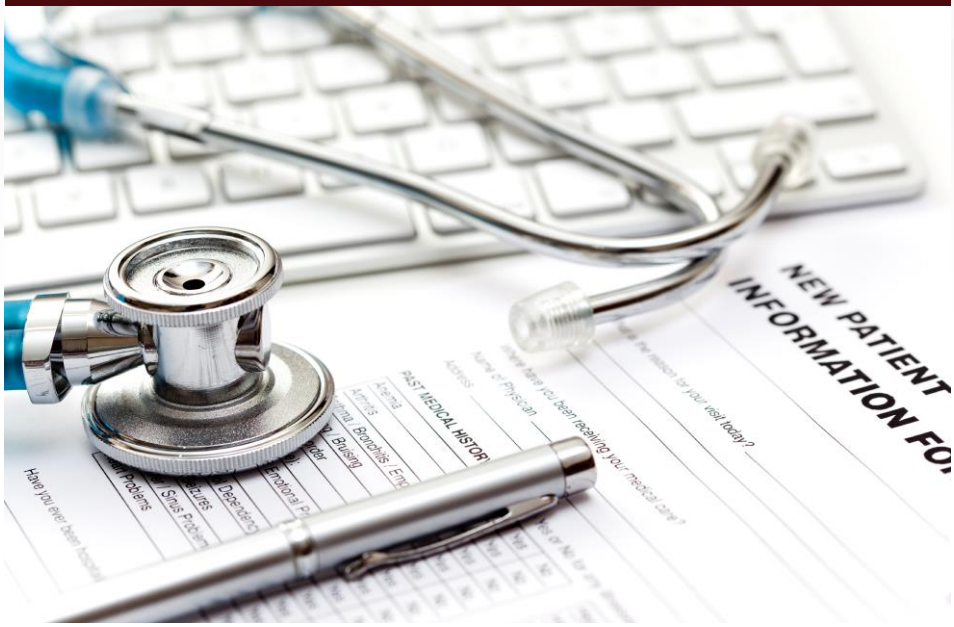
AN EXECUTIVE REVIEW

Managing Cybersecurity Risk in a HIPAA-Compliant World

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

Dr. Bryan S. Cline, CISSP-ISSEP, CISM, CISA, CCSFP, HCISPP
Senior Advisor, HITRUST



Atlanta | Boston | Dallas | Denver | Los Angeles | Orlando | New York | San Francisco | Seattle | Washington, D.C. | UK
877.224.8077 | info@coalfire.com | www.coalfire.com

Introduction

Organizations are at a crossroads when deciding on the proper course of action for compliance with regulations applicable to the healthcare industry and how to manage risk to the security of sensitive health information. 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 risk management and how can you get there? Should you assess your healthcare compliance and risk management posture against the HIPAA Security Rule or should you choose the HITRUST Common Security Framework? What's the difference? What is the most comprehensive risk management solution and which option can help with continuous compliance management needs? 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 help identify the best approach to protecting ePHI and PHI data and developing a solid security and risk management program.

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 type of safeguard includes a series of Standards and Implementation Specifications (or requirements) designed—with the exception of the risk analysis requirement—to address specific 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 services 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) and mobile 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. The Alliance considers security to be critical in realizing the promise for quality improvement and cost containment in America's healthcare system.

Under HITRUST's guidance, multiple healthcare organizations worked together to develop the Common Security Framework (CSF), an industry consensus-standard of due care and diligence that incorporates security controls and requirements from multiple general standards, regulations and best practices applicable to 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: the HIPAA Final Omnibus Rule, Payment Card Industry Data Security Standard (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 for which Covered Entities and Business Associates are already subject. 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:

- **Administrative 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 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 information 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 and report many" by simultaneously meeting multiple compliance and security risk 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 27002:2013
- ISO/IEC 27799:2005
- COBIT 5
- HIPAA Final Omnibus Rule
- Stage 2 Meaningful Use Reqs.
- NIST SP 800-53 Revision 4
- NIST SP 800-66
- CMS ARS 2013v2
- MARS-E v1.0
- IRS Pub 1075 (2014)
- PCI DSS version 3.0
- FTC Red Flags Rule
- 21 CFR Part 11
- Joint Commission (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 Health & Safety Code § 181
- Title 1 Texas Admin. Code § 390.2
- Infrastructure Cybersecurity v1

HIPAA and HITRUST: Addressing Compliance and Security Risk

What is the difference between compliance and security risk?

Regulatory compliance refers to the adherence to laws, regulations, guidelines and specifications relevant to an organization's business. Subsequently compliance risk—or perhaps more accurately the risk of noncompliance—is associated with civil punishment, either through regulatory penalties or possible tort action as the result of negligence due to a general failure to comply with applicable requirements. Typical compliance requirements include legislation such as the Dodd-Frank Act, regulations such as the HIPAA and industry specifications such as the Payment Card Industry Data Security Standard (PCI DSS). Furthermore, in some cases there may be a risk of criminal punishment, as with Sarbanes-Oxley (SOX).

Subsequently, organizations manage the risk of noncompliance simply by complying with the requirements. For example, if a Covered Entity is required to have a privacy officer, then it either has one or it doesn't. It's essentially a 'Yes or No' proposition. For more complex requirements, such as the encryption of sensitive data

on portable devices, an organization could very well be partially compliant if, for example, it cannot demonstrate that all data on devices that contain such information are encrypted. When considering whether or not to comply with a law, regulation, guideline or specification, most organizations typically weigh the operational and financial impact from implementing the requirement against the likelihood of noncompliance being discovered and the subsequent operational, financial and reputational impact. Other types of risk—such as the operational, reputational and financial risks from an actual loss of confidentiality, integrity and availability—are simply not a normal part of the compliance equation. This is generally handled separately as information security risk.

What is HIPAA compliance?

In recent times, "HIPAA compliance" and "HIPAA compliant" have probably been some of the most overused yet least understood terms in the healthcare industry. This is because the HIPAA Security Rule provides numerous standards and implementation specifications for administrative, technical and physical safeguards that, as mentioned previously, lack the prescription necessary for actual implementation by a healthcare organization.

However, this approach was necessary as no two healthcare organizations are exactly alike, which means no single set of information-protection requirements could possibly apply across the entire industry. In other words, one size truly does not fit all. Regardless, this lack of prescription along with a general lack of guidance from Health and Human Services (HHS) and the Office for Civil Rights (OCR) on how organizations should interpret "reasonable and appropriate safeguards" and "adequate protection" resulted in wildly varying information protection programs amongst healthcare entities, including those of similar size and scope. Yet all these organizations likely believed they were "HIPAA compliant" because they had done something around each of the HIPAA standards and implementation specifications. By checking the box (erroneously in some cases) against the general requirements in the Rule's implementation specifications, organizations subsequently checked the box—albeit inappropriately—for the risk analysis without actually conducting one. This position is borne out by the first round of HIPAA audits by the OCR, in which the complete lack of, or inaccurate, risk analysis was the number-one finding.

Further, when asked at the 2014 Health Care Compliance Associate (HCCA) Conference in San Diego, Linda Sanches, Senior Advisor and Health Information Privacy Lead, stated that OCR would not accept an assessment based on the original OCR Audit Protocol developed by KPMG as a valid risk analysis. Although the Audit Protocol addressed each of the Security Rule's standards and implementation specifications, the controls reviewed would not sufficiently address all reasonably anticipated threats, as required by HIPAA. This supports the notion that focusing on the HIPAA Security Rule's standards and implementation specification language is flawed and would not constitute an acceptable risk analysis.

This position also appears to be supported by HHS, which states in their *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* that "conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule." Defining and implementing controls to address the standards and specifications will not ensure

compliance with the risk analysis requirement; but a risk analysis will help ensure compliance with the standards and implementation specifications while also providing the opportunity for organization's to lower their residual risk.

Refer to the papers, *Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection*, and *Risk Analysis versus Risk Assessment – What's the Difference?* for more information.

How do HIPAA and HITRUST address risk?

Both HIPAA and HITRUST help organizations address the multiple and varied risks to ePHI, but they do so in different ways. As previously stated, HIPAA identifies specific information security requirements for Covered Entities and Business Associates in its standards and implementation specifications with one exception—the requirement for risk analysis, which is intended to help organizations implement a complete set of security controls that address all reasonably anticipated threats to the security of ePHI.

HHS' *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* states in its risk analysis that an organization must:

- Scope the assessment to include all ePHI
- Identify and document all assets with ePHI
- Identify and document all reasonably anticipated threats to ePHI
- Assess all current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of a threat occurrence
- Determine the level of risk
- Document assigned risk levels and corrective actions

But as stated previously, most healthcare organizations have difficulty conducting the required analysis. The reasons vary, but often it's the organization's confusion on how to conduct a risk analysis, including their inability to identify all reasonably anticipated threats and determine their likelihood of occurrence and potential impact.

An alternative to this traditional risk analysis approach is to rely on a comprehensive control framework, which is already built on a broad analysis of threats faced by a specific type of organization with specific types of information, using similar information technologies. This is the approach employed by the U.S. intelligence community (IC), Department of Defense (DoD) and civilian agencies of the federal government with their respective information security control and risk management frameworks.

From its inception, HITRUST chose to use a risk-based, rather than a compliance-based approach to information protection and to help mature the healthcare industry's solution to safeguarding information. By integrating

NIST's moderate-level control baseline into the CSF, which is in turn built upon the ISO 27001:2005 control framework, HITRUST leverages the comprehensive threat analyses employed by these frameworks to provide a robust set of prescriptive controls relevant to the healthcare environment. The CSF also goes beyond the three baselines for specific classes of information used by NIST and provides multiple control baselines determined by specific organizational, system and regulatory risk factors. These baselines can be further tailored through normal submission, review and acceptance by HITRUST of alternative controls, or what the PCI DSS refers to as compensating controls. This provides healthcare organizations with additional flexibility in the selection of reasonable and appropriate controls and also provides assurance for the adequate protection of PHI.

The risk analysis guidance from HHS can subsequently be modified to support the use of a comprehensive control framework—built upon an analysis of common threats to specific classes of information and common technologies—as follows:

- Conduct a complete inventory of all ePHI and its location
- Perform a Business Impact Analysis (BIA) on all systems with ePHI (criticality)
- Categorize and evaluate these systems based on sensitivity and criticality
- Select an appropriate framework baseline set of controls
- Apply an overlay based on a targeted assessment of threats unique to the organization
- Evaluate residual risk
    - Likelihood based on an assessment of control maturity
    - Impact based on relative (non-contextual) ratings
- Rank risks and determine risk treatments
- Make contextual adjustments to likelihood and impact, if needed, as part of the corrective action planning process

How do HIPAA and HITRUST support the NIST Framework for Improving Critical Infrastructure Cybersecurity?

The NIST Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") is not intended to provide or replace an organization's cybersecurity program. Instead it offers an overarching set of guidelines to critical infrastructure industries for providing a minimal level of consistency as well as depth, breadth and rigor of an industry's cybersecurity programs. The NIST Cybersecurity Framework relies on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing cybersecurity risk by providing a common language and mechanism to:

1. Describe their current cybersecurity posture
2. Describe their target state for cybersecurity
3. Identify and prioritize opportunities for improving the management of risk
4. Assess progress toward the target state

5. Foster communications among internal and external stakeholders

Technically, HIPAA has always required organizations to address cybersecurity as the risk analysis specification requires organizations to identify and protect against all reasonably anticipated threats to the security and privacy of ePHI and PHI. But as previously discussed, many organizations have focused on implementing compliance-oriented security programs focused on the HIPAA Security Rule's standards and implementation specifications without really doing a real risk analysis (i.e., as described by OCR). As a result, there are significant gaps in the type, number and robust nature of these organizations' security controls. Notable examples include gaps in configuration management, system and services acquisition, and system and information integrity (based on an analysis of the NIST controls that are not mapped to HIPAA in *NIST SP 800-66 rev 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. So if an organization was focused on HIPAA compliance without truly satisfying the intent of the regulation (specifically around the risk analysis requirement), then it would likely not have addressed cyber threats to ePHI, which in today's world poses a significant risk.

On the other hand, the HITRUST risk management framework (RMF), which consists of the CSF, CSF Assurance Program and supporting tools, methods and services, is actually a model implementation of the NIST Cybersecurity Framework for the healthcare industry. As discussed in a recent HITRUST presentation to the Department of Homeland Security (DHS) Cross-Sector Cyber Security Working Group (CSCS WG), the HITRUST RMF maps completely to the sub-categories in the NIST framework and is further supported by an implementation maturity model that also maps to NIST. HITRUST also goes beyond the NIST framework recommendations by providing a fully functional cyber threat intelligence and response program to enable the U.S. healthcare industry to protect itself from disruption by these attacks.

The HITRUST Cyber Threat Intelligence and Incident Coordination Center (C3) is a source of intelligence on threats targeted at healthcare organizations and medical devices, providing actionable information for strategic planning and tactical preparedness and coordinated response for both large and small organizations.

If an organization fully implements the CSF controls duly tailored by its organizational, system and regulatory risk factors, then it will have adequately addressed both HIPAA compliance as well as cybersecurity risk.

HIPAA and HITRUST: Assessing Compliance and Risk

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

While there can be many types of assessments (e.g. gap, validation, and 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 requirements specifically addressed by HIPAA. A HITRUST assessment and certification, 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. Also, neither HIPAA nor HITRUST (when opting for a self-assessment) 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, and NIST) as a baseline. HITRUST 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.

Although HITRUST has worked with the healthcare industry to establish an industry-accepted standard of reporting, various customers—some of whom are outside the healthcare industry—request multiple reporting formats. Since healthcare entities need to be prepared to efficiently respond to all types of requests, HITRUST provides additional flexibility through the "SOC2 for HITRUST" report, which can become the default method of reporting to meet the widest range of requests.

A Service Organization Controls (SOC) Type 2 examination reports on the design, implementation, and operating effectiveness controls at a service organization to address the American Institute of Certified Public Accountants' (AICPA) Trust Services Principles and Criteria (TPA Section 100) related to security, availability, processing integrity, confidentiality, or privacy. A SOC 2 examination is similar in structure and general approach to the SSAE 16/SOC 1 reporting standard (legacy SAS70), but also allows the flexibility to incorporate additional suitable criteria, for example, around adherence to public industry-specific frameworks such as the HITRUST Common Security Framework (CSF). The HITRUST reporting model and the SOC 2 reporting model are subsequently complementary since both are facilitated through the efficient assessment and implementation of

controls to satisfy the CSF. Organizations can therefore use the SOC 2 for HITRUST report as the default method of reporting to meet the widest range of requests.

How do the frameworks compare?

The table below provides a comparison of the pros and cons of using HIPAA, the HITRUST CSF and several 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 government 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 in 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 assisted organizations with meeting HIPAA compliance requirements since the Security Rule was first released. The knowledge and expertise that third-party professionals bring to the table serve to identify the risks in comparison to best practices for becoming compliant with HIPAA and other requirements. In addition, they offer testing services that help secure data with an ongoing proactive approach to monitoring systems.

HITRUST, through the CSF, offers 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, including cyber risk. Certified HITRUST CSF assessors, their clients, and the industry as a whole now benefit from an industry-wide methodology to security that simplifies compliance through a common control, assessment and reporting structure.