ophthalmoscope, which was invented in the 1840s and subsequently improved (Lusby, 2015). The ophthalmoscope is used to assist medical professionals in performing eye examinations, and is notable for the innovative use of magnification through mirrors to give medical professionals a clear and enlarged view of the eye.

Shortly after the invention of the ophthalmoscope, numerous other advances came along, including: the x-ray, the stethoscope, the laryngoscope, and many other technological instruments (Loudon, 1997). These instruments empowered medical professionals to become better equipped to perform their job, all the while decreasing the need for smaller exploratory surgeries through medical imaging.

Shortly after the Second World War, computer information systems were introduced to the healthcare field. This allowed for past medical history to be accessed through a terminal and later a computer at speeds previously not possible with paper files. An first attempt to standardize the exchange of this information and to make it easily interchangeable among healthcare providers within a state was made by the Massachusetts General Hospital in 1966 (Snell, 2016). This effort led to the production of the programming language MUMPS (Massachusetts General Hospital Utility Multi-Programming System). MUMPS is still widely used in modern health information systems, including EPIC Systems (Moukheiber, 2013), GE Healthcare (Ibanez. 2012), Quest Diagnostics (Vorhies. 2016), and many others.

HEALTH IT SECURITY BACKGROUND

While each advance in technology brought its own challenges, all of these advances served an important purpose: to advance science and improve healthcare. However, it became apparent that with the growing role of healthcare information technology in the United States, that there was significant information being collected by such technological systems. This information was subject to potential abuse or mishandling from healthcare workers, as well as being compromised by malicious hackers. Further, before 1996, the United States federal government possessed little power in terms of healthcare regulations (Trinckes, 2013), leaving the vast majority of the power to individual states in terms of governance of standards.

HIPAA

In addition to potentially causing misunderstandings with proper information handling from out-of-state or travelling health professionals, the lack of uniform health data governance led to issues with insurance policy differences between states, medical coding differences, fraud, and many other issues. These differences in governance led to increased healthcare costs, increased health insurance cost, and may have contributed to sensitive patient information being disclosed improperly by first and third parties due to the lack of unifying, national privacy set of laws (Trinckes, 2013).

The United States Congress set out to address the lack of uniform health information data handling standards. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed to address these concerns (Trinckes, 2013). In addition to establishing clear standards for the conditions of health data disclosure by healthcare providers, it also established standards for: information security, privacy, fraud prevention, electronic data exchange, healthcare access, revenue, and insurance standards (Sullivan, 2004).

The HITECH Act

In the decade after HIPAA was passed, there was a growth in healthcare demand, caused by an aging population, an increase in population size, and other factors (Howden and Meyer, 2011). This placed a strain on the capacity of health environments to accurately keep track of the patient data, and to have a way to securely transmit and disclose the information. In addition, there was a recession that began in the United States in 2007 (IMF, 2009) that severely limited the budget of many healthcare providers, leading to hiring freezes, discretionary spending cuts, customers unable to pay their bills, and reduced spatial expansion (AAFP, 2009).

The United States congressional bodies recognized the challenged caused by the increased demand and shrinking budgets, and set out to have hearings about it. These hearings featured many differing viewpoints from medical and IT professionals (CEC, 2010).

Despite the differences of opinion expressed at the HITECH Act's hearing, there was a general consensus that further health information reform was needed. In contrast to the previous HIPAA guidelines, which did not mandate electronic records in most instances, the HITECH Act set a deadline of 2015 before penalties would be imposed upon health providers who were not compliant with electronic record requirements (Dark and Andrews, 2012). The lawmakers realized this endeavor would cost the health field a significant amount of money, so they included grants to offset the cost of migrating to an enterprise health records system. This added the HITECH Act to the American Reinvestment and Recovery Act of 2009 (ARRA), as this provided an unprecedented amount of funding to assist eligible providers in funding the initiatives set forth in the HITECH Act.

Additionally, the HITECH Act set relatively strict guidelines for the data handling, insisting that the data be used meaningfully by eligible providers (Dark and Andrews, 2012). This allowed struggling facilities to employ cost savings that are associated with storing records electronically.

Brief Data Security Background

Prior to widespread electronic health record usage, most breaches of information and trust in the healthcare environment occurred on a small scale through more primitive attack methods. These methods included methods that primarily relied on abusing human trust, such as social engineering, shoulder surfing, using misplaced documents, and breaking into record rooms (Gostin and Turek-Brezina, 1995).

The most common method used by attackers to gain sensitive medical information prior to the passage of HIPAA was social engineering. There were many ways this took place. For example, if there was a high profile local figure in a health environment, a media employee or contractor may attempt to gain information about the figure by going to the health environment they are in and posing as a grieving family member. The employee would then ask for as much information as they were able to, and given the lack of established protocol, they were often able to get the room number the figure was in, the condition for which they were actively being treated, and their medical history. With this information, the media employee now is able to publish the information before other agencies, bringing fame and curious viewers to their media entity.

With the passage of HIPAA, patients have a right to know the directory information that will be provided to guests of the facility, as well as redact the information in a fashion the patient sees fit, which would have prevented the above hypothetical situation from transpiring (HHS, 2003).

Shoulder-surfing and eavesdropping techniques were also frequently used in the healthcare environment prior to the passage of HIPAA (Covvey and McAlister, 1980). To shoulder-surf, an individual would stand near a medical professional, and look over their shoulder to view patient information, including: medical records, social security numbers, insurance and financial information, and other classified information. Similarly, an eavesdropper would be within earshot of departments where patient data is collected or dispersed, such as registration, the emergency department, or billing.

To counteract this potential for sensitive information to be compromised, HIPAA mandates that privacy be maintained through necessary measures, including privacy screens where needed, and not having boards such as the emergency department's patient triage board visible to people other than those with an immediate connection to the department (HHS, 2003).

Prior to the passage of HIPAA, health record storage practices were not standardized across the United States. It was not uncommon in many health environments to have a patient's medical records sitting on a counter beside registration, containing the patient's: social security number, street address, phone number, marital status, insurance information, billing information, medical history, and other sensitive information (Irvine, 1994). This was taken advantage of by individuals of nefarious intent, including: identity thieves, insurance fraudsters, sexual predators, house robbers, and other criminals.

MODERN THREATS

While the modern healthcare providers face new and challenging problems each day, such as drug-resistant bacteria, emerging diseases, legal and compliance changes, and so on, the information security departments that work with these facilities face new threats every day as well, which can have potentially devastating effects, as well. Health information has been reported to be worth 10 to 20 times as much on the Dark Web as credit card numbers (Humer and Finkle, 2014).

One such risk could be a terrorist threat involving placing a payload on the interface engine that is used to transform the data sent between departments. The interface engine is usually found in larger hospitals, and is an internal device that is responsible for allowing communication of Health Level 7 data between appropriate electronic medical record systems. The interface engine is not needed in smaller facilities, as they often use a single electronic medical record system to store patient information, as opposed to a network of electronic medical record systems that different departments use.

However, attacks on hospital IT infrastructure could occur on any system, and is not limited to critical systems such as the hospital's interface engine. Further, attacks can have any motive, and is not limited by any factor whatsoever. This is why the securing of every single system that is connected in any way to the healthcare facilities network is crucial to ensuring that all patients get the timely and professional care from the healthcare workers.

Recent ransomware attacks have shut down computers connected to critical health systems in a number of hospitals in the US and Canada, demanding ransom in the tens of thousands of dollars to restore access to patient files, storage, and computer systems (Finkle, 2016). Advanced persistent threats (APT's) from unfriendly nation-states and organized criminal organizations are also an ongoing concern for healthcare information providers.

Securing all aspects of computer systems and networks, including network devices not traditionally considered computers, remains key. In the Target data breach in which over 40,000,000 credit card numbers were compromised, it was discovered that the hackers had entered the network through a computer that was running a Linux distribution (Krebs, 2015). The computer was installed by the HVAC company, and the company left all passwords at their default values. The company was allowed by Target to have the system open for remote access to monitor and control the HVAC system as needed. The system was in no way segregated from the internal Target network, despite Target's internal information security team being aware of all of this.

Hospitals use HVAC, surveillance, and other network-connected systems, too, and such a device can be the breach that costs over $10,000,000 in direct damages, and possibly billions in indirect damages in Target's case, when costs such as issuing new cards, refunding fraudulent purchases, loss of consumer confidence, etc. are accounted for (Krebs, 2015).

To further complicate matters, Microsoft has recently estimated that 17.9% of online systems will come in contact with malware in 2016 (Microsoft, 2016), and Symantec has over 4.1 Million (Symantec, 2016) individual virus signatures in its virus definitions as of August, 2016. For the healthcare industry, this can be everything from slowing a computer in the registration office, to stopping the operation of the life support machines in the critical condition facilities.

For example, an employee in the registration department may have visited a site that was recently compromised by malware, or may even have visited a honeypot of a common misspelling of legitimate website, and downloaded and installed a keylogging application on a production registration computer. Assuming the keylogger operates at startup, has the appropriate permissions provided it, is not detected by the antivirus program(s) employed by the facility, and is available to all users of the computer, the employee and others then input their usernames and passwords into the various programs that they use to record registration, billing, and other information about the patients, which is recorded by the keylogger. Additionally, any information typed by the employee using the infected machine is subject to this recording, including: patient's full names, phone numbers, dates of birth, social security numbers, medical history, insurance information, etc. With this valuable information, the hacker can either use the information themselves, or more commonly can sell this information on black market exchanges in exchange for bitcoins, or any other currency medium that is not easily tracked.

However, information is not the only resource that healthcare facilities have. Almost every healthcare facility in the developed world has a powerful, high-speed network and many powerful nodes on it. An attacker may want to use some of this potential to perform nefarious acts, such as distribute illegal content, perform distributed denial of service attacks on websites, send spam email, etc. utilizing these resources. The attacker may then add certain nodes on the facility's network to a botnet, which is a collection of computer that work together to accomplish goals set by a central authority, which is usually a hacker.

Luckily, botnets at current tend to produce traffic patterns that are easily recognizable by commercial firewalls that are almost certainly deployed by a facility of any size, and this attack medium would not generally be successful in the long term for that reason (Cisco, 2016). However, in smaller facilities, this is a real threat that may overtake the network and all machines if not properly monitored and prevented.

Apart from this, there are countless other types of malware attacks capable of wreaking havoc on networks in healthcare environments in ways similar to the described attacks, such as viruses, worms, Trojan horses, etc. To remain in compliance with the HITECH Act and to maintain information security and integrity as outlined in HIPAA, it is extremely important that all healthcare facilities place great emphasis on safeguarding all aspects of data, which requires a constant and conscientious effort by all employees, contractors, and associates of the facility to achieve (HHS, 2015).

HEALTH IT CYBER ATTACK PROOF OF CONCEPT

In reality, it is relatively easy for a dedicated hacker to access and take control of aspects of a network. Tools are widely available on the internet to aid in this task, as well as to demonstrate where the vulnerabilities are in implementations of employed solutions, such as network, system, software, etc. Additionally, there are a growing number of websites and videos online that teach prospective hackers how to best utilize the available tools, many of which are available without payment for personal use.

At this point, it is important to emphasize that these tools can be used by "black hat hackers" or "white hat hackers." The main difference between the black and white hats is the motive; white hat hackers generally are doing penetration testing that they are directly authorized to do, usually to test the safeguards and defenses of a system or systems (Hafele, 2004). Black hat hackers are generally motivated by another factor, such as stealing property, vandalism, fame, terrorism, or other criminal motives.

However, white hat and black hats also generally act differently in how they react to compromising. A white hat may get in and plant a "dummy payload," which proves that penetration is possible without disrupting actual operations, whereas a black hat may plant a malicious payload, which not only proves that penetration is possible, but then disrupts operation and allows the hacker a large amount of control over the network.

One of the most popular tools available for this purpose is Kali Linux. Kali is a freely available Linux distribution based on Debian. Kali Linux has been downloaded over 1,000,000 times (Aharoni, 2015), and is used extensively by both white and black hat hackers.

One of the things that Kali prides itself on is being relatively easy to use. Compared to other solutions, Kali is free to download, and will run on most x86 machines made in recent years. In addition, Kali is loaded with a plethora of utilities that are usable right after installation, that allow everything from password cracking, to network scanning, to social engineering attacks.

To demonstrate this, all that is needed is a bootable Kali flashdrive and a computer capable of running 64-bit software. This flashdrive is easily made by first downloading the latest Kali Linux *ISO* file from a reputable distributor, and verifying the SHA checksum of the file with the provided information on the Kali Linux downloads page (Hertzog, 2016). The purpose of verifying the SHA sum of the download is to ensure that the *ISO* file has not been compromised by either corrupted files or man-in-the-middle attacks, and can be done using a variety of programs on modern operating systems. Once the file has been downloaded and verified for integrity, it simply needs to be copied to a freshly formatted flashdrive using either a terminal command such as "dd" or an application capable of copying *ISO* images to external media that allows them to be bootable devices.

Once the bootable device has been made, it simply needs to be inserted into the appropriate port of the computer, and selected in the device boot options upon startup of the computer. Depending on how permanent the hacker wishes the installation to be, they will either select the option for live boot, in which the operating system will be loaded on the memory of the computer in a temporary fashion, or the installation option, in which Kali's system files are transferred and installed on the computer's hard drive.

With Kali running, the hacker will do a series of things, but for this example we will open the Metasploit program in Kali Linux for the first time. Metasploit will open a terminal window in which the program is initialized and loaded, as well as the database of exploits it contains. Once Metasploit is fully loaded, in this example, the hacker types "Armitage" and hits the enter key. Armitage, which a powerful graphical user interface that allows novice hackers to use Metasploit with ease, will then load. From this point, the hacker will either import a previously scanned nmap scan using the import hosts option, or perform an nmap scan from the Armitage window. Nmap scans are used to determine what devices are on a specified IP address or range of addresses, as well as which ports are open and services are running on said devices.

With the hosts imported, the hacker will then select the option to find attacks. This will test each exploit in the database to see if it is able to run, and is highly dependent upon the updates run on the system, the open ports, the antivirus program, the firewall, and the packages installed. From there, the hacker will simply right click on the machine in the Armitage window, select an exploit, and run it. It will either allow the hacker in or not, and if it does not, the hacker simply tries another exploit until they gain access. Once they have access, they can do a variety of things, depending upon the type of machine, but will typically monitor the network internally, create administrator accounts, install spyware, etc.

It is important to note that in the previous example, the hacker already had the IP address of the machine that they wished to access. This is not always the case when hacking, however, it is generally not difficult to locate the IP address of a network. For example, an attacker could get a public address of the webserver by simply visiting the website of the hospital. Social engineering could be used on any employee in the building by simply calling, asking to speak with a name found in a public directory, asking them to run a command such as ipconfig /all in command prompt, and having them read off the applicable information (McDowell, 2009). In addition, the attacker could simply go to the facility, locate an Ethernet port, connect a machine to it, and then locate the IP address.

It is also important to note that the previous example used very basic steps for hacking, and that it will not always be limited to the above steps. For example, if the attacker wished to change the content on a webserver running Linux and MySQL, they may simply use a program such as Burp Suite in Kali Linux to test for SQL injection vulnerabilities. There are many types of systems in many locations for many purposes, and many ways to compromise them.

SECURITY RESPONSE

Despite the ease that hackers experience when accessing many systems, it is an achievable task to ensure that hackers are not able to access systems without the proper authorization. Although every health organization is unique, the following will prevent most attacks from being successful: **1) keeping all software up-to-date, 2) running an enterprise antivirus on all applicable machines, 3) employing network security including strict network segmentation, 4) educating and training employees on information security risks, 5) encrypting all sensitive file storage and communication with secure algorithms, 6) enforcing a strong password policy, and 7) limiting access via access groups.**

The importance of patching is evidenced by the 2016 Enterprise Security Report that Hewlett Packard recently released. In this report, they determined that 68% of exploits used in 2015 that they analyzed were patched over two years ago (Barsamian, 2016). These old, patched exploits very likely would not have been able to have been used by hackers on the enterprise systems to attack them had their system administration team been adamant about patching software in a timely and responsible fashion.

The same report by Hewlett Packard illustrates the following new malware discovery increases by platform in 2015: Microsoft Windows, 88%; Google Android, 153%; Linux, 212%; Apple iOS, 235%. For this reason, having a strong, enterprise class antivirus program that blocks malware from being loaded on systems is important to the healthcare field, and it is crucial that regular scanning be done to verify that systems remain clean.

The need for strong network security is well-evidenced in the aforementioned example of Target's data breach. Had they not allowed remote access, and segmented their network, the attackers very likely would have been able to recover over 40,000,000 credit card numbers from the corporate network.

For the healthcare environment, given the regulations that employees are expected to be in full compliance with at all times through HIPAA, HITECH, and other legislation, **it is crucial that employees be trained often on information handling principles, such as avoiding phishing scams, social engineering, and malware**. This is accomplished through training and having skilled information security experts available to answer questions at all hours, and will have a varying but generally positive outcome on the information security of enterprise environments (Sanchez, 2011).

Even with the best technological safeguards, it is still possible that a zero-day exploit can allow a hacker unauthorized access to a healthcare system's network. For this reason, it is imperative that sensitive information be encrypted using the best algorithms available, such as the Advanced Encryption Standard. With 256-bit AES, the hacker will not receive files that are easily usable, and will instead need to use advanced hardware for a long time that at this point is not generally feasible for individuals to have (EFF, 1998).

However, even with firewalls and other network security devices fully up-to-date, it would still be relatively easy for a hacker to access the network using a user's insecure or repeated password. For example, it is estimated that approximately 1/3 of users use the same password on every website (Martins, 2014), meaning that if a hacker hacks a site and finds a user's login information, they are then able to use that login information to access the healthcare's network approximately 33% of the time. For this reason, it is generally best to have passwords expire after a set amount of days, such as 90, and to not allow passwords to repeat previous passwords. Additionally, to allow for a much larger pool of possible combinations of characters, it is best to set strong complexity and length requirements, as for each additional character, there can be millions more combinations (Martins, 2014).

One of the most important aspects of maintaining compliance is to do so with meaningful use, and one of the easiest ways to accomplish this is through utilizing role-based access groups by position. Tools such as Microsoft's Active Directory make this task easy, and through Active Directory Federation Services, it is possible to use this information across a multitude of platforms, including keycards and other tokens for accessing restricted areas.

CONCLUSION

Compared to previous record storage methods, digital information is far more susceptible to access without authorization. While it was previously possible to break into the records room in a health facility, it was not easy to do so without detection. It was also not feasible to take an entire hospital's records and hold them hostage, as is possible today with easily deployed ransomware.

However, with a vigilant staff who work together to protect all health-related information, it is an achievable goal to remain in compliance with both the HIPAA and HITECH Acts and prevent most unauthorized use of electronic records, as well as mitigate damages from attacks that do occur.

ACKNOWLEDGMENTS

This research was supported in part by the Center for Undergraduate Research and Creative Activities (CURCA) at the University of North Georgia.

Our thanks to the Honors Program Director, Dr. Steve Smith, and special thanks to University of North Georgia IT InfoSec personnel Cole Edgar and Corey McCown.

REFERENCES

Aharoni, M. (2015, October 15). Kali Moto End of Life & Kali Dojo Slides. Retrieved August 11, 2016, from https://www.kali.org/news/kali-moto-eol/

Ayers, R. U. (1990, April). Technological transformations and long waves. *Technological Forecasting and Social Change, 37*(2), 111-137. http://dx.doi.org/10.1016/0040-1625(90)90065-4

Barsamian, S. (2016). The collateral damage of cybercrime. Retrieved August 12, 2016, from http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2 - Configuring the Botnet Traffic Filter [Cisco ASA 5500-X Series Firewalls]. (n.d.). Retrieved August 12, 2016, from http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_botnet.html

Covvey, H. D., & McAlister, N. H. (1980, August 9). Computer-assisted medicine: Privacy and security. *Canadian Medical Association Journal, 123*(3), 231st ser. Retrieved June 12, 2016, from http://libproxy.northgeorgia.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=35342362&site=eds-live&scope=site

Cracking DES: Secrets of encryption research, wiretap politics & chip design. (1998). San Francisco, CA: Electronic Frontier Foundation.

Crisis and recovery. (2009). Washington, D.C.: International Monetary Fund.

Dark, J., & Andrews, J. (2012). *CompTIA healthcare IT technician HIT-001 authorized cert guide*. Indianapolis, IN: Pearson.

Gostin, L. O., & Turek-Brezina, J. (1995, January 1). Privacy and security of health information in the emerging health care system. *Health Matrix: Journal of Law-Medicine, 5*(1), 1-36. Retrieved June 12, 2016, from http://eds.a.ebscohost.com/eds/detail/detail?sid=a9f4e96f-93ea-4f5d-9ae3-15a075581d16%40sessionmgr4004&vid=0&hid=4210&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#db=fth&AN=9508234184

Hafele, D. M. (2004, February 23). Three Different Shades of Ethical Hacking: Black, White, and Gray. Retrieved August 12, 2016, from https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390

Hearing Before the Subcommittee on Health of the Committee on Energy and Commerce, 111th Cong., 32 (2010) (testimony of David Blumenthal, Anthony Trenkle, Frank Vozos, Gregory Starnes, Christine Bechtel, Roland Goertz, Matthew Winkleman, Glen Tullman, Peggy Evans).

Hertzog, R. (n.d.). Kali Linux Downloads. Retrieved August 12, 2016, from https://www.kali.org/downloads/

Howden, L. M., & Meyer, J. A. (2011, March). Age and Sex Composition: 2010. *US Government Census Data*, 2. Retrieved June 6, 2016, from http://www.census.gov/prod/cen2010/briefs/c2010br-03.pdf

Ibáñez, L. (2012, February 2). Join the M revolution. Retrieved June 6, 2016, from https://opensource.com/health/12/2/join-m-revolution

Irvine, D. (1994). Confidentiality: Data and permissible disclosure. *Journal Of The Royal Society Of Medicine, 82*(22), 42-43. Retrieved June 12, 2016, from http://libproxy.northgeorgia.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=mnh&AN=8064760&site=eds-live&scope=site

Krebs, B. (2015, September 21). Inside Target Corp., Days After 2013 Breach. Retrieved August 11, 2016, from http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Loudon, I. (1997). *Western Medicine: An Illustrated History*. Oxford: Oxford University Press.

Lusby, F. M. (2015, February 17). Ophthalmoscopy: MedlinePlus Medical Encyclopedia. Retrieved June 5, 2016, from https://www.nlm.nih.gov/medlineplus/ency/article/003881.htm

Martins, F. (2014, May 10). 3 Quick Facts on Why a Strong Password Policy Matters. Retrieved August 12, 2016, from https://blog.digicert.com/3-reasons-for-strong-password-policy/

McDowell, M. (2009, October 22). Avoiding Social Engineering and Phishing Attacks. Retrieved August 11, 2016, from https://www.us-cert.gov/ncas/tips/ST04-014

Microsoft Security Intelligence Report (SIR). (2016, January). Retrieved August 11, 2016, from https://www.microsoft.com/security/sir/default.aspx

National Survey of Family Doctors Shows Recession Takes Startling Toll on Patients. (2009, May 19). Retrieved June 06, 2016, from http://www.aafp.org/media-center/releases-statements/all/2009/nationalsurvey-familydoctors-recession.html

Rodrigues, J. (2010). *Health information systems: Concepts, methodologies, tools and applications*. Hershey PA: Medical Information Science Reference.

Sanchez, M. (2011, May 12). 5 Ways to Educate Employees about Network Security. Retrieved August 12, 2016, from http://blogs.cisco.com/smallbusiness/5-ways-to-educate-employees-about-network-security

Snell, K. (n.d.). About 21st Century Mumps. Retrieved June 5, 2016, from http://www.m21.uk.com/newtom.php

Sullivan, J. M. (2004). *HIPAA: A practical guide to the privacy and security of health data*. Chicago, IL: American Bar Association, Health Law Section.

Symantec. (2016, August 11). August 11, 2016 Rapid Release Definitions - Detections Added. Retrieved August 11, 2016, from https://www.symantec.com/security_response/definitions/rapidrelease/detail.jsp?relid=2016-08-11

Trinckes, J. J. (2013). *The definitive guide to complying with the HIPAA/HITECH privacy and security rules*. Boca Raton, FL: CRC Press.

U.S. Cong. (2003). *Summary of the HIPAA privacy rule HIPAA compliance assistance* [Cong. Bill]. Washington, D.C.: U.S. Dept. of Health and Human Services.

U.S. Dept. of Health and Human Services (2003) (enacted).

U.S. Dept. of Health and Human Services. (2015, December 14). $750,000 HIPAA settlement underscores the need for organization-wide risk analysis. Retrieved August 12, 2016, from http://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html

Vorhies, W. (2016, January 28). MUMPS – The Most Important Database You (Probably) Never Heard Of. Retrieved September 12, 2016, from http://www.datasciencecentral.com/profiles/blogs/mumps-the-most-important-database-you-probably-never-heard-of