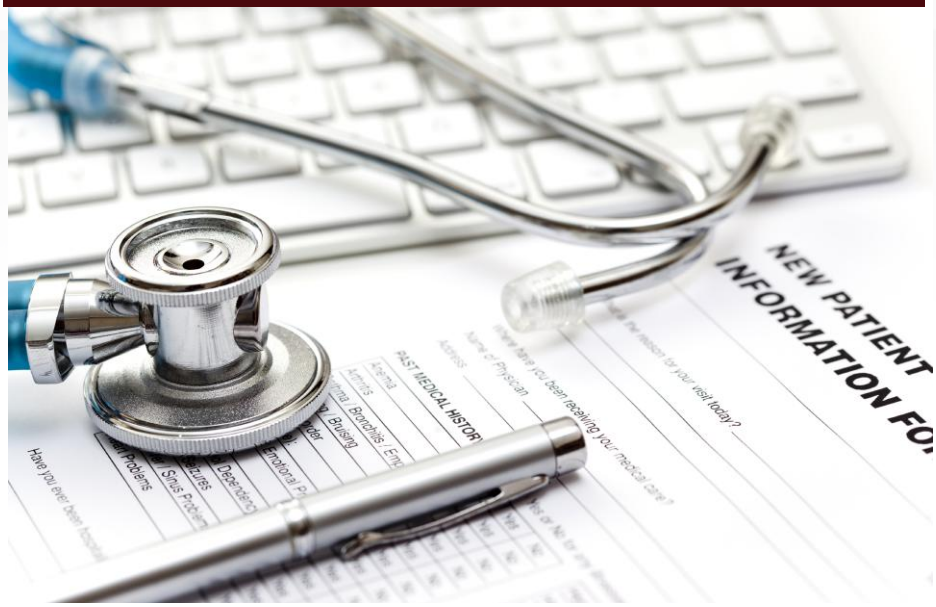
A COALFIRE WHITE PAPER

HIPAA and HITRUST - FAQ

by Andrew Hicks, MBA, CISA, CCM, CRISC, HITRUST CSF Practitioner
Director, Healthcare Practice Lead
Coalfire

February 2013



Introduction

Organizations are at a crossroads when deciding on the proper course of action to take in becoming compliant with regulations applicable to the healthcare industry. This is an important decision that shapes the foundation of an organization's security culture and prepares the company for longevity amongst the vast range of business and regulatory requirements. As a result, organizations need to know what choices are out there so they can get the peace of mind that comes with making a well-informed decision.

What is the optimal path to compliance and how can you get there? Should you assess your healthcare compliance posture against the HIPAA Security Rule, or should you choose the HITRUST Common Security Framework? What's the difference? These are questions commonly asked by healthcare IT security professionals.

The objective of this document is to provide guidance to Covered Entities, Business Associates, and subcontractors (as defined by HIPAA), and to assist in identifying the best overall approach to becoming compliant and secure in the healthcare industry.

HIPAA and HITRUST

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996. Under the Administrative Simplification provisions of HIPAA, the Security Rule was developed with the objective of safeguarding Protected Health Information that exists in an electronic form, otherwise known as ePHI. At a high level, the HIPAA Security Rule is based on three types of security safeguards: Administrative, Technical, and Physical. Each safeguard includes a series of Standards and Implementation Specifications (or requirements) designed to address the risks associated with the confidentiality, integrity, and availability of ePHI data. Certain safeguards in the HIPAA Security Rule are required, while others are addressable. Addressable requirements are not optional; instead the organization can choose not to implement them if there is a valid rationale (e.g., the risk is significantly low) which must be documented. HIPAA provides limited guidance to covered entities and Business Associates in determining risk however, often referring organizations to guidance available from the National Institute of Standards and Technology (NIST).

HIPAA applies to healthcare providers, healthcare plans, and healthcare clearinghouses, collectively known as Covered Entities. Additionally, HIPAA applies to any organization contracted by Covered Entities to perform work on their behalf, where ePHI is involved. These organizations are referred to as Business Associates. Some common Business Associate functions include claims processing, data analysis, utilization review, and billing, but can also extend to organizations that provide services such as data hosting, managed services, as well software as a service (SaaS) applications.

What is HITRUST?

The Health Information Trust Alliance (HITRUST) was established for the purpose of promoting the security of healthcare information, while allowing for the adoption of health information systems and exchanges. HITRUST believes that security is critical to the broad adoption, utilization, and confidence in health information systems, medical technologies, and electronic exchanges of health information. It also believes that security is critical to realizing the promise for quality improvement and cost containment in America's healthcare system.

Under HITRUST, the Common Security Framework (CSF) incorporates the security controls and requirements from multiple standards, regulations and business requirements applicable in the healthcare industry. HITRUST harmonizes these requirements into a single set of controls and provides references back to the sources for compliance purposes. The authoritative sources incorporated and referenced in the CSF include: HIPAA, HITECH, Payment Card Industry Data Security Standards (PCI DSS), Control Objectives for Information and Related Technology (COBIT), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), the Federal Trade Commission (FTC), and many others. The resulting framework is no more burdensome than the requirements healthcare organizations and Business Associates are already subject to. Instead, the CSF streamlines the risk and compliance process by providing a comprehensive, prescriptive and scalable framework to protect sensitive healthcare information.

In addition, HITRUST operates in conjunction with healthcare, business, technology and security leaders to identify solutions to challenges related to streamlining the effective implementation and assessment of security controls that are applicable to all organizations in the healthcare industry.

HIPAA and HITRUST: A Comparison of the Frameworks

What is the HIPAA Security Rule Framework?

As previously mentioned, the HIPAA Security Rule is comprised of three types of safeguards, all of which are designed to protect ePHI data. Each safeguard is briefly explained below:

- **Adminstrative Safeguards:** Encompassing over half of the entire HIPAA Security Rule, Administrative Safeguards are generally requirements related to “soft”, or process oriented controls, such as policies, risk analysis, termination procedures, and training. In short, the administrative safeguards define the policies and standard operating procedures (SOPs) for how an organization will comply with the Rule.

- **Physical Safeguards:** Arguably the easiest safeguard to understand and comply with, Physical Safeguards identifies the requirements for how an organization will control physical access to locations where ePHI exists. Though policies and procedures are necessary, this safeguard focuses on the physical controls that protect the ePHI systems and their requisite facilities, equipment, and other infrastructures from natural and environmental hazards, as well as unauthorized intrusion.

- **Technical Safeguards:** Building on the Administrative and Physical Safeguards, Technical Safeguards provide systematic controls over the protection of ePHI data. When properly implemented, these preventative-type controls are aimed at controlling access to ePHI data through the use of unique user accounts, automatic account logout, and user authentication. Additionally, the technical safeguards are responsible for the encryption of data "at rest" and "in transit".

In addition to the above safeguards, the HIPAA Security Rule also defines the following requirements: "Organizational Requirements" and "Policies and Procedures and Documentation", each comprising two standards. Under "Organizational Requirements", Business Associate contract requirements and the plan documents of group health plans are identified. Furthermore, under "Policies and Procedures and Documentation" the requirements for implementing and maintaining written policies, procedures, and documentation are defined. The complete HIPAA Security Rule framework is available here.

What is the HITRUST Common Security Framework?

The HITRUST CSF was developed to provide organizations with a framework specifically devoted to the protection of ePHI and PHI data in the healthcare industry. Unlike the HIPAA Security Rule, the CSF is not a new standard or regulation, rather, the CSF is a certifiable framework of security controls that scales according to the type, size, and complexity of the organization and its systems. The CSF streamlines the compliance process because it is built from existing standards and regulations that already apply to healthcare organizations, as previously mentioned, allowing organizations to assess once while simultaneously meeting multiple compliance initiatives. The HITRUST CSF has two key components, the Information Security Implementation Manual and the Standards and Regulations Mapping.

Information Security Implementation Manual: To ensure the effective and efficient management and security of healthcare information, the Information Security Manual is a certifiable collection of control requirements that are based on security governance practices (e.g., organization, policy, etc.) and sound security control practices (e.g., people, process, and technology). The Implementation Manual encompasses 13 different security categories that are comprised of 42 separate control objectives and 135 specifications. It is within these control categories that the specifications are organized.

- Information Security Management Program
- Access Control
- Human Resources Security
- Risk Management
- Security Policy
- Organization of Information Security
- Compliance
- Asset Management
- Physical and Environmental Security
- Communications and Operations Management
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management

Standards and Regulations Mapping: Similar to a consolidated audit program, the Standards and Regulations Mapping tool normalizes requirements associated with the current version of the HITRUST CSF, as well as the many other accepted standards and regulations that apply to healthcare organizations. This proves to be extremely beneficial for organizations susceptible to multiple regulations and frameworks, including:

- ISO/IEC 27002:2005
- ISO/IEC 27799:2005
- COBIT 5
- HIPAA Security Rule
- HITECH Act
- Stage 2 Meaningful Use Reqs.
- NIST SP 800-53 Revision 4
- NIST SP 800-66
- CMS ARS
- PCI DSS version 2.0
- FTC Red Flags Rule
- 21 CFR Part 11
- JCAHO IM
- The CORE Security Requirements
- 201 CMR 17.00 (State of Mass.)
- NRS 603A (State of Nev.)
- CSA Cloud Controls Matrix v. 1
- Texas House Bill 300

Assessments for HIPAA and HITRUST

What is the difference between a HIPAA and a HITRUST assessment?

The original intent of the HIPAA Security Rule was to be scalable so that its requirements could be met by a wide range of organizations from a small, one doctor clinic to a large 100+ bed hospital system. The end result is a Security Rule whose requirements are vague and open to interpretation. More often than not, interpretation can only be successfully achieved by referencing robust standards such as ISO or NIST, or through the assessment of an experienced third-party assessor.

While there can be many types of assessments (e.g. gap, validation, certification), HIPAA and HITRUST assessments each share the common objective of safeguarding healthcare information, however, the similarities end there. A HIPAA Security assessment will provide an organization reassurance that when all audit recommendations have been resolved, the organization will be compliant with the HIPAA requirements. A HITRUST assessment and certification, on the other hand, takes a more risk-based approach, scaling the requirements to the risk characteristics of the organization and focusing on controls related to the leading causes of breaches in the healthcare industry. This approach also considers compliance with regulations such as HIPAA, allowing organizations to take a more holistic approach towards protecting sensitive information.

The HITRUST CSF fully integrates the requirements of the HIPAA Security Rule with the standards of ISO, NIST and many other federal, state and business requirements previously listed. By selecting the characteristics of the organization(s) and system(s) to be evaluated, the CSF's control requirements scale based on risk. This allows small, medium and large organizations to leverage the CSF as the baseline for their security program or assessment process in a way that is appropriate for each unique environment. For organizations looking to attest to business partner, customer or third-party security requirements, HITRUST offers a Certification program that defines a methodology, subset of requirements from the CSF, and toolset to support a streamlined and consistent assessment of an organization's security program.

It is worth noting that there is no official "compliance" designation or seal associated with the HIPAA Security Rule. Organizations can only attest to their compliance by providing a supporting risk assessment and evidence of their security controls. HITRUST recognizes and addresses this gap through its Certification program as previously discussed. It is also worth noting that neither HIPAA nor HITRUST require an assessment to be performed by an independent, third-party assessor. Because there is no official compliance designation with HIPAA, an assessment may be performed internally using any standard (e.g., HITRUST, ISO, NIST) as a baseline. HITRUST also offers organizations looking to conduct an assessment internally with a self-assessment option to receive a report from HITRUST for third-party attestations (of course an organization may conduct a CSF assessment internally with no report from HITRUST). Still, many organizations may seek the expertise of a qualified IT professional to gain reassurance of the strengths and weaknesses of their security programs and recommendations for how to effectively remediate the gaps identified.

A Comparison of Approaches

The table below provides a comparison of the pros and cons of using HIPAA, HITRUST and many other industry leading standards and frameworks for implementing and assessing security controls.

Consideration	ISO 27001	NIST 800-53	HIPAA Security Rule	PCI DSS	COBIT	HITRUST CSF
Comprehensive – general security	✓	✓	P	✓	✓	✓
Comprehensive – regulatory, statutory, and business security requirements						✓
Healthcare specific			✓			✓
Prescriptive	P	✓		✓	✓	✓
Practical and scalable		P	✓		✓	✓
Audit or assessment guidelines		✓	P	✓	✓	✓
Certifiable with support for third party assurance	✓			✓		✓
Open and transparent update process	✓	✓	✓	✓	✓	✓
Cost to access source documents	$	Free	Free	Free	Free	Free

P = Partial

✓= Addressed

Conclusion

Since the release of the HIPAA Security Rule, healthcare organizations and their Business Associates have struggled to comply with the Rule. HIPAA is subjective, making it difficult to apply and open to interpretation. Since HIPAA is a federal mandate, organizations have found satisfactory solutions through other standards such as ISO and NIST. But with the continued expanding scope of requirements applicable to healthcare—HIPAA Omnibus / Breach Notification, Meaningful Use, State requirements such as Texas, Massachusetts, or Nevada, and many others—reliance on a single standard is becoming too difficult. Organizations must determine the requirements applicable to them based on type, size and regulatory risk, and determine a practical assessment approach, create assessment tools, and prioritize corrective actions.

Professional services firms, such as Coalfire, have been assisting organizations in overcoming HIPAA compliance challenges since the Security Rule was originally released. The experience that third-party professionals bring to their clients serve each in identifying the risks compared with the best practices for becoming compliant with HIPAA and other requirements.

HITRUST, through the CSF, has thoughtfully brought further clarity and guidance to these challenges by providing the healthcare industry with a certifiable framework that incorporates and cross references the requirements of existing standards and regulations while considering organizational risk. Certified HITRUST CSF Assessors, their clients, and the industry as a whole now benefit from an industry-wide methodology to security that also simplifies compliance.