

# The Hi-Tech Balancing Act: *Securely Walking the Tightrope of Patient Care*

October 2009

By John McNeely  
President and CEO  
Sword & Shield Enterprise Security, Inc.



## Introduction

---

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). While the act contains incentives related to health care information technology and for the adoption of electronic health record (EHR) systems, the HITECH Act has also put a premium on privacy and security and effectively expanded the scope and depth of the Health Insurance Portability and Accountability Act (HIPAA) requirements. Health care providers who exchange health information electronically are required to ensure that such information remains private and secure. With changes to the privacy and security provisions of the HITECH Act all covered entities and business associates will be held to a higher standard of accountability.

Health care institutions have a tough job when it comes to security. Not only do they have to address a complex set of regulations for compliance but they also have to deal with the very real day-to-day threats. We have seen institutions that are, by all accounts, “compliant,” yet, despite best efforts, succumb to very real threats and are left to deal with the after-math of protected health information (PHI) data disclosure. The moral to the story is that *compliance does not give you security*. A forward thinking approach is to take a risk-based view of managing security so that your efforts ensure that not only is your organization compliant, but that the modern day threats have been addressed.

The stakes are high. At a time when it is imperative that trust in the use of electronic health records (EHRs) is preserved, the need for entities to address privacy, security, and enforcement concerns is paramount.

## Breach Notification

---

The rules have changed regarding breach notification. The cost of complacency and what the HITECH ACT deems “willful neglect” is high. Previously, HIPAA did not require covered entities to notify individuals of breaches. Now, with the HITECH Act, such notification is required. Consider some of the key changes brought about with the HITECH Act:

- Business associates are now required to notify their respective covered entities of any breaches they experience.
- If a breach involves 500 or more patient records then Health and Human Services (HHS) must also be notified.
- Under certain circumstances the media outlets are required to be notified.
- Notification is required whether the breach occurs internally or externally.

The notification requirements are triggered when “unsecured PHI” is compromised. The definition of what is “secured PHI” and “unsecured PHI” is still being ascertained.

While covered entities have experience dealing with HIPAA requirements, many business associates have not. Many business associates have not undergone risk analysis, policy development, and controls assessments required by HIPAA. This presents a scenario of increased risk to the business interest - not only of the business associates, but also to the covered entities they serve.

## Changes in Enforcement

---

For some time now the consensus view within the health care industry has been that HIPAA has not been rigorously enforced. More focus has been placed on satisfying certification and accreditation requirements by organizations like the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), sometimes leading to “pass the audit” exercises at the expense of truly complying with HIPAA requirements.

With the HITECH Act, provisions have been made for increased criminal and civil penalties. Combined with the fact that not only covered entities but business associates are liable and that HHS is required to conduct periodic audits, the impact of non-compliance has been significantly increased.

## A Risk-Based Approach to Security

---

The tendency by executives and management to address the impacts derived from the HITECH Act may be to simply create new compliance initiatives. While compliance is an important result, forward thinking companies are realizing the stakes are simply too high to gloss over with an audit/compliance checklist and controls cross-walk exercise. *A risk-based approach to*

*enterprise security is required in order to preserve trust, protect brand/reputation, and to ensure security/privacy of PHI while realizing the benefits of EHR systems.*

When discussing a risk-based approach to security we aren't just talking about knowing what patches need to be installed on a router or what security policies need to be developed. Now the discussion is about creating an enterprise-aware framework to provide all levels of the organization with the ability to manage risks in a business-driven and sustainable way. Consider a few of the following benefits to a risk-based approach to security:

- Balances both the requirements of compliance with the critical need of dealing with real security threats;
- Enables a strategic view of managing risk and security instead of a more expensive bottom-up tactical approach;
- Eliminates redundancies in the compliance process; i.e., cost-savings that can be applied to improve infrastructure and healthcare services;
- Enables the ability to automate labor intensive components of assessment and auditing practices;
- Provides a management driven approach to resource allocation for addressing security;
- Reduces costs by spending for security using risk-based decisions rather than simply "perceived need";
- Improves control and visibility through risk management tracking and reporting to give governance boards and management a view of progress against initiatives and ability to determine where adjustments should be made; and
- Preserves and enhances trust with stakeholders and patient care community by securing brand and reputation.

The American Recovery and Reinvestment Act of 2009 ("the stimulus") includes provisions that significantly raises the stakes on the privacy and security for health information. The Act calls for ambitious investments in Electronic Health Records (EHRs) in order to improve patient healthcare and to reduce associated costs. While the goals of improving healthcare nationally is laudable, the reality is that healthcare providers – covered entities and their business associates – are going to be held to a higher degree of accountability to ensure trust in the use of EHR systems and to ensure this use is progressive and no harm comes to individuals through the disclosure or misuse of Protected Health Information (PHI).



A risk-based approach to security offers the “safety-net” organizations need when walking the tight rope of patient care.

---

## ***JOHN MCNEELY***

John McNeely currently serves as the President and Chief Executive Officer for Sword & Shield Enterprise Security, Inc. and is a diversely skilled technology and business professional with more than 20 years of experience in information technology, software engineering, systems engineering, and information security. As an experienced information security professional, John provides consulting for security strategies, IT risk management, and compliance to key federal and commercial accounts. His client list includes US federal agencies, international agencies, and Fortune 1000 companies

John is responsible for establishing and executing the major goals and objectives of Sword & Shield as well as providing leadership, direction, and guidance on corporate activities. John manages, analyzes, and evaluates the effectiveness of all operations; develops and maintains effective organizational structure and personnel to align with corporate strategies in federal and commercial markets; and provides corporate representation to the local community as well as to outside vendors, partners, national organizations, and key clients.

John holds a BS and MS in computer science from the University of Tennessee with additional studies in economics, accounting, business management, and operations research. He holds the following certifications: CISSP, CISM, PCI and QSA.

