



Whitepaper:

HITECH COMPLIANCE SIMPLIFIED

FEBRUARY 2010

866.333.2133
www.solutionary.com

INTRODUCTION

Many news analysts, scholars, and politicians alike are calling the current times the Healthcare decade. President Obama has supported¹ the above notion with his continued calls for healthcare reform and many other initiatives that have been in and out of the news since he took office. This paper discusses the initiative known as the American Reinvestment and Recovery Act (ARRA), signed into law on February 17, 2009. The specific area of the law that is of interest is the Health Information Technology for Economic and Clinical Health (HITECH) Act². HITECH is called by many the law that gives teeth to Health Insurance Portability and Accountability Act (HIPAA) Compliance.

One of the first steps in lowering healthcare costs while maintaining high quality is to adopt and implement Electronic Medical Record (EMR) systems across the industry. As part of this legislation, the federal government has allocated huge incentives for health organizations that upgrade their current paper-based systems to EMR systems; but that's just part of the puzzle. The other part is addressing what keeps the CIO and the executive management of any healthcare organization up at night.

PROBLEM STATEMENT

The first step for all healthcare organizations is to begin provisioning of an EMR system; which is no small task. Upon completing the provisioning phase and the system is in place, the next challenge is to keep the Patient Health Information (PHI) data they store, process, and transmit, secure. HITECH distributes penalties for failures to protect PHI data. Lack of securing systems and data is what will keep executives worrying that their organization will show up in the headlines the next day for the wrong reasons – data theft, loss, or disclosure (i.e., breach).

ARRA also requires a program to oversee the voluntary certification of healthcare IT as compliant with HITECH. Although the details of the compliance standards and the certification process are not standardized at the time of this paper, three independent bodies provide some guidance and help on this issue, albeit in a very different manner.

The Joint Commission³ is the oldest of all and is considered the primary authority on accrediting and certifying healthcare organizations against standards for providing safe and effective care of the highest quality and value.

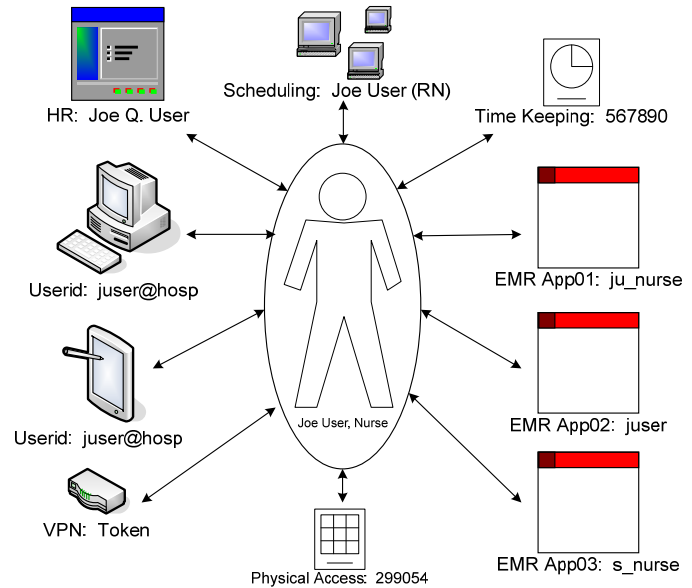
The Certification Commission for Health Information Technology⁴ (CCHIT) is a certification body for EMR products and vendors; its certification process released in October 2009 has been approved as a requirement for all EMR systems under the HITECH Act. In fact, a few EMR systems are already CCHIT 2011 certified. ([Click here](#) to see the list.)

With patient safety and quality being provided for, the need for guidance on how to configure EMR systems to ensure security across the enterprise needs to be properly examined, in other words a framework needs to be applied that provides guidance on not just how to secure the data, but also for the systems that store, transmit, and relay this information. Enforcing common security policies, procedures, and standards across disparate EMR systems used by ambulatory, emergency, inpatient, pharmacy and



various other business units within the organization is no small task. Tracking users accessing PHI sounds straight forward, but how can identities and data access be tracked across applications, systems, and the rest of the infrastructure? Users may have dozens of credentials tied to one actual user, as shown in Figure 1.

Fig 1: User identity(s) at a healthcare organization



Finally, how can the security and compliance of individual systems and the organization as a whole be effectively managed and monitored? Security and compliance have to address every level of the environment starting with people, applications, databases, storage, network and the rest of the infrastructure.

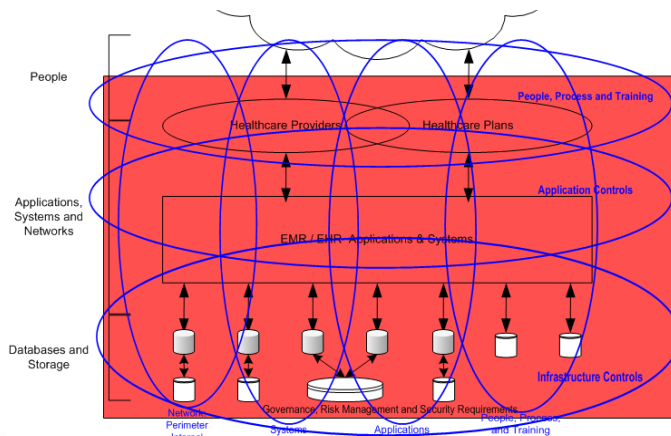
PREVIOUS OPTIONS

After HIPAA went into effect in August 1996, healthcare organizations had some mandate and direction on protecting their Healthcare Information Technology (HIT) infrastructure. There were two major problems with HIPAA: first, it wasn't really enforced and second, it wasn't very specific.

The first problem was solved in April 2003, when the final grace period ended and penalties were levied upon non-compliant organizations. However, the second issue let CIOs come up with their own strategy in implementing and ensuring HIPAA compliance. Those with a long-term vision and executive support adopted a framework such as ISO 27001 (BS 7799) incorporating best practices where possible.

While others used convenient interpretation of the requirements using a minimalist approach, enough to check a box and get by. It became very clear that as far as securing HIT was concerned, HIPAA was not working. As theft of electronically stored PII and credit card data dramatically increased, the Payment Card Industry Data Security Standard (PCI DSS) was created and offered specific guidance and compliance requirements for organizations accepting electronic payments via

Fig 2: Typical healthcare environment

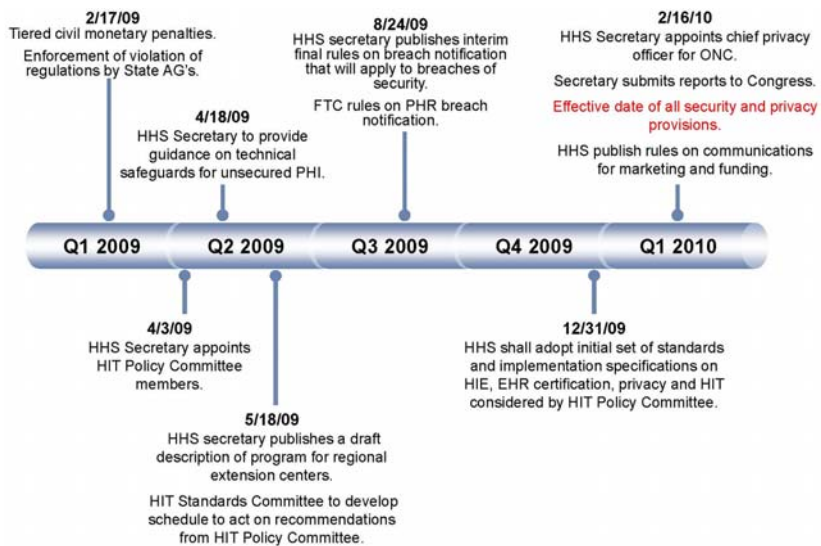


credit cards. State governments and individual industries responded to this increasing problem of unprotected consumer data with local laws and regulations. The healthcare industry attempted to play catch-up with these standards, but could only apply band-aid solutions where they could. Hospitals and healthcare entities are still struggling due to lack of a solid foundation (i.e., framework) that is flexible enough to be applied against all of the above standards. The contributing factor for the struggle is due to a lack of resources (e.g., tools, technology, and people) to monitor and manage the compliance through all the changes and upgrades to existing system components and business areas.

Fig 3: HITECH Timeline⁵

HITRUST Solution

The Health Information Trust (HITRUST) Alliance is a collaboration of leaders representing healthcare, business, technology, and information security industries. Realizing that healthcare organizations may need to comply with many other standards and regulations, HITRUST created a framework, the [Common Security Framework \(CSF\)](#) that can be used by any and all organizations that create, store, access, or exchange PHI, PII or other sensitive information.



On February 11, 2010 HITRUST⁸ [announced](#) that it plans to update the CSF to add support for - State of Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth.

The first security framework for healthcare information, CSF, is **free** for qualified⁶ organizations and intended to be the foundation for all information security and compliance needs of healthcare organizations. In addition to HIPAA and HITECH, the CSF currently supports⁷ industry standards including PCI, CobiT, NIST, FTC, CMS, and ISO 27001 series.

Because CSF was created out of a need for a common set of security guidelines that can be accredited and are certifiable against all healthcare relevant regulations and compliance standards, HITRUST has also created a CSF Assurance program to help simplify the compliance assessment and reporting requirements of HIPAA, HITECH, state, and business associate requirements.

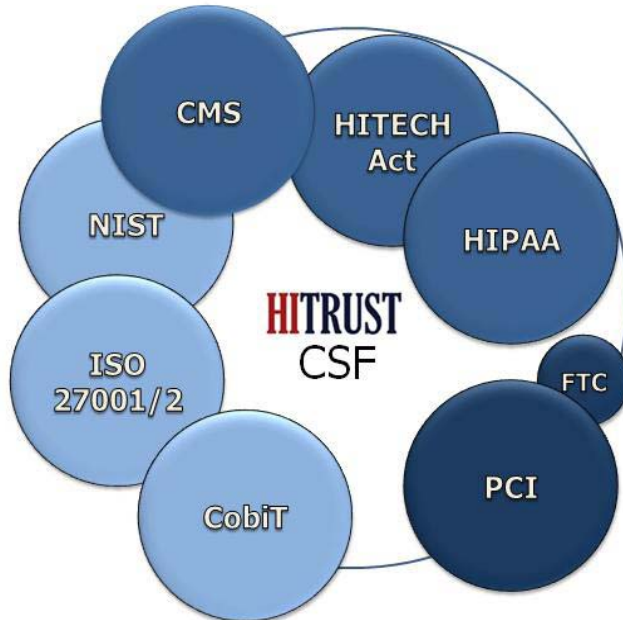


BENEFITS OF HITRUST CSF

Scalable and Flexible

A key strength of the CSF is its flexibility and scalability to organizations of different sizes, business units, etc. It allows a practical and certifiable framework for the largest to the smallest of organizations with the help of sizing questionnaires and justifiable interpretations.

Fig 3: One Framework; Many Standards



As shown in the figure to the left⁹, the CSF framework ([free download](#) for qualified organizations) can not only support all the leading standards and regulations, it also includes cross-references and mappings for items that are common across them. This saves a lot of time and effort spent in re-validating and documenting requirements that are similar across multiple standards.

Assurance Program; Simplified Compliance

In order to assist healthcare organizations further, HITRUST has created a methodology for performing risk assessments. The CSF assurance program is designed to address the unique mix of regulatory and business needs in the healthcare industry.

HITRUST METHODOLOGY	
STEP 1	Scope
STEP 2	Gap Assessment
STEP 3	Remediation
STEP 4	On-going Compliance Mgmt

In addition to the methodology, organizations also have an option to hire certified¹⁰ [CSF Assessors](#) to help in performing gap analysis, documenting findings and generating roadmaps and recommendations for achieving and maintaining a steady HITECH compliance management program.

Community Collaboration – Source of Support and Information Exchange

Although there are many other benefits of using HITRUST services and the CSF, one of the most unique yet proven feature of the HITRUST alliance is the [community collaboration](#) of forums and idea exchange.

The forums¹¹ are used for asking questions and peer discussions. Idea exchange is used strictly for submitting and commenting on new ideas for enhancing CSF framework and HITRUST services.

EXAMPLE POSTS FROM HITRUST CENTRAL	
FORUMS	<i>'IFR comments on security and meaningful use of HIT'</i>
IDEA EXCHANGE	<i>'eClinicalWorks Configuration Pack'</i>

The forums are amazing tools for organizations that need help implementing a new system or even for requesting adding support for a state based regulation that could be potentially useful to other organizations as well.

EXAMPLE APPROACH: ACME HOSPITALS & CLINICS

Following is an abbreviated case study of a healthcare organization (we'll call it 'Acme') facing a similar challenge of HITECH compliance. The study will also briefly showcase how Acme has used this opportunity to go above and beyond the letter of requirements and implemented a combination of tools and techniques that enable the business in providing high-quality service to their customers (internal and external).

CHALLENGES:

Acme Hospitals & Clinics is a world-renowned ~500 bed academic hospital and clinics system that found difficulties in compliance with relatively new but specific standards like PCI and HITECH. Due to the lack of a singular process or foundation, Acme continuing to repeat work efforts, undergoing multiple audits, and scrambling to meet compliance deadlines. The compliance audits also took precious time away from privacy assurance monitoring and investigations.

OBJECTIVES:

- Achieve and maintain compliance with HIPAA, PCI, and HITECH with minimal repetition. Ideally relieve some of the "audit fatigue" from addressing each of these requirements separately.
- Comprehensive event/log management and proactive monitoring of inappropriate or suspicious activities in EMR systems and clinical applications. Tracking users accessing PHI data – who, when, and what – with enough intelligence and supporting information to act on the alerts and reports.
- One-stop shop for security and compliance management to enable better coordination, communication and correlation of incident response and investigations.

SOLUTIONS:

Solutionary, a trusted security advisor¹² of Acme proposed a strategy to better align security initiatives with business objectives.

Acme and Solutionary tackled log management and event correlation first. Using Solutionary's patented¹³ ActiveGuard® technology to provision log aggregation, event/identity correlation, customized real-time alerts, and advanced reporting as a managed solution for EMR and clinical applications.



Using log information from dozens of disparate transactional, contextual, and identity sources, ActiveGuard, “knitted” together these disparate sources and used provided a world-class proactive compliance solution. They combined the healthcare specific solution with ActiveGuard’s core strengths in infrastructure security; taking in log information from operating systems, network devices, and security devices throughout the network.

Acme could then track user access to data from the application, the network, and from the system level. This provided both the compliance and the security teams, proactive tools to get ahead of issues and a powerful data mining capability to research past issues.

Meanwhile, using HITRUST CSF as the core foundation for meeting compliance requirements, Solutionary suggested a comprehensive methodology based on CSF assurance program. The steps included are:

- Scope
- Assessment
- Reporting & Remediation
- Compliance Management

Scoping included identifying the applicable rules and regulations, system components, sensitive data and roles and privileges for accessing the data.

Assessments are effectively gap analyses against one or many standards and regulations that are performed by highly skilled and certified professionals from Solutionary’s consulting services department.

Reporting and remediation involves documenting findings and generating compliance reports as well as creating recommendations and roadmaps for non-compliant items.

Compliance management¹⁴ ensures that appropriate controls (administrative, technical, and so on) are put in place to monitor and manage Acme’s compliance.

Finally, Solutionary created a Acme Health Information Exchange – a secure web portal that can be used by various Acme teams (compliance, security operations, infrastructure, etc) to monitor, respond to, and investigate suspicious behavior seen across the enterprise from firewalls, IDS systems, and other network devices to servers, EMR systems, Clinical applications and user desktops, etc.

BENEFITS:

- Acme will now be able to use one security framework created for Healthcare organizations to measure and meet its compliance requirements with all applicable state, federal, and industry standards, especially HITECH.
- Acme will be able to utilize Solutionary’s award winning managed services platform to collect, correlate, analyze, and alert appropriate stakeholders of suspicious activities in EMR systems and clinical applications.



- Acme will have no additional hardware or software to manage and can use a single online portal to monitor and manage its security and compliance requirements.

SUMMARY

In conclusion, the healthcare landscape is changing across America and as we move towards a paperless and collaborative HIT arena there will be issues and gaps. Some of these challenges will revolve around meeting compliance with regulations created to protect EMRs and some around managing resources to achieve and maintain compliance once it is achieved. To tackle these challenges we recommend that you:

- **Select a framework:** Identify to what extent HITECH applies to you and your business associates and find out if you have a security foundation in place that is flexible and scalable enough to support your HITECH compliance efforts. Optionally, take a look at CSF and other resources¹⁵ provided by the HITRUST Alliance. Most of it is free for qualified healthcare organizations.
- **Evaluate options:** Analyze and decide if there are enough resources – skilled people, appropriate tools and technology to effectively support and manage HITECH compliance. Evaluate all options including in-house solution versus managed services to find the best fit for your organization.
- **Get creative:** Take this opportunity to identify other business objectives such as proactive monitoring, identity correlation, and privacy assurance and find out if any of the high ROI projects can be combined with the above initiative.
- **Engage Trusted Partners:** Engage trusted partners to help fill the resource, skill set, or technology gaps in your environment. Maintaining experts in every discipline is unrealistic; make sure you reach out and engage specialists where and when you need them.

REFERENCES & RESOURCES:

1. The White House Blog: Health Care - <http://www.whitehouse.gov/blog/issues/Health-Care?page=3>
2. HITECH Act Breach Notification Guidance - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html
3. CCHIT, Joint Commission central to health care certification, funding - <http://searchhealthit.techtarget.com/tip/CCHIT-Joint-Commission-central-to-health-care-certification-funding>
4. CCHIT Town Call: New 2011 Certification Programs - <http://www.cchit.org/about/towncalls/commission-seeks-input-2009>
5. Solutionary-Forrester Presentation - HIPAA, HITECH and HITRUST - <http://www.solutionary.com/index/intelligence-center/webinars/forrester-hipaa-hitech-hitrust.html>
6. Understanding and Leveraging CSF - <http://www.hitrustalliance.net/csf/>
7. HITRUST CSF - http://hitrustalliance.net/csf/hitrust_central_information.php
8. HITRUST News Blog - <https://www.hitrustcentral.net/blogs/ht/archive/2010/02/11/massachusetts-data-protection-reg-201-cmr-17-00-csf-authoritative-source-update-request-for-comments.aspx>



9. HITECH FAQs - <http://www.solutionary.com/index/intelligence-center/webinars/forrester-hipaa-hitech-hitrust/forresterwebinar-lp.html>
10. CSF Assessors - <http://hitrustalliance.net/assessors/>
11. HITRUST Central - <https://www.hitrustcentral.net/>
12. Healthcare Compliance - <http://www.solutionary.com/index/compliance/hipaa.html>
13. ActiveGuard technology - <http://www.solutionary.com/index/solutions-and-services/activeguard.html>
14. Solutionary Compliance Management - <http://www.solutionary.com/index/compliance.html>
15. HITRUST Secure Configuration Guidelines for Health Care apps - http://hitrustalliance.net/csf/security_configuration_packs.php

The Author:

Phoram Mehta, Senior Security Consultant, Solutionary, CISSP, CISM, QSA

Phoram's focus is in the areas of enterprise security architecture, compliance program management, and trusted security advisory. Phoram [blogs for Solutionary](#); his posts cover standards and regulations, preparing for audits, and creating and tuning compliance management programs.

About Solutionary

Solutionary is an information security company that delivers a wide range of managed security solutions and professional services to reduce risk, increase security and ensure compliance for medium-to-large businesses.

The company's services are based on next generation security intelligence and offer true security and compliance management. Solutionary provides customers with advanced service delivery, patented technology, thought leadership, years of innovative groundwork and proprietary certifications that exceed industry standards, enabling the company to have one of the highest client retention rates in the industry.

Recognized as a leading managed security services provider by industry analysts Gartner and Forrester, Solutionary maintains multiple 24/7, fully redundant security operations centers.

