10-2013

Managing Government Regulatory Requirements for Security and Privacy Using Existing Standard Models

Gregory Schymik
Grand Valley State University, Schymikg@gvsu.edu

Dan Shoemaker
University of Detroit Mercy, dan.shoemaker@att.net

Managing Government Regulatory Requirements for Security and Privacy Using Existing Standard Models

Gregory Schymik
Grand Valley State University
C-2-312 Mackinac Hall
1 Campus Dr.
Allendale, MI 49401
616 331-8687
schymikg@gvsu.edu

Dan Shoemaker
University of Detroit Mercy
4001 W. McNichols Road
Detroit, MI 48221
313 993-1170
dan.shoemaker@att.net

Abstract: This paper posits the use of a well-established standard approach to Federal compliance, which can be easily adapted to satisfy all legal and regulatory requirements for protection of patient personally identifiable information (PII) in health organizations. This approach is embodied in the three standards that dictate how to comply with the Federal Information Security Management Act (FISMA). These standards also provide an excellent foundation for organizing a secure operation anywhere. The discussion revolves around the application of the FIPS 199 and FIPS 200/NIST 800-53(4) standard approach to the satisfaction of the present and upcoming legal and regulatory requirements for health care PII. The outcome would provide a proven, systematically secure and cost efficient solution to those protection needs. The general approach will be explained and justified.

Keywords – PII, federal regulation, security and privacy, HIPAA, FISMA

INTRODUCTION

Public Law 109–41, which is commonly known as the Patient Safety and Quality Improvement Act of 2005 (PSQIA) is the Act that created patient safety organizations (PSOs) and their attendant patient safety databases (PSQIA, Sec.922). PSQIA establishes a voluntary reporting system to assess and resolve patient safety and health care quality issues (Clinfowiki, 2013). The aim of that Act was to "encourage the reporting and analysis of medical errors". The primary motivator for which was the finding that most preventable errors leading to patient harm are the result of "faulty systems, processes, and conditions"(Kohn, 1999). In that respect, the Report recommended that the health care system should be "designed to improve safety at all levels"(Kohn, 1999).

PSQIA mandates privilege and confidentiality protections for patient safety information, which include any, "data, reports, records, memoranda, analyses, or written or oral statements, which could improve patient safety, health care quality, or health care outcomes"(PSQIA, 2005). All relevant data is assembled and reported to the PSO as a "patient safety work product". The aggregated patient safety work products are the basis for the analysis of data from participating health organizations. The data is intended to be accessed and analyzed in order to identify overall trends/outcomes that can be used for the improvement of individual patient care processes.
In that respect however, the sensitivity of the information being kept and analyzed demands assurance of secure access and reporting. Care providers are understandably reluctant to report their patient care data externally for fear of liability, or the violation of regulatory requirements. Yet, if there is insufficient data to underwrite the characterization of patterns of care leading to improved patient safety, there is almost no point in having a PSO. Consequently, the Affordable Care Act (ACA) now mandates that hospitals with 50 or more beds will not be able to

provide services through the Act unless that hospital has implemented a patient safety evaluation system that reports to a patient safety organization (ACA, 2010).

THE INFORMATION SECURITY CHALLENGE

The information security challenge lies in assuring that each patient's personally identifiable information (PII) is passed to the PSO in such a way that it does not violate the HIPAA Privacy Rule. PSOs are among the entities that fall under the HIPAA Privacy Rule (Title 45 CFR, Part 160-164, 2010). The HIPAA Privacy Rule provides federal protections for individually identifiable health information and it gives patients an array of rights with respect to that information.

Protection of the privacy of information depends in large part on the existence of measures to secure that information. Thus HIPAA has both a Privacy Rule and a Security Rule. The Security Rule specifies the need for basic safeguards, which are installed to protect electronic health information from unauthorized access, alteration, deletion, and transmission. The Security Rule stipulates administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic health information. The Privacy Rule specifies the disclosures that are authorized and the rights that patients have with respect to their health information. In concept the Privacy Rule applies to health information in any form, whereas the Security Rule applies only to health information in electronic form. However for the sake of this discussion, both Rules will apply only to electronic information.

The HIPAA Privacy Rule regulates the protection of privacy of patients' medical records and other health information maintained and processed by health plans, health care providers, and other entities involved in the processing of health care claims (45 CFR 160, 162, and 164, 2013). The HIPAA Security Rule specifies a series of administrative, technical, and physical security procedures to assure the confidentiality of electronic protected health information (45 CFR 160, 162, and 164, 2013). In addition, the procedures in the Security Rule also assure the integrity and availability of health information (HHS, 2013a). These procedures require significant control over the use and disclosure of patient information (HHS, 2013a). HIPAA compliance was required as of April 20, 2005, (HHS, 2013a). HIPAA compliance requirements were extended to cover business associates (contractors and subcontractors) of those "health care providers, health plans, and other entities that process health insurance claims" covered originally by HIPAA by the final omnibus rule released by HHS in January of 2013. The rule requires these business associates to be in compliance by September 23, 2013 (HHS 2013b).

At its core, the Security Rule requires effective risk management. The risk analysis determines which safeguards are appropriate to satisfy the Security Rule. The risk analysis assesses the likelihood and impact of potential risks and develops rational measures to reduce risk and vulnerabilities to a reasonable and appropriate level. That risk analysis is an ongoing process, where the organization regularly reviews its records to identify how adequately existing and emerging risks are addressed within the organization.

According to this Rule risk has to be addressed in three generic areas, administrative, physical and technical. Specifically, the Security Rule requires an explicit set of procedures to implement role based access control as well as enforce appropriate supervision over personnel and ensure proper training of the workforce. In addition, an organization must have procedures in place to ensure that only authorized entities have physical access to its facilities. Finally the organization has to control use of and access to physical devices and media.

All forms of control are expressed as policies and procedures. Thus, the organization must develop practices to ensure authorized access to electronic information, as well as audit controls to ensure sufficient confidentiality and integrity of the information (HHS, 2013a). In addition, there should be technical countermeasures to ensure the confidentiality and integrity of the health information that is being transmitted over an electronic network (HHS, 2013a).

CREATING A REALISTIC PROTECTION PROCESS FROM EXISTING STANDARDS

For each PSO, risk has to be mitigated by a concrete set of administrative, physical and technical countermeasures, while, at the same time, the standards that underlie HIPPA compliance for PSOs as specified in 45 CFR Parts 160, 162, and 164 are not standards in the prescriptive sense. Instead they are more a specification of generic criteria that require some form of organizationally standard response. Table 1 (below) summarizes the eight areas where these considerations need to be addressed (HHS, 2013a):

1. *Security Standards*- the organization must adopt security standards that meet statutory requirements
2. *Security Governance* – the organization must develop policies and procedures to govern the anonymization, disclosure and tracking of patient safety work product
3. *Personnel Security* – the organization must ensure that employees and contractors uphold and maintain their personal obligations regarding confidentiality of patient safety work product
4. *Secure Space* – the organization must ensure that access to patient safety work product is restricted only to members of staff that work in the defined patient safety evaluation system
5. *Physical Security* – the organization must implement physical measures to prevent unauthorized external access to the secure space (as defined in section 3.106(a)), prevent unauthorized physical access, tampering, and theft of patient safety work product within the secure space
6. *Network Security* – the organization must implement electronic safeguards against intrusion, If such controls are not implemented other measures must be taken to prevent intrusions
7. *Access Control* - the organization must formally identify, authenticate, authorize and track access by users (internally) and authorize recipients externally
8. *Assessment*-the organization must conduct periodic risk assessments to ensure adequate process security

Table 1: Generic Areas of Consideration to Satisfy HIPAA Privacy and Security Rules

In actual practice, in order to satisfy the HIPAA Security Rule, explicit, real-world countermeasures are required. Moreover, to ensure proper implementation these countermeasures have to be both concrete in form and tangible in effect. This requirement justifies the use of an existing set of standards for the security of Federal information systems. Federal Information Processing Standards (FIPS) 199 and 200 and the National Institute for Standards and Technology (NIST) Standard 800-53(4) work together to fully and completely specify the control objective infrastructure to satisfy the HIPAA Rules at a range of levels of security.

Structuring HIPAA compliance processes using an existing regulatory model merits discussion because of two pragmatic factors. First, where compliance is mandated, it is helpful to have a proven conceptual framework in place to guide the development of the real-world practices needed to generate tangible proof of compliance. More importantly, the regulatory models discussed in this section constitute a legitimate legal framework for ensuring comprehensive best practice in securing information in any form. Thus the three standards that dictate how to comply with the Federal Information Security Management Act (FISMA) also provide an excellent foundation for organizing a secure operation within a health care setting.

The Federal Information Security Management Act (NIST, 2013) applies to all agencies of the U.S Government. Combined into a single process, the standards that implement this Act; FIPS 199 (NIST, 2013) and FIPS 200 (NIST, 2013) and NIST Special Publication 800-53 (NIST, 2013), help ensure that sufficient security control exists for all federal information systems. FISMA implementation is based on a formal risk assessment process, which validates the initial security control selection and determines if any additional controls are needed to protect organizational operations (NIST, 2013). The resulting collection of standard security controls establishes a defined level of due diligence for the organization.

FINALLY: A COST JUSTIFICATION FOR SENSITIVITY CLASSIFICATIONS

The Federal Information Security Management Act, known officially as Title III of P.L. 107-347, authorizes the use of a compliance model for federal information systems. Unlike HIPAA, which is tailored to a particular sector and environment, FISMA is comprehensive legislation that dictates every aspect of correct security practice for every large-scale information system environment. Although this paper uses HIPAA as an example, FISMA can be applied to almost any information system in almost every type of regulatory situation. In fact one point should be kept in mind as a side note; the general applicability of FISMA standards to any information system security situation makes it a "one size fits all" solution for any regulatory situation.

The advantage of combining sensitivity classification with control deployment, as FISMA does, is easy to justify. It would be a daunting task to comply with HIPPA if every piece of information had to be protected to the same degree of sensitivity. However, since an individual's SSN or financial account number is generally more sensitive than an individual's phone number or ZIP code, and breaches of 25 records and 25 million records may have different impacts, organizations can categorize the PII that is maintained into levels of required protection. If this is done right, then the protection approach can be appropriately scaled based on that "level of protection" or sensitivity classification. That ensures cost efficient implementation and operation.

DETAIL OF IMPLEMENTING AN EFFECTIVE MODEL FOR HEALTH CARE FROM FISMA REQUIREMENTS

FISMA requires each federal agency to "develop, document, and implement an enterprise-wide program to secure information and the information systems that support the operations of every federal agency." (FISMA, 2002) FISMA is implemented by two federal information processing standards publications (FIPS PUBS). These standards are issued by the National Institute of Standards and Technology (NIST) and authorized and approved by the Secretary of Commerce. The two FIPS PUBS used in the implementation of FISMA are FIPS 199 and FIPS 200.

FIPS Publication 199, "Standard for Security Categorization of Federal Information and Information Systems," stipulates criteria for assigning classification levels to the information systems that fall under FISMA (FIPS, 199). FIPS 199 serves as the basis for selecting appropriate security controls based on the relative security needs of the information that is protected. Information is categorized by FIPS 199 based on three levels of risk: high, medium, and low. FIPS 199 requires federal agencies to categorize the information processed by their systems as having low impact, moderate impact, or high impact on security.

This classification is dictated by the confidentiality, integrity, and availability requirements of the information in each system. The sensitivity of the information in each system is categorized at its highest level of potential impact on security. This concept is called the high water mark. The concept is important because significant security dependencies are built into all systems. That is, a compromise in one security objective ultimately affects the other objectives as well. Because the potential impact values for confidentiality, integrity, and availability may not always be the same for every item of data in the system, the high water mark concept is used to value the overall impact level of the information that is in the system.

FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," is meant to promote the development, implementation, and operation of more secure information systems within the federal government (FIPS, 200). FIPS 200 utilizes a risk-based approach for the selection of the security controls that are needed to satisfy the minimum requirements of FIPS 199. FIPS 200 ensures minimum levels of due diligence for information security and helps federal agencies follow a more consistent, comparable, and repeatable approach to the development of explicit security controls for information systems (FIPS, 200). The 17 areas covered by FIPS 200 represent a broad-based response that addresses all aspects of management, operations, and technology. Policies and procedures play an important role in the effective implementation of enterprise-wide security and the long-term success of the resulting measures. Table 2 lists the security-related control areas are specified in FIPS 200.

1. *Access control*—Limit information system access to authorized users, processes, and devices.
2. *Awareness and training*—Ensures that personnel are adequately trained
3. *Audit and accountability*—Ensures that actions can be traced to ensure accountability.
4. *Certification, accreditation, and security assessments*— Monitors security to ensureeffectiveness.
5. *Configuration management*—Establish and enforce baseline configurations for information assets.
6. *Contingency planning*—Implement plans to ensure availabilityand continuity of operations
7. *Identification and authentication*—Identify users and processes and authenticate their identities.
8. *Incident response*—Establish operations for incident handling within the organization.
9. *Maintenance*—Establish controls for maintenance techniques, mechanisms, and personnel
10. *Media protection*—Protect mediaand sanitize media before disposal or release for reuse.
11. *Physical and environmental protection*—Limit physical access to equipment and environments.
12. *Planning*—Develop plans that describe current and planned security controls
13. *Personnel security*—Ensure that people in positions of responsibility are trustworthy
14. *Risk assessment*—Assess risk to operations as a result of processing, storing, or transmitting data
15. *Systems and services acquisition*—Ensure security in sourcing and acquisition
16. *System and communications protection*—Monitor, control, and protect communications
17. *System and information integrity*—Identify defects and protect against malicious code

Table 2 – The Seventeen Security Related Control Areas of FIPS 200

NIST 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations", specifies a comprehensive set of control objectives appropriate to each of the FIPS 199 baseline levels of protection and each of the requisite security control areas in FIPS 200. The controls that are specified are at the discrete behavioral level and taken as a set constitute current best practice in satisfying each security control area's requirements. In order to provide comprehensive definition of the necessary controls for each level of sensitivity, NIST 800-53 is a substantial document. However, if utilized as intended the degree of practical and detailed control specification will guarantee a proper level of security for each level of sensitivity. More important, the resulting tangible control set can be verified by audit and used as documented proof of due diligence in complying with future requirements for rigorous protection of patient PII.

CONCLUSIONS

The premise for this discussion is relatively straightforward and the conclusions are simple. Increased regulatory requirements for the protection of patient PII will require rigorous and well-proven methods for both implementing and auditing health care system security. The existing standard process for securing federal information provides a detailed, practical and cost effective basis for both ensuring the confidentiality, integrity and availability of patient information; as well as allowing the organization to optimize the deployment of that protection in a cost efficient manner.

Because the FISMA approach has been in place for almost a decade there are a large number of studies and reports to guide deployment and the process itself has stood the test of time. The FISMA approach also has the advantage of being based on the same type of compliance requirements that existing health care information protection regulations will impose. Consequently, the proof of due diligence is built in for Federal auditors. Given all of these factors a health organization struggling to meet mandated patient information protection laws could benefit considerably from this approach.

REFERENCES

Clinfowiki, "The Patient Safety & Quality Improvement Act of 2005 (PSQIA): The Lesser Known Privacy Rule", clinfowiki.org/wiki/index.php/Patient_Safety_and_Quality_Improvement_Act_(PSQIA), accessed July 2013

FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, February 2004

FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD March 2006

HHS 2013a, www.hhs.gov/ocr/privacy/index.html, Office of Civil Rights, accessed July 2013

HHS 2013b, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf, accessed September 2013.

Kohn, Linda T.; Corrigan, Janet M.; Donaldson, Molla S., (ed.) To Err is Human—Building a Safer Health System. Washington, D. C.: National Academies Press. 2000p. 312

Office of the Secretary Department of Health and Human Services, 45 CFR Parts 160 – 164, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule", Federal Register, Vol. 78, NO. 17, January 2013

National Institute of Standards and Technology, csrc.nist.gov/groups/SMA/fisma/index.html, accessed July 2013

H.R. 3590, Patient Protection and Affordable Care Act of 2010, 111th United States Congress, Second Session, Washington DC, 2010

H.R. 3590-55, at Part II, section 1311(h)(1)(A)(i) Patient Safety and Quality Improvement Act of 2005, Public Law 109-41 (S.544), 109th United States Congress, First Session, Adam L. Scheffler (ed.), Version 5.0, March 29, 2006, Chicago

Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, 04/30/2013

Wikipedia (a), Patient Protection and Affordable Care Act, en.wikipedia.org/wiki/Patient_Protection_and_Affordable_Care_Act, Accessed July 2013