Global Information Assurance Certification Paper

Beau Fidler
Version 1.2e

Mobile Medicine

Background

Health care providers have traditionally been excluded from the same privacy standards that the rest of the business world has been subjected to over the years. Credit card companies, insurance agencies, and financial institutions have all been regulated to insure that sensitive client information is not disclosed without proper consent. With the ever-increasing usage of wireless technology, more and more health care providers are beginning to transfer patient communications and medical records via wireless communication devices because they realize it can streamline everyday operations and lower costs. This poses additional security threats to patients because now their confidential medical records are exposed to yet another insecure environment unless the proper security management system and security procedures are successfully implemented to prevent such invasions. Bill Braithwaite, Senior Advisor on Health Information Policy, states, *"Most industries that use information technology pay close attention to the need for security in their systems. They value the information they have and strive to protect it. For many reasons, many of which are incomprehensible, health care has been very lax."* For this reason, the Department of Health and Human Services (DHHS) created a set of rules called the Health Insurance Portability and Accountability Act (HIPAA) to help regulate the use and disclosure of protected health information. Although many perceive the security rules of HIPAA as burdensome and even difficult to implement, they are actually intended to be scalable, cost effective, and representative of industry consensus. The rules do not endorse or specifically state that a covered entity must utilize a particular application or network component. Instead, HIPAA allows each affected entity to assess its own security needs and risks, and then develop, implement, and maintain appropriate security standards based on its business requirements. This gives health care providers more latitude to deploy a customized security management system that meets their environment's needs. With the creation of HIPAA, many health care providers are revising their business models to include a wireless platform in hopes that it will transcend them into the next generation of health care, but not without addressing serious security concerns.

Why Wireless?

It is no secret why more and more health care providers are investing in wireless platforms – increased efficiency, increased productivity, lower costs, reduced errors, and improved patient care. These key driving factors have led health care providers to challenge their everyday practices. From the way physicians collect data to the way they report it, health care providers cannot afford for their physicians to have anything less than real-time access to business critical

data in an accurate and timely manner. Wireless technology gives physicians the flexibility and mobility they need to support their critical decisions. Many health care providers have already begun to incorporate simplistic wireless technology, such as telemetry devices, to help monitor patients' vital signs from a distance. This enables physicians and nurses to monitor several patients at the same time, while still being able to assist others in the interim. This example proves that wireless technology is increasing efficiency and productivity in the health care industry, thus reducing costs for the institution using the equipment because patient monitoring and data entry are totally automated. This ultimately results in more accurate medical records, better service, and lower medical costs for patients. More advanced capabilities of wireless technologies include:

- *Electronic Medical Records (EMRs)* – The online management of patient medical records.
- *Electronic Prescriptions* – The electronic transfer of patient prescriptions directly to local pharmacies.
- *Referencing* – The act of querying pharmaceutical management systems to check drug references, formulations, and side effects.
- *Digital Transcription* – The process of automatically translating and storing a physician's verbal notes in an electronic format.
- *Digital Imaging* – The process of storing X-rays, MRIs, and other medical films in an electronic format.
- *Voice-over-IP* – Direct voice communications with any faculty member in the same facility.

The potential of these wireless technologies to help revolutionize health care is why so many providers are considering investing their futures in them. Health care providers believe these technologies will be the catalysts that will enable them to fight the spiraling costs of health care. While wireless technology does offer a lot of opportunity for the health care industry, many providers are still uncovering the challenges associated with implementing a secured wireless environment.

What is a Secure Environment?

A secure environment is a relative term that information technology specialists across all industries have been debating for years. No one really knows how secure an environment has to be before it is declared SECURE. In most industries, security has been left up to individual organizations to decide how they want to protect their information due to entity-specific variables such as data sensitivity, cost constraints, exposure, customer perceptions, litigation concerns, etc. However, the DHHS has proposed a set of security standards as part of HIPAA to help eliminate this confusion for the health care industry. These security standards offer a basic set of guidelines that will enable providers to efficiently and effectively protect their environments in a reasonable manner. The major areas of concern that the HIPAA security standards address are: administrative procedures, physical safeguards, technical security services and mechanisms,

access controls, and electronic signatures. Together, these areas ensure that health care providers have proper policies and procedures in place to enforce the necessary controls to manage a secure environment. These areas are interdependent, thus an environment is not secure unless all areas are working in harmony. Periodic audits of security processes and controls should be performed to identify any existing security gaps. No environment is 100% secure, but providers should feel much more confident knowing that they have taken the proper measures to reduce the risk of their environment(s) being compromised by complying with the security standards defined by HIPAA.

Wireless Security Concerns

Wireless platforms present a unique set of security concerns that continue to multiply exponentially with each new wireless user and device. Gartner Group estimates that the number of wireless users in the U.S. is expected to soar from 40 million in 2000 to 225 million by 2002. If this forecast is any reflection of the potential growth rate for wireless users in the health care industry, providers must begin developing wireless integration strategies to cope with future demand. Some of the primary security concerns that providers must address when developing a wireless integration strategy include: ownership, scope, compatibility, privacy, and interference.

Physicians and nurses are the early adopters of wireless technology in most health care organizations today because they bring their own personal digital assistants (PDAs) or use free ones provided by pharmaceutical companies and other medical suppliers to increase their efficiency. This creates ownership issues because health care providers have no control over the hardware or software invading their environments. If providers do not have control over their environments, how are they going to comply with the security standards defined by HIPAA? Physicians and nurses are using these devices for work-related tasks such as accessing patient medical records, lab results, prescriptions, and clinical notes. Who is legally responsible if one of these devices is lost or stolen and accessed by an unauthorized user? These types of vulnerabilities create large liabilities for health care providers that employ wireless devices in their environment(s) knowingly or unknowingly.

While wireless technologies used by health care providers are primarily dominated by text, more and more medical personnel are demanding Web, voice, graphical, and audio content. This will enable users to view online digital images and record patient visits, which ultimately changes the scope of the provider's wireless integration strategy. Currently, PDAs have processing, memory, and power constraints that allow them to operate at a fraction of the level of a conventional PC. This means that most physicians and nurses use multiple devices to perform their daily operations based on application requirements. For example, the same physician might use a PDA to transfer an electronic prescription, a laptop to view a client's electronic medical record, and a desktop to view a MRI online all because of hardware constraints. Unfortunately, modern wireless devices are not capable of handling the complexities of the PC, but health care providers should design their integration strategies with these trends in mind.

Another concern surrounding wireless technologies is the degree of compatibility or interoperability, which is the ability of one manufacturer's products to communicate with another's, among competing software and hardware vendors. Many vendors boast that their systems have interoperability capabilities, but in reality there are usually multiple problematic glitches (e.g., formatting) that inhibit modern wireless devices from successfully communicating with other devices. Two of the main reasons are: 1) memory-starved wireless devices can not process data produced by larger systems, and 2) industry protocol standards such as IEEE 802.11b High Rate (HR) are being highly contested by more advanced standards (e.g., Wireless Application Protocol (WAP) and Bluetooth). For many health care providers, most of the data that they want wireless access to (e.g., patient records and patient accounts) resides on legacy systems that currently have no way of reformatting their output in a form or size that is compatible with most wireless technologies. Additionally, more and more protocol standards are entering the market that are offering higher transmission rates and other added benefits that are not compatible with the current industry standard 802.11b. This presents a challenging situation for health care providers because they must fully understand the needs and constraints of their current environment to design a successful wireless integration strategy.

As health care providers decide whether or not to fling protected health information through the air, concerns of how to properly ensure the privacy of this information being transmitted is seriously being reviewed. Many of the wireless communication applications and protocols on the market today have safeguards in place to help prevent such security or privacy breaches from occurring, but none of them provide an end-to-end solution. Wireless security vendors such as IBM, Cisco Systems, RSA Security, and Network Associates are all trying to fill the gap with proprietary solutions, but no industry-wide standard to protect wireless communication currently exists. HIPAA has compounded the privacy issue by requiring stricter standards for access controls, audit trails, de-identification, authorizations, routine and non-routine disclosures, etc. This means that heath care providers trying to design a wireless integration strategy are going to have to work closely with wireless software vendors to ensure that their products have the capabilities to meet certain privacy requirements specific to the provider's needs.

Last but certainly not least is the concern of how wireless technologies are going to coexist with sensitive medical equipment. For example, telemetry devices that track patient vitals currently use wireless communications that are captured by a centralized monitoring system. If these telemetry devices ever encountered any type of interference that would prevent them from accurately tracking patient vitals, there could be serious and even fatal consequences for patients. Additionally, concerns surrounding the unauthorized interception of wireless communications that contain protected health information is a major issue that needs to be addressed. If wireless communications are intercepted, how will senders and receivers be able to accurately detect such breaches? There are many wireless security concerns that health care providers need to evaluate before developing a wireless strategy. However, several organizations have found solutions that have allowed them to dramatically increase value for their personnel and their patients.

Wireless Security Solutions

Once health care providers understand the leading security concerns surrounding wireless technologies, the next step is to decide how health care providers are going to tackle them. It is inevitable that all health care providers are going to have to integrate some form of wireless platform into their environments in the near future because patients and health care personnel are demanding it, and the benefits of wireless technologies far outweigh the costs associated with it.

Many organizations have found that the most secure and cost-effective way to integrate wireless technologies into their environment is through the use of a local area network (LAN). Local area networks have evolved as the platform of choice because costs have dropped and standards are beginning to emerge as technology has matured. The cost of wireless base stations, the bridge between wireless devices and the network, and client devices (e.g., PDA) have significantly decreased over the past 12 months, while memory capacities for client devices have increased. This makes wireless networks more affordable and practical for health care providers to employ. Most wireless network vendors (e.g., Nortel, Cisco, and 3COM) have standardized around the 802.11b wireless communications protocol, which is capable of speeds up to 11 megabits per second (Mbps). Additionally, increasing bandwidth and memory-intensive wireless devices is making it possible for providers to implement more advanced technologies such as voice-over-IP and EMRs. This will allow health care providers to use voice communications on the same wireless infrastructure that supports mobile handheld devices running data applications. The ability for providers to seamlessly integrate voice and data is what is really going to drive down costs and provide value to patients.

While there is currently no end-to-end security solution to protect data transmissions from being compromised, most health care providers are using technologies created by security specialty companies such as Certicom, NTRU, Entrust Technologies, and VeriSign to address their immediate privacy and security needs. These companies provide security solutions such as Public Key Infrastructure (PKI), Wired Equivalent Privacy (WEP), digital certificates, digital signatures, 128-bit encryption, and single user sign-on. A combination of these security solutions is the most popular approach because it is the most effective way of minimizing any encryption gaps that may occur at wireless gateways during the encryption/decryption process. The possible exposure of encryption gaps have led many providers to place wireless gateways inside their trusted networks to mitigate this risk. There are technologies out on the market that providers can use to help manage their wireless networks. Sniffers can be implemented on network backbones to perform real-time, wireless, protocol analysis on packets crossing the network. This tool will help monitor, detect, and log any unauthorized activity, and it even has additional reporting functionality to better analyze results. The proper security design will help the overall manageability, scalability, and risk management of the wireless network.

The Future of Mobile Medicine

With the proper planning and design, the integration of wireless networks into health care organizations provides an incredible opportunity for the industry to revolutionize its operations.

Increased productivity, lower operation costs, better customer service, tighter integration of mobile workers, suppliers, and customers are just a few of the ways wireless networks will impact health care providers. Many experts believe that the integration of wireless technologies into health care organizations will significantly reduce average overhead costs (30 % of gross revenues) to a percentage closer to other leading industries (e.g., manufacturing, 6%). HIPAA creates additional challenges, but it has forced providers to really assess their policies and procedures for gaps because now they are going to be held accountable for their actions or lack of them. There is even a possibility that wireless networks might reduce an organization's exposure to lawsuits because wireless devices are typically more accurate and complete than manual systems. Therefore, patients are more likely to be satisfied with the services they have received, and less likely to impose litigation against a provider. As technologies mature and adoption rates increase, issues such as security, compatibility, and hardware restrictions will diminish. This will make wireless networks more manageable and scalable. Health care providers must start taking the initial steps towards wireless integration, otherwise, they will cease to exist ten years from now due to the fluctuating costs of health care and competition.

Sources

Ante, Spencer E., Borrus, Amy and Hof, Robert D. "In Search of the Net's Next Big Thing." BusinessWeek Online. March 26, 2001. URL: http://www.businessweek.com/magazine/content/01_13/b3725022.htm (10 April 2001).

Day, Roseann and Daly, John. "Widening Your Secure eBusiness to Wireless." IDC. December 2000. URL: http://www.idc.com (10 April 2001).

Edwards, John. "Mobile Medicine Starts Slow." MbizCentral. March 2001. URL: http://www.mbizcentral.com/m-business_story/mobile-med (10 April 2001).

Fields, Jay. "Handheld-to-Handheld Combat in the Doctor's Office." BusinessWeek Online. May 9, 2001. URL: http://www.businessweek.com/smallbiz/content/may2001/sb2001059_494.htm (July 16, 2001).

Merillat, John Charles and Cox, James. "Security Impacts Physicians...as well as Developers." Health Management Technology. October 2000: 26-27.

Schou, Jeff. "From Gee-Whiz to Must-Have." Health Management Technology. April 2001: 44-45.

Stammer, Lisa. "As Technology Improves, New Applications Take Off." Healthcare Informatics. February 2001: 50-52.

Tabar, Pamela. "Healthcare Faces a Tricky Conundrum of Confidentiality, Data Integrity and Timeliness." Healthcare Informatics. February 2000: 50-52.

Tabar, Pamela. "A Security Strategy: Possibly the Biggest Task on Healthcare's To-Do List." Healthcare Informatics. February 2001: 46-48.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS