



# Securing Electronic Health Records – Defining and Maintaining Compliance with HITRUST CSF

## POWERFUL INSIGHTS

In 2009, only 10 percent of healthcare facilities in the United States used electronic health records (EHRs). By 2014, the government (via the American Recovery and Reinvestment Act/Health Information Technology for Economic and Clinical Health Act, or HITECH) wants more than half of all healthcare organizations and related third parties to use them, and is offering financial incentives to spur the initiative. Physicians who implement EHR systems can receive as much as \$64,000 (depending on Medicare/Medicaid volumes) to help defray technology costs; a typical 275-bed hospital would be eligible for nearly \$6 million.

### Issue

Among the priorities of healthcare organizations, protecting patient information is second only to providing quality care to those patients. A loss of patient data can jeopardize patient care as well as put an organization out of compliance with government and industry regulations. It can also be costly in terms of remediation, regulatory fines and reputational damage. The increasing flow of patient information between doctors, hospitals, insurance companies, pharmacies and other parties only makes protecting it more complicated and vital.

### Challenges and Opportunities

Many organizations are unsure of how to begin – or refine – an EHR implementation. The Health Insurance Portability and Accountability Act (HIPAA) and HITECH provide little specific guidance about EHR-related security controls. Yet increased requirements for breach notification indicate that hackers already are pursuing stolen medical information. Unauthorized use of medical records (medical identity theft) has created a new kind of crime where a criminal poses as another person to obtain medical treatments, using that person's insurance.

This, of course, is not the only security and privacy risk healthcare organizations face. In 2009, a computer hard drive with seven years' worth of personal financial and medical information for 1.5 million customers was stolen from a large managed healthcare company. The hard drive also contained names, addresses and Social Security Num-

bers. This led to active litigation and fines from the affected states as well as the U.S. government.

This organization is not alone. According to a Ponemon study, 80 percent of healthcare organizations have experienced at least one incident of lost or stolen health information in the past year. Almost 70 percent of IT managers said management does not view privacy and data security as a priority, and 53 percent said their organizations do not take appropriate steps to protect patient privacy. Less than half judge their existing security measures as "effective or very effective."

With so much at stake, what should healthcare organizations do to better protect this sensitive information? And given the large and interdependent ecosystem of controlling entities and business associates, what can be done to effectively communicate the information security strength of each of the players among the participants?

### Our Point of View

Healthcare organizations should leverage the Health Information Trust (HITRUST) Alliance Common Security Framework (CSF) when designing and implementing EHR systems. The HITRUST Alliance, in collaboration with healthcare, technology and information security leaders, developed this framework to provide a clear and concise structure to guide health information security initiatives. Created by leveraging existing standards and regulatory requirements, it includes 130 specific industry-accepted security controls. Of note, it complements certification activity already underway in many organizations. It is a logical extension of the HIPAA and HITECH guidance, defining specific control elements to support general guidance those regulations provide.

Adoption of the HITRUST CSF has been rapid and is providing a common understanding and parlance of security strength. Industry leaders including WellPoint and Humana already have announced they will be leveraging the framework internally and accepting CSF certification as evidence of compliance among their business associates. In addition, a majority of healthcare providers have licensed the HITRUST CSF and are in the process of evaluating its use. ➤

## PROVEN DELIVERY

### How We Help Companies Succeed

Protiviti provides security strategy, process and implementation services to help improve an organization's information security needs. With regard to HITRUST CSF certification, we have assisted our clients in three key areas:

- **Gap analysis** – We assess the current state of an organization's information security implementation, compare it to the HITRUST CSF standards and define areas in which changes need to be made.
- **Remediation definition and assistance** – We help define a path to attaining CSF compliance, implement the requisite changes and ensure they are providing the operational value expected.
- **Certification support** – As one of a small number of Certified CSF Assessors, Protiviti has the ability to analyze an enterprise environment and prepare documentation the HITRUST Alliance requires for certification.

Our clients tell us that pursuing HITRUST certification provides several benefits to them:

- **Independent verification** – Verify to patients, partners and members that the organization's information security practices are an imperative and meet industry-defined standards.
- **Risk mitigation** – The organization obtains a clear and comprehensive understanding of its information risk exposure using the CSF.
- **Competitive advantage** – Healthcare organizations want business partners that they can trust to retain and protect their patient information.

### Contact

Cal Slempp  
+1.203.905.2926  
cal.slempp@protiviti.com

Susan Haseley  
+1.469.374.2435  
susan.haseley@protiviti.com

### About Protiviti

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

- **Industry validation** – Rely on the collective decisions of an industry group as validation for which security controls are appropriate for the organization.
- **Improved partner security** – The CSF provides the benchmark by which an organization can measure business associates to quantify the risks of sharing data.
- **Simplified compliance management and reduced audit overlap** – The CSF supports the compliance reviews and documentation of other major security standards, thereby reducing the time spent on overlapping audits.

### Example

Our client experienced a data breach and was looking for help to become compliant very rapidly with new industry security standards. To assist our client, Protiviti's IT Security and Privacy professionals:

- Proposed a remediation approach to reduce scope and cost without compromising security effectiveness.
- Designed and implemented a secure network architecture for the organization.
- Developed 30 policies related to IT processes and performed internal and external network security penetration tests.

Within six months, our professionals had designed and implemented a secure architecture, including secure encryption and tokenization of credit card numbers, intrusion detection, log consolidation and file integrity monitoring. Following the project's completion, Protiviti issued a report validating our client's compliance with industry security standards.