

[WP-006]

Whitepaper: HIPAA, Security and You

An Opinionated Discussion about Securifying Healthcare Environments and their Impact

Version 040517

May 2004

Author: Bob Radvanovsky, rsradvan@unixworks.com

(A special thanks goes to those listed for being my “sounding board” on this project.)

Copyright © 2004 Mike Smith. All rights reserved.



Limited Liability Statement

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for the purpose of discussing a possible, and/or proposed IT security issue, and is not dependent upon any specified infrastructure, architectural condition or its issue(s).

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

NOTE: UNIXWORKS is publishing this document on behalf of Mike Smith.

JCAHO Compliance Statement

The level (and measures) of version control within this document complies with the minimum requirements and guidelines outlined by the Joint Commission of Accredited Hospital Organizations (JCAHO) for any version control of IT documentation.

HIPAA Compliance Statement

Information contained within this document does not contain any patient record information whatsoever. Any information outlined within this document that appears to coincide with an actual patient or representation of any transaction, rule, document, docket containing any portion of patient information is purely coincidental. All information presented within this document contains false record information and does not constitute (or represent) any patient or individual under the care, guidance, or direction of any medical services representative of, by and for any healthcare organization, its facility, or verification thereof; nor is it representative of any such patient or individual ever having been a patient or visitor of any healthcare organization, or its facility thereof. This statement complies with the minimum requirements and guidelines outlined of the final rule adoption standard of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR Part 160, 162 and 164: Health Insurance Reform: Security Standards; Final Rule.



Introduction

With the introduction of the twenty-first century, specifications, rules and newly introduced regulations at both state and federal levels regarding health information came under fire of a set of federal regulations representing the national healthcare information infrastructure, and how healthcare currently exchanges information. As healthcare continues to improve upon itself through increasingly greater dependence upon technology to providing faster and more reliable communications both within and between healthcare organizations, significantly greater sophistication of technology and methodologies provides (hopefully) improved and advanced opportunities in integrated healthcare systems, improving access time, quality of care for their patients and (at the same time) significantly reducing administrative costs to operate and maintain. Currently, patient record and healthcare information may be accessed from several locations openly through multiple healthcare providers, insurance carriers and health plan organizations. With greater information availability comes the increased threats and risk associated with the integrity, availability, and privacy of that information. HIPAA is supposed to promote the adaptation of lowered cost information exchange technologies, such as the Internet (for example). Ironically, the direction of community-based environments that shared their information through privatized pipes and tunnels across the Internet offers greater flexibility and significantly reduced costs through a common networking medium. As such, the “securification” process needed to ensure that patient and medical record information remains private (or at least designated to the correct and authorized individual or healthcare entity), continues its high level of data integrity, and is consistently available to those who need it, when they need it.

Around the year of 1996, during President Bill Clinton’s years, was introduced the Health Insurance Portability and Accountability Act (HIPAA PL 104-191) and was passed with several provisions subtitled “Administrative Simplification”. The purpose of this regulatory act was to improve Medicare under Title XVIII and XIX under the Social Security Act, not to mention improving efficiency and effective information system standards and requirements of any given healthcare system through its development and improvement cycles, esp. for the transmission of patient or medical record information near or across publicly accessible networks.

HIPAA is the first federal regulation specific to healthcare and medical records privacy, and is (by far) the most significant and complex of privacy laws to date, specifically involving healthcare information and its management that affects its use, release and transmission of private patient or medical records information. Healthcare providers, doctors offices, clinics, medical records organizations – will need to be in compliance with the provisions outlined within HIPAA – as penalties are severe and significant if found non-compliant.



HIPAA has several important requirements for all healthcare providers, and those who work directly with patient and medical records information. The Administrative Simplification standards are quite lengthy and extremely complex, often requiring several reviews of their implications; however, what will be the immediate impact is what will be placed upon those involved with the following functionalities:

- ❖ implementation of a standardization of electronic patient/medical record and patient financial information, and how information is exchanged and transmitted
- ❖ define, implement and utilize unique identifiers for healthcare providers and those who work directly with patient and medical record information
- ❖ regulate the confidentiality of patient and medical record information
- ❖ modify/alter business methods and procedures at a technical level that will ensure the integrity, privacy and availability of healthcare information

HIPAA Security Requirement

HIPAA mandates that a set of rules are to be implemented throughout the entire service-chain of the healthcare process, from the healthcare providers, the insurance carriers, government benefit agencies, pharmacy organizations, claims processors and other transaction clearinghouses (e.g. NEBO). Though HIPAA's security and privacy requirements may be separate requirements, they are tightly cohesively bound together. The tie-in between the two requirements is that privacy defines the method by how the information is displayed and who (or how) it is displayed, whereas security is the defined and administered procedural mechanism that ensures its safety. Privacy concerns itself to both written and oral communication forms to any individual who may disclose patient or medical record information. That information identifies a patient/individual, or may be used (derivatively) to help identify a patient/individual. Thus, HIPAA will require significant changes in the healthcare industry in how information is handled, disseminated, communicated, accessed and stored.

The security requirements were defined with the intention of remaining technologically independent, as technology continues to develop rapidly; thus the requirement may not be applicable if (at the time) the current technology is out-of-date or no longer available. Essentially, the security requirement recommends and mandates certain safeguards for the physical storage and maintenance, as well as transmission, access and availability to patient and medical record information. The requirement also specifies safeguards such as cryptography (and its use) to ensure that unauthorized access of data/information that is transmitted over unsecured networks (e.g. "Internet") remains safe.

These requirements are a compendium of a much larger set of complex requirements that must be met, one way or another. Though the solutions may vary from healthcare provider to healthcare provider, each provider must meet some rudimentary requirements, one of which is a concern expressed by many healthcare providers in that the cost of addressing some (if not most) of the requirements, especially compliance requirements, are very vague in their definition. Nonetheless, it soon will be a required compliance, though the big question will be how it will be enforced.



You Have 20 Seconds to Comply

The risks that may be associated with improperly or inadequately secured IT infrastructure (this includes all aspects of information technology which include: networking, systems and applications) may include the following: harm to an individual or patient (physical or mental anguish), liability of information leaked into public channels, loss of market share (usually applies to publicly traded companies, but can apply to private organizations as well), reduced or tarnished public image, and (perhaps one of the worse ones) continued mistrust of the public towards the IT department and the healthcare provider affected by the situation.

Access to patient or medical record information will be based similarly to that used by military and defense organizations over the past 50+ years, referred to as "role based authentication". Essentially, access to patient or medical record information must meet certain criteria based upon specified job roles of those requesting the information, such as a physician, nurse, clinical technician, pharmacist or site administrator.

Some potential threats to patient/medical record information include:

- ❖ intentional misuse from healthcare personnel
- ❖ malicious or criminal use/misuse from healthcare personnel (such as identity theft)
- ❖ unauthorized access of data through an external source (such as the Internet)
- ❖ unauthorized access of data through poorly configured physical access methods (can be healthcare personnel, or an outsider)

Although the HIPAA requirements require a common sense mindset towards security implementations, according to the Department of Human Health Services (DHHS), HIPAA requires a technically neutral base of security procedures, controls and mechanisms, but does not provide explicit security methodologies for configurations using an unsecured network, such as the Internet. There are several mechanisms that presently exist that would enable healthcare providers methods of securification of their environments for use over unsecured networks, such as authentication methods, strong encryption, smart cards (proxy cards with built-in circuitry that "think") or security identification cards. The list goes on and on.

Though HIPAA culminates more than just securing data, and complying with security and privacy requirements, the regulations of HIPAA will be extremely challenging to many healthcare providers and organizations. One of the most significant problematic areas is shared account information, usually at the frontline of the healthcare industry, such as a nursing station or the front desk of the hospital or physician's clinic. Shared accounts or accounts that have guessable passwords (in many cases, no passwords), can be easy intercepted by individuals who may want to harm the healthcare organization, or target an individual or specific patient. A common feature found at most hospitals and physician clinics are accounts with passwords stuck on PostIt[™] Notes of the workstation monitor or terminal CRT screen.



Additionally, if it is a workstation, the workstation does not have an auto-lock/auto-disable feature enabled such that the administrator, nurse or clinician that was using the workstation should leave, that it automatically locks the workstation, requiring a password – observably, this does not appear to exist at all. This is probably one of many challenges facing healthcare providers today, and because the process is engrained in the onsite staff, often any change is met with an extremely strong resistive.

Healthcare providers, like many corporatized organizations, have very limited budgets to expend towards security or training involving security. Additionally, many of their budgets are already strained to meet health issues and other standards and regulatory issues in which both privacy and security only compounds and exacerbates the issue even further. Fact is, many healthcare providers would wish/rather that someone else handles the security issues than themselves; in some cases, healthcare providers are considering outsourcing the security aspects to security management companies, specific to the healthcare industry, such as VISICU.

Nonetheless, HIPAA security is infantile in its implementation; as it continues to lack any good coordination or specific direction; whereby often the directives are convoluted and awkward to understand. Since its interpretation is left up to those have absolutely no knowledge of neither the mirad of computer technologies, nor how security policies would be imposed (let alone enforced), raises may concerns about how healthcare providers will comply to federal regulations on both the privacy and security fronts. Until specific questions may be met (and not through endless meetings of committees -- and quickly), the security implementations will be (mostly) useless and ineffective. The mindset associated with security is not necessarily simply a technical aspect of it, but rather a social and psychological interpretation of how security intervenes within the organization, and how it should be implemented. Unless these basic fundamentals are understood, any implementation will be met with prejudice and extremely biased opinion.

In closing, HIPAA security has much to go before it can be an effective and useful tool by healthcare providers. And, until healthcare providers, are willing to acknowledge the need for increased security awareness, this too, will fall flat on its face.

