31st Annual International Conference of the IEEE EMBS
Minneapolis, Minnesota, USA, September 2-6, 2009

Potential Impact of HITECH Security Regulations on Medical Imaging

Fred Prior[a], Mary Lou Ingeholm[b], Betty A. Levine[c], Lawrence Tarbox[a]
[a] *Mallinckrodt Institute of Radiology, Washington University School of Medicine, St. Louis, MO*
[b] *The Informatics Application Group, Reston, VA*
[c] *ISIS Center, Georgetown University Medical Center, Washington, DC*

Abstract— Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act (ARRA) of 2009 [1] include a provision commonly referred to as the "Health Information Technology for Economic and Clinical Health Act" or "HITECH Act" that is intended to promote the electronic exchange of health information to improve the quality of health care. Subtitle D of the HITECH Act includes key amendments to strengthen the privacy and security regulations issued under the Health Insurance Portability and Accountability Act (HIPAA). The HITECH act also states that "the National Coordinator" must consult with the National Institute of Standards and Technology (NIST) in determining what standards are to be applied and enforced for compliance with HIPAA. This has led to speculation that NIST will recommend that the government impose the Federal Information Security Management Act (FISMA) [2], which was created by NIST for application within the federal government, as requirements to the public Electronic Health Records (EHR) community in the USA. In this paper we will describe potential impacts of FISMA on medical image sharing strategies such as teleradiology and outline how a strict application of FISMA or FISMA-based regulations could have significant negative impacts on information sharing between care providers.

I. INTRODUCTION

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), which called for a set of federal standards for protecting the privacy of protected health information (PHI) - the HIPAA Privacy Rule [3], and later a set of standards for digital information security known as the HIPAA Security Rule [4]. A major objective of HIPAA is to ensure that a patient's privacy is protected while facilitating the exchange of healthcare related information and improving healthcare delivery. In 2007, the Institute of Medicine published a report [5] which concluded in part "that the HIPAA Privacy Rule does not protect privacy as well as it should, and that, as currently implemented, it impedes important health research."

Title XIII of ARRA, also known as the "Health Information Technology for Economic and Clinical Health Act" or the "HITECH Act", addresses the promotion of Healthcare IT. Subtitle D of the HITECH Act expands the HIPAA Privacy and Security Rules. The HITECH Act specifically states that HIPAA and the Privacy and Security Rules remain in effect but must be amended to be consistent with the new objectives of the HITECH Act. In particular section 13402(h)(2) of HITECH requires the department of Health and Human Services (HHS) to issue and regularly update "guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals"[1] which may be interpreted to include encryption technologies. HITECH also places technical responsibility for security standards and guidelines with the National Institute for Standards and Technology.

With the HITECH act the government has expressed a clear intent to facilitate information exchange in order to promote electronic health record and personal health record technology development and adoption. There appears to be an understanding that to accomplish these goals it is necessary to improve information security in the healthcare domain. Given the apparent role for NIST in redefining security requirements for the private sector, it is logical to assume that NIST may draw on the security framework put in place by FISMA.

II. RELEVANT FISMA REGULATIONS

Through the Federal Information Processing Standards (FIPS) and the 800 series of Special Publications [6], NIST sets computer and network security requirements with which agencies of the federal government must comply. FIPS PUB 200[7] defines the minimum security requirements for computer and information systems and the data that they store, process and communicate. Seventeen requirement categories are identified including: access control; audit and accountability; certification, accreditation, and security assessments; configuration management; identification and authentication; media protection; physical and environmental protection; system and communications protection; and system and information integrity.

These requirements include the encryption of all data while stored on computers or in transit. The encryption algorithms used to protect this information must be tested and validated under the Cryptographic Module Validation Program (CMVP) to confirm they are in compliance with the requirements of FIPS PUB 140-2. A mechanism for key management is also required.

III. HYPOTHETICAL USE CASE

A simple use case can help to explore the potential impact of FIS**MA** on current clinical information sharing. Teleradiology is a common practice whereby one or more imaging centers acquire digital images and then send those images to a central reading site as illustrated in Figure 1.

Frequently the imaging sites are in rural or suburban areas and the data is transported to a metropolitan hospital. It is also not uncommon for the image reading process to be distributed so that radiologists may read their case load from multiple locations including their home. PHI is gathered at the imaging site, which is commonly not part of the same HIPAA covered entity as the reading site (often a business associate agreement is in place), and must be transferred to the Image Server/Database along with the images. Images and other identified information are managed at the central site and distributed to multiple reading locations. The Radiologist generates a report, usually by verbal dictation, and that dictation record (also containing PHI) is transported to a transcriptionist (possibly associated with another business associate) who converts the speech to text. The final text report is returned to both the central site and to the imaging center either via a digital file sharing means or via fax.

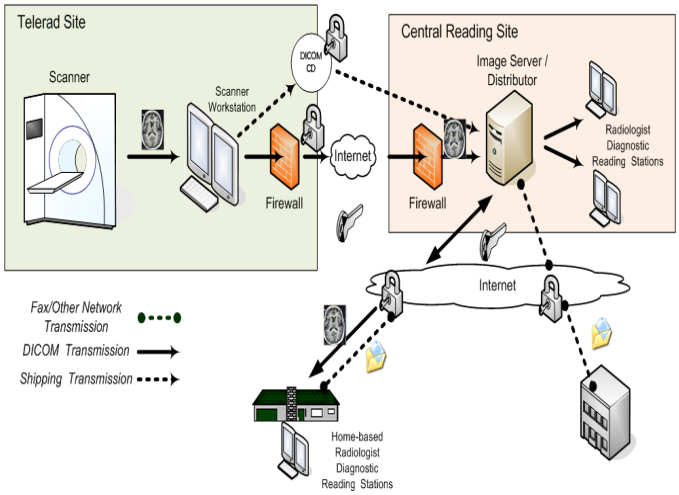

Figure 1. Teleradiology Use Case. Potential FISMA impacts are indicated by the lock and key symbols.

IV. Potential Impacts of New Security Regulations

Medical image exchange is most commonly based on the Digital Imaging and Communications in Medicine (DICOM) standard [8] for both network communication and the formatting of removable media. Often integration profiles provided by the Integrating the Healthcare Enterprise (IHE) effort [9] are used to define how DICOM and other Health Information Technology (HIT) standards are employed to solve specific problem. The DICOM and IHE security models are not explicitly FISMA compliant.

FISMA requires that FIPS140-2 encryption must be used both for network and removable media based information exchange. While DICOM itself does not restrict the encryption algorithm that can be used, most medical imaging devices do not incorporate encryption algorithms into their DICOM implementation. Therefore, the only way to securely transfer the DICOM image is over an encrypted channel like a virtual private network (VPN) or secure file transfer. Other FIPS 200 requirements include the use of authentication mechanisms and digital credentialing, both of which are not part of currently available teleradiology products.

The creation and shipping of removable media introduces its own problems since the removable media must be encrypted and there are not currently any mechanisms for encryption key management with removable media. And even if key management was solved, the burden placed on the busy healthcare worker to encrypt the removable media and files prior to sending would be large and possibly prohibitive.

FISMA also places requirements on the Image Server/Database. In particular, such components must pass a rigorous certification, accreditation, and security assessment and must incorporate security related operating system patches in a timely manner. Because medical image management systems have been classified as medical devices and therefore are regulated by the FDA, device manufacturers must regression test their software with all new patches to ensure proper operation of their regulated systems. This is a process that takes time and is at odds with a requirement to autopatch such systems. At the very least, the vendors of the medical image management systems should be involved in vetting patches applied to their systems [10].

Stricter user authentication and access control requirements included under FISMA may impact remote readers and their ability to access PHI labeled image data or at a minimum force the redesign of existing teleradioloy and Picture Archive and Communication Systems (PACS). In addition it is not clear that all teleradiology systems in operation today utilize an encrypted communication channel between their image server and remote viewing clients. Such a secure channel would be required to be in strict compliance with FISMA.

The common practice of digital dictation and remote human transcription (as opposed to speech-to-text technology) may be seriously impacted by heightened computer security requirements including encrypted communication, authentication and credential management.

V. Can new DICOM/IHE features help?

Both the DICOM Standard and IHE profiles outline mechanisms that can be used to securely exchange PHI. The DICOM Standard explicitly mentions the option of layering the DICOM networking protocol on top of the Transport Layer Security (TLS) protocol. The TLS protocol is compatible with the Secure Sockets Layer (SSL) protocol commonly used in secure web communications [11], and does offer encryption using algorithms allowed by FIPS 140-2. The IHE Audit Trail and Node Authentication (ATNA) profile also specifies the use of TLS for secure communications. While many vendors implement ATNA and TLS in their systems, in the authors' experience, most sites do not turn it on. Although the reasons for not enabling it vary, the most common roadblock is that ATNA and TLS are not available on all equipment that a site might use. Hence sites tend to drop to the lowest common denominator, which is to leave TLS turned off.

A more common practice for protecting DICOM communications with a remote site or a remote reader, such as those involved in teleradiology, is to secure the communication channel at the network level. For instance, the channel could be a private communication network with

encrypting access hardware. But since deploying private networks incurs significant expense and administrative overhead, many sites involved in teleradiology utilize Virtual Private Network (VPN) connections. VPN connections tend to work very well for securing communications for employees working on the road or at home (e.g. remote reading), or to secure communications with partners who have an established business associate agreement in place. VPNs also incur administrative overhead and can become unwieldy as the number of connections becomes large.

Grid-based technologies such as the Globus Medicus [12] or Virtual PACS [13] systems have also been used for securely exchanging images between remote sites. These systems typically set up gateways at each site that transform local DICOM protocol messages into Grid-based messages when communicating with remote sites, essentially allowing the DICOM protocol to tunnel through the grid. The gateways utilize Grid-based security mechanisms to protect the communications.

DICOM specifies mechanisms that can be employed to encrypt DICOM objects exchanged on removable media, such as recordable DVDs. Each object on the removable disk can optionally be enclosed in a cryptographic envelope similar to those used in secure e-mail, thus protecting the object's contents.

DICOM also supports the exchange of DICOM objects in e-mail messages, which can be protected by cryptographic envelopes. DICOM even supports encrypting portions of DICOM objects, such as those containing PHI, and 'hiding' them in a cryptographic envelope held inside the object. This allows for the protection of sensitive portions of the DICOM object, while still allowing the object to be handled by systems unaware of the encrypted contents. Unfortunately these DICOM specified encryption techniques have not been broadly or consistently implemented in currently available commercial systems.

IHE, in cooperation with the DICOM standards committee, created the XDS-I profile (cross enterprise document sharing for images) as an alternative mechanism to the DICOM network protocols for locating and accessing DICOM data. XDS-I utilizes web services for ease of deployment across firewalls. In XDS-I, cooperating institutions, such as those in a regional health network, register manifests of images to be shared in a central registry. Users can then access the registries to locate and download the manifests of images that are available for a particular patient. From the information in the manifests, the user can locate the DICOM objects for download. Although a system could use DICOM network protocols to retrieve the images, XDS-I also specifies that WADO (Web Access to DICOM Objects) can be used to either download or view DICOM images. As in all web-based protocols, WADO can be secured through using SSL or TLS.

In the IHE web services world (such as XDS) the XUA (Cross Enterprise User Authentication) profile defines how user credentials in the form of Security Assertion Markup Language (SAML) assertions can be securely exchanged between organizations. The IHE Enterprise User Authentication (EUA) profile utilizes Kerberos tickets for exchanging user credentials. DICOM also provides mechanisms for securely exchanging user credentials either as SAML assertions or as Kerberos tickets.

The security mechanisms already defined in DICOM and in the IHE profiles likely could be used to securely communicate data as required by FISMA. However, other FISMA requirements may present more significant hurdles in setting up secure communications between entities that are not part of the same organization. The differing security policies established by unrelated entities often prohibit the establishment of secure communications or even the sharing of information between those entities. Adding stricter controls in an effort to satisfy FISMA requirements might only exacerbate an already chaotic situation. While reasonable and enforceable security policies should be in place, they need to be developed in a way that fosters, not prohibits, appropriate trust relationships for data sharing between otherwise unaffiliated organizations. Some interpretations of FISMA make establishing such trust relationships very difficult at best.

Implementation and deployment (i.e. getting vendors and organizations to use the standards) is another major hurdle to improving security. Full implementation of FISMA requires that encryption be done by a certified (per CMVP) implementation of the encryption algorithms. Those few existing medical devices that support encryption likely are not using certified implementations. Short of reworking the product, one would have to certify the entire medical product, which could be a time-consuming and expensive process. Until all the systems in use support the security standards, turning on full security could cause major disruptions in operations.

VI. Conclusions

Legislators and government regulators must not lose sight of the fact that if computer security requirements become too complex and restrictive they will most likely not be used and that the ultimate goal of promoting the electronic exchange of health information to improve the quality of health care will be delayed. Small imaging centers will not have the expertise for complicated security procedures so vendor products must be rapidly updated to incorporate enhanced security technologies. The alternative is a new cottage industry in specialized image gateways and secure image receivers that are bolted on to existing infrastructure at added expense and reduced efficiency. In today's standard practice, computer security, let alone patient privacy and PHI protection, is pretty lax. We need to improve this situation BUT if we take a hard core approach that does not take into account the real needs and IT capabilities of healthcare practitioners; we are looking at a massive set of unintended consequences.

References

[1] United States Congress, HR1. 2009. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf

[2] Electronic Government Act, P.L. 107-347 Title III, the Federal Information Security Management Act (FISMA) of 2002.

[3] The HIPAA Privacy Rule: Standards for Privacy of Individually Identifiable Health Information, December 28, 2000, 65 FR 82462, as amended August 14, 2002, 67 FR 53182

[4] The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.

[5] Institute of Medicine. Report Brief, February 2009 Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Available on-line:http://www.iom.edu/CMS/3740/43729/61796/61836.aspx

[6] Guide to NIST Information Security Documents located on the NIST Computer Security Resource Center (CSRC) Web site at http://csrc.nist.gov.

[7] Minimum Security Requirements for Federal Information and Information Systems FIPS Publication 200, March 2006 available at http://csrc.nist.gov.

[8] Mustra, M.; Delac, K.; Grgic, M., "Overview of the DICOM standard," *ELMAR, 2008. 50th International Symposium*, 1:39-44, available on-line: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4747434&isnumber=4747417

[9] Carr, C; Moore, S., "IHE: a model for driving adoption of standards", Computerized Medical Imaging and Graphics, 27(2-3):137-146.

[10] Joint NEMA/COCIR/JIRA Security and Privacy Committee, "Patching Off-the-Shelf Software Used in Medical Information Systems", available on-line at: http://www.medicalimaging.org/documents/Patching_OffTheShelfSoftware_Used_in_MedIS_October_2004.pdf

[11] Internet Engineering Task Force, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246 available on-line at: http://tools.ietf.org/html/rfc5246

[12] Erberich, S; Silverstein, J; Chervenak, A; Schuler, R; Nelson, M; Kesselman, C., "Globus MEDICUS - Federation of DICOM Medical Imaging Devices into Healthcare Grids"; Studies in Health Technology and Informatics, IOS Press, 126:269-278, 2007

[13] Sharma, A; Pan, T; Cambazoglu, B; Gurcan, M; Kurc, T; Saltz, J., "VirtualPACS—A Federating Gateway to Access Remote Image Data Resources over the Grid"; Journal of Digital Imaging Sep 2007.