

February 15, 2005

Executive Summary

Cross-walking Security Requirements

Background

The Healthcare Information and Management Systems Society (HIMSS) in conjunction with the NIST/URAC/WEDI Security Health Care Certification and Accreditation Workgroup, originally supported the effort to create a crosswalk of security requirements focused specifically on the Health Insurance Portability and Accountability Act (HIPAA). This security crosswalk is an outgrowth of an activity that originally started as a voluntary exercise in the HIMSS/NIST/URAC/WEDI Workgroup.

The HIPAA Security Crosswalk document is designed to help organizations to

“build upon and maximize the existing security processes and - procedures in place within an organization while complying with new security related regulations, namely the HIPAA Security Rule.”

Depending on the environment, there are potentially several other information security requirements and accreditations that a health related entity may already have implemented even prior to HIPAA becoming law. As covered entities struggle to achieve compliance with the HIPAA Final Security rule on or before the compliance date of April 20, 2005, [1] one of the first questions to ask is:

“What security practices are presently in place in the organization that may help in meeting the security requirements dictated in the HIPAA Security Rule?”

All healthcare organizations must/should have some security measures in operation in accordance with sound business practices. The extent of these measures usually varies based on the size, location, mission, function, insurance requirements, and other factors related to a healthcare entity. HIPAA is the current driver for more closely examining and evaluating the current security procedures, policies, processes, and protections and determining their adequacy toward complying with the HIPAA Final Security Rule.

The HIPAA security crosswalk document was sponsored by the respective organizations to be a resource tool for their member companies and others in the health community as they attempt to comply with HIPAA in as timely, efficient and through a manner as possible. To this end, objectives of the cross walk include providing a document by which an organization could perform a “gap analysis” against security requirements already in place, achieving economies of scale in the area of security, eliminating duplicative efforts and documentation,

February 15, 2005

achieving cost-efficiencies, and fully complying with all security mandates. In addition, because the HIPAA Security Rule is a framework, without specific requirements, the document is intended to be an industry consensus on the details of health information security implementation. This should give both industry and regulators an indication of current industry practices, making both implementation and compliance easier.

Subject Matter Experts

The crosswalk could not have been created without the knowledge and efforts of a dedicated group of subject matter experts. The list of reviewers and participants in regular conference calls from HIMSS, NIST, URAC, and WEDI is too long to replicate here. The core group of subject matter experts, however, must be acknowledged for their time and effort. Following is a list of persons who contributed to the information in the crosswalk, along with their email addresses.

Mike Bell, Mintz Levin, mdbell@mintz.com
John Bogen, Health CIO, jdb8432@consultant.com
Mike Cummins, TecSec, Inc., mikec@tecsec.com
Mike Fisher, MDF Consulting, mdfconsult@yahoo.com
Lisa Gallagher, Javelin Technology Group, lgallagher@comcast.net
Bruce Gnatowski, Cyber Trust, Bruce.Gnatowski@cybertrust.com
George Goble, Trinity Health, goblegr@trinity-health.org
Joan Hash, NIST, joan.hash@nist.gov
Arnold Johnson, NIST, Arnold.Johnson@nist.gov
Devin Jopp, URAC, djopp@urac.org
Mark McLaughlin, McKesson, Inc., Mark.McLaughlin@McKesson.com
Bob Perlitz, Healthcare IS Consultants, bobp@hiscllc.com
Ron Ross, NIST, ron.ross@nist.gov
Dennis Seymour, Veterans Health Administration,
Dennis.Seymour2@med.va.gov
Carla Dancy Smith, Booz, Allen Hamilton, smith_carla@bah.com
Catherine Solomon, Kindred Healthcare, Inc.,
Catherine.Solomon@kindredhealthcare.com
Adam Stone, Assurant, Adam.Stone@assurant.com
Denise Turner, State of New York, Denise.Turner@omr.state.ny.us
Ken Yale, EduNeering, Inc., kyale@eduneering.com

Scope

The crosswalking of security requirements is a useful first step because it maps the requirements that come from multiple sources to see where duplication and redundancies occur. This crosswalk project selected HIPAA as the driver and identified three specific regulations for “mapping requirements.”

Regulations	Description/Summary
DRIVER: Health Insurance Portability and Accountability Act (HIPAA)*	<p>Centers for Medicare and Medicaid Services (CMS) Web Site, HIPAA Administrative Simplification – Security, Final Rule</p> <ul style="list-style-type: none"> • URL:http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp
International Organization for Standardization (ISO) 17799	<ul style="list-style-type: none"> • “Detailed security standard organized into ten major sections, each covering a different topic or area: <ol style="list-style-type: none"> 1. Business Continuity Planning 2. System Access Control 3. System Development and Maintenance 4. Physical and Environmental Security 5. Compliance 6. Personnel Security 7. Security Organization 8. Computer & Operations Management 9. Asset Classification and Control 10. Security Policy • Within each section are the detailed statements that comprise the standard.” • http://www.iso17799software.com/
CMS Core Security Requirements (CMS CSR)	<ul style="list-style-type: none"> • “Detail technical requirements for business partners who use IT systems to process Medicare data. Business partners must establish and maintain responsible and appropriate controls to ensure the confidentiality, integrity, and availability of Medicare data. CMS has organized the Core Security Requirements into Categories, General Requirements, Control Techniques, and Protocols. There are ten Categories <ol style="list-style-type: none"> 1. Entity-wide Security Program Planning and Management Elements 2. Access Control 3. System Software 4. Segregation of Duties 5. Service Continuity 6. Application Software Development and Change Control 7. Application System Authorization Controls 8. Application System Completeness Controls 9. Application System Accuracy Controls 10. Networks” • http://www.cms.hhs.gov/manuals/pm_trans/AB03005.pdf
Federal Information Security Management Act of 2002 (FISMA)	<ul style="list-style-type: none"> • Includes a section on information security requiring program management, evaluation, and reporting activities • Establishes a framework for ensuring effectiveness of Federal information security controls along with guidance regarding the development and maintenance of minimum standards • http://www.whitehouse.gov/omb/memoranda/m01-08.pdf

The above list of requirements is admittedly is not exhaustive. There are many other standards, rules, regulations, and guidelines that are not covered by this crosswalk project, but may nevertheless apply to your organization.

Benefits of Crosswalking Security Requirements

There are several direct benefits to be achieved by a security regulations crosswalk exercise. These benefits address how the outcomes of the crosswalk may be utilized.

- As noted above, the crosswalks allow organizations to identify existing security safeguards and mechanisms.
- The documents will allow the user to gain familiarity with other standards and guidelines, several of which were used by the government to create the HIPAA Security Standards.
- The analysis can reveal to senior executives where there are already policies, procedures, processes and tools in place to meet the HIPAA Security Rule by virtue of existing security operations.
- The exercise can highlight where adjustments in the current state can be made with minimal effort to ensure compliance.
- The summary analysis can show where there is a potential problem or an issue area that is not addressed to the required degree and immediate action may be necessary to endure compliance with HIPAA.
- The crosswalk methodology can possibly serve as a bridge among the various security (and privacy) stakeholders who may have overlapping or conflicting compliance related responsibilities within an organization.
- The security crosswalk results can be used to build a business case for more investment in needed security related resources in order to comply with requirements, where compliance gaps are identified. The cost of compliance versus the potential financial losses associated with a violation, depending upon the infringement, the enforcement mechanisms and consequences that can include fines, negative publicity, and other immeasurable consequences, are easily outlined though not often specifically calculated.

Limitations of the Security Crosswalk Activity

Although there are numerous benefits to this crosswalk initiative, it is important to recognize the limitations of this crosswalk process. The following is a non-exhaustive list of limitations to consider:

- The level of analysis in the crosswalk errs on the side of being “detailed,” but it is not absolute. This means that two provisions might be related, but not crosswalked because the commonality between the two provisions is insufficient. See Methodology Section below.
- The user will need to perform a “real-world verification” of the activities described in the standards being compared as applicable for each setting.
- The crosswalk is a paper exercise. Each organization using the crosswalk product will need to conduct on-site interviews or use some to be methods to determine the degree to which the standards are actually being followed.

February 15, 2005

- An in-depth gap analysis of the structures and business relationships within the organization as it relates to these interconnecting security requirements may produce more program specific compliance guidance.
- The user must define crosswalk limitations, assumptions, disclaimers, and parameters as applicable to their organization. Terms to describe the degree of potential “satisfaction of a security standards requirement” need to be carefully defined, understood and agreed at the onset.
- In several instances, HIPAA compliance will not substitute or negate the requirement for compliance with other regulations and policies, and vice versa.

Methodology

The security crosswalk methodology employed by the reviewers and outlined here is but one recommended approach. This crosswalk methodology is purposefully presented in as non-technical manner and in as simplistic terms as possible so that it may be embraced by non-security experts, including healthcare professionals.

This security crosswalk process followed these basic steps:

A. Select the Standards for the Crosswalk Exercise

DRIVER: Health Insurance Portability and Accountability Act (HIPAA)

The standards selected for the crosswalk are:

International Organization for Standardization (ISO) 17799
CMS Core Security Requirements (CMS CSR)
Federal Information Security Management Act of 2002 (FISMA)

B. Crosswalk the Existing, More Granular Guidelines to HIPAA

Since a primary purpose of this project was to facilitate HIPAA security compliance efforts for those organizations already complying with another set of security requirements or guidelines, our reviewers crosswalked the existing, above-mentioned security requirements to HIPAA and not vice-versa. Adopting this approach has resulted in a document that compares these granular guidelines to the more general HIPAA Security Standards. Due to the broad, flexible and often “addressable” nature of the HIPAA Security Standards, the alternative approach (HIPAA-to-existing guidelines) is subject to a considerably higher degree of subjective interpretation—something our reviewers strived to avoid.

C. Use the Literal Language of the Guidelines

For thoroughness and completeness, the reviewers used excerpts of the actual text from the two crosswalked standards (i.e., they “cut and pasted or typed” the provisions into the template). While this was a painstaking process, the workgroup believed that it was essential that the terms and the qualitative depth of the data captured enabled an “apples to apples” comparison of data.

D. Mandate a High Degree of Relevance between the Crosswalked Provisions

In general, the crosswalked security guidelines (e.g., ISO, CMS CSR) are much more specific and detailed with respect to the actions or

mechanisms expected to be performed or implemented by the organization. This dynamic creates a situation where the crosswalked guidelines, while relevant and informative, contain numerous provisions not required under HIPAA as a standard or implementation specification (addressable or otherwise). So as to avoid creating any confusion or an appearance that a crosswalked provision would be required by the HIPAA Security Standards, the reviewers crosswalked only those provisions that closely resembled, both with respect to nomenclature and intent, the standard or implementation specification set forth in the HIPAA regulations. The reviewers included comments to describe certain of the relationships between the crosswalked documents (e.g., where a crosswalked standard reasonably could be implied in HIPAA).

Indeed, the ISO, CMS CSR, and FISMA standards will be very helpful to any organization that seeks an understanding of the potential scope of a HIPAA security standard. However, the goal of this crosswalk initiative was not merely to crosswalk related provisions among the documents, which can simply be performed by reviewing the various Tables of Contents, but rather to identify those existing provisions in ISO, CMS CSR, and FISMA that arguably are required (or must be addressed) under HIPAA.

D. Use a Standard Template for Capturing the Relevant Security Requirements

The workgroup adopted Microsoft Excel as the means to capture and sort the crosswalk data. It was believed that most in the healthcare community could manage the Excel spreadsheet presentation versus a more complex database management presentation format.

There are other relational databases that can be deployed to create the mapping matrix. However, if the detailed analysis of the crosswalk is to be shared widely within an organization, it was important to select a user-friendly and easily accessible template.

Implementation

The crosswalk product is a stand-alone document that requires implementation and application for each unique organization. The next recommended step is to conduct an analysis to determine where there is some degree of coverage or potential satisfaction (towards compliance) for each requirement.

This analysis process is highly subjective. A summary sheet can be prepared to indicate at a high level using checkmarks, or numerical values or color-coding to indicate the degree to which a security requirement may be satisfied. At a minimum, there may be three ranges indicated:

High: (Green) - Great degree of similarity and overlap between the two security requirements or standards.

Medium: (Yellow) - Some potential overlap, with some degree of modification or change in the existing policy or procedures; there is something to leverage

Low: (Red) - No overlap, out of scope, non-complaint or non-applicable.

Below is a sample summary chart for a high-level presentation of the potential areas of overlap and other areas of potential exposure in a HIPAA Security Rule and DITSCAP crosswalk. Disclaimer: The contents of this sample chart are for illustrative purposes only, and not to be interpreted or accepted as real crosswalk data as it is hypothetical information.

HIPAA SAFEGUARD	CRITERIA TO MEET SAFEGUARD	INCLUDED IN DITSCAP	RISK
Technical	Access Controls	Yes	LOW
	Unique User Identification	Yes	MEDIUM
	Emergency Access Procedure	Yes	MEDIUM
	Automatic Logoff	Yes	MEDIUM
	Encryption and Decryption	No	HIGH
	Audit Controls	Yes	LOW
	Person or Entity Authentication	Yes	LOW
	Integrity	Yes	LOW
	Mechanism to authenticate Electronic Protected Health Information	No	HIGH
	Transmission Security	Yes	
	Integrity Controls	No	HIGH
	Encryption	No	HIGH

Following the analysis, the results should be summarized and an action plan developed. For example, those security requirements with a red color-coding, or an indication of a low degree of satisfaction should be ranked for immediate or first attention in the action plan. An action plan should document the decisions made as to how to close and gaps, or clearly identify non-compliant subject areas. An action plan could include the major milestones, with realistic dates for completion of the corrective measures, and an estimate of resources required to resolve the issue so that management can monitor the completion.

Next Steps

February 15, 2005

As we know, non-compliance, or the failure to implement the proper security safeguards, can result in loss or damage to valuable assets; including but not limited to: competitive or proprietary data; customer information; personnel resources; credibility and brand; protected health information – and ultimately - productivity, time and money. Individuals responsible for compliance intuitively ask:

- Where should we begin on the road towards security compliance?
- Which security regulations should be implemented first?
- What security standards are already being implemented?
- Where are the gaps between current security activities, and those required by April 20, 2005 to be in compliance with HIPAA?
- How can we leverage current security activities to meet new/additional requirements?
- How do we evolve our security program as security risks, threats, and vulnerabilities evolve?

The goal of the HIPAA security crosswalk exercise is to build upon existing security practices that may be in place as one proceeds down the path to security compliance. There are other self-assessments, gap-analyses, risk assessment tools, and security audits that can be pursued to assist in the goal to achieve compliance with HIPAA.

There are also numerous commercial vendors and consultants who offer automated tools, products, software and services to help organizations complete security crosswalks and security risk assessments, and other security related documentation and compliance activities. The purpose of this crosswalk is to offer small organizations, as well as other entities, an option to self-conduct and internally handle this process, where feasible. No endorsement of any other tools is made or implied herein.

In the commercial sector those responsible for security requirements implementation must be current in their understanding as to the security standards that are applicable in the environment, as well as for new and emerging technologies, such as wireless. The fact that there are many required and optional security standards, but no one definitive source for all security standards and industry best practices for private companies, makes the task uniquely challenging. Conversely, every U.S. government Federal agency has its list of security mandates, with specific oversight from the Government Accounting Office (GAO), the Inspector General (IG) and other numerous periodic performance monitoring and evaluation sources.

This HIPAA security crosswalk should be viewed and used as a resource, or aid, but not as the total answer to an organization's HIPAA compliance efforts. Other actions may be necessary to accomplish and ensure HIPAA compliance.

February 15, 2005

Furthermore, as security risks, threats, and vulnerabilities evolve and the science and discipline of health information security progresses, we see this crosswalk as a “living” document that will also evolve to help users keep up with health information security advances.

-