HIPAA/HITECH Compliance
The Starting Point for Secure Health Care Services

CORE Security
+1 617.399-6980
info@coresecurity.com
www.coresecurity.com
blog.coresecurity.com
Executive Overview

The health care industry is at a transformational crossroad. In recent years the drive for care quality, patient access and cost containment has driven tremendous IT-led innovation. Compliance and security now go hand-in-hand to ultimately determine a true organizational risk picture. Those organizations that successfully address compliance and security issues can not only avoid millions of dollars in HIPAA risk-assessment audits and security-rule settlements but also earn lucrative incentives as offered under HITECH regulations for demonstrating Meaningful Use of patient health records. To this end, research firm Gartner has forecasted an increase of 4.7 percent in overall IT investment for health care between 2010 and 2015.¹

The keys to success are supporting electronic health record (EHR) and electronic protected health information (ePHI) initiatives with automated, continuous security intelligence and risk assessment that tie together ever-evolving IT security infrastructures. A study by CDW IT Monitor suggests that 55% of IT health investments that were put off in 2011 are slated for actualization in 2012.²

This paper, used in conjunction with the imsmartin whitepaper entitled Information Security Compliance Health Check, describes key capabilities of CORE Security solutions and associated services that assist health care organizations in achieving this endeavor.

Innovation-Driven Industry Regulations are Framed with Rewards and Penalties

The Health Insurance Portability and Accountability Act (HIPAA) was created to confront the rising number of stolen private health information (PHI) incidents. Its companion regulation, the Health Information Technology for Economic and Clinical Health (HITECH) Act, strengthens HIPAA, particularly by raising the financial penalties and adding specific requirements for breach disclosures.

HIPAA mandates that all covered entities must establish administrative, technical, and physical safeguards to protect the privacy and security of sensitive information. Covered entities include providers, health plans, clearinghouses, and their business associates. Health-related institutions must also employ procedures that protect the disclosure of individual personal health information while ensuring the privacy and security of information collected, processed and transferred to other organizations.

The compliance urgency, potential liabilities, and costs are real. Penalties can reach $25,000 per year for violations of a single requirement. Penalties for wrongful disclosure include fines up to $250,000 as well as up to 10 years’ imprisonment. These penalties can quickly add up, as a single incident can trigger multiple violations. Additionally, HITECH permits states to pursue civil charges on behalf of victims in addition to fines for HIPAA violators of up to $1.5 million per year. A recent pilot program by the Office of Civil Rights on HIPAA security enforcement included 303 open cases up and 259 closed cases.

¹Source: Gartner, 'Forecast: Enterprise IT Spending by Vertical Industry Market, Worldwide, 2009-2015, 3Q11 Update
²http://resource.onlinetech.com/2012-health-it-spending-trends/
Health data privacy and security ranked #5 on the Top 10 Health IT Trends of 2011.3

HIPAA has had a major effect on the manner in which health care organizations approach electronic data security, and it continues to be a primary driver of overall IT security strategy for the health care industry. Organizations must work diligently to ensure they meet all appropriate administrative, physical and technical controls to assure the confidentiality, integrity and security of ePHI.

HITECH strengthens and extends HIPAA enforcement and breach disclosure, placing even more attention to the need for information security. Compliance and security are the means to the end: HITECH aims to improve the overall quality of health care, increase patient access, and provide cost containment. This bill allocated $59 billion for health care with $20 billion designated for EHR adoption.

Unfortunately, innovations such as EHRs, mobile devices, and cloud computing have introduced risks and threats to privacy and security—with ePHI being a prime target for cyber criminals. This comes at a time when budgetary and staffing resources continue to come under greater pressure while internal and external security requirements advance rapidly in their volume and complexity.

More information about HIPAA and HITECH can be found in the Information Security Compliance Health Check whitepaper.

Predictive Security Intelligence Enables Vulnerability Management Forecasting

Protecting patient information means more than simply preventing identity theft and other crimes. And, with more than 430 major breaches affecting more than 20 million individuals4, a well thought-out and holistic information security and risk assessment program is critical if an organization is to truly secure ePHI and related data, ultimately implementing safeguards for patient safety and confidential clinical information.

To meet this need, CORE Security offers solutions that equip health care organizations with information to prevent security breaches before they occur and to allow ePHI integrity to be maintained while also ensuring patient safety. CORE Security developed its solutions by partnering with security, audit, and compliance leaders across a wide spectrum of health care providers, payers and other covered entities.

To date, more than 430 major breaches have affected more than 20 million individuals.5

CORE Security also helps health care organizations take a proactive approach to assessing the ability of their infrastructure to protect patient and employee privacy as well as avoid millions of dollars in HIPAA risk-assessment audits and security-rule settlements. The result is a focused, cost-efficient, vulnerability-management and compliance program that aligns resources and budgets to address real business risks.

3 http://resource.onlinetech.com/2012-health-it-spending-trends/
4 As of June 2012
5 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
Using CORE Security solutions and services to carry out comprehensive security assessment across multiple threat vectors—along with a vast library of commercial-grade exploits—health care organizations and their business associates (who also must address HITECH and HIPAA regulations) gain extensive visibility into the cause, effect and prevention of sophisticated data breaches.

The unique attributes of CORE Security’s predictive security intelligence are that it is real-world and goal-based. Most organizations have difficulty keeping track of new, disparate systems and data—making secure infrastructures impossible. CORE Security offers comprehensive asset visibility to help determine if an attacker has access, not just if an employee has rights. Organizations can then ascertain the most at-risk portions of the enterprise (patient data, history, billing) assets, applications and infrastructure.

By allowing health care companies and their business partners to test their IT security standing in direct relation to real-world threats and data breach attempts, CORE Security solutions enable organizations to directly address the HIPPA and HITECH Acts.

In addition, these solutions carry out comprehensive security testing across multiple threat-vectors using a vast library of commercial-grade exploits. This allows health care organizations and business associates to gain extensive visibility into the cause, effect and prevention of sophisticated data breaches—and verify they are maintaining layered defenses and encryption controls required under those regulatory audit guidelines.

**Achieving the Letter of the HIPAA Law is a Must**

There are several categories and individual guidelines that an organization must adhere to if they are to be HIPAA compliant. A number of processes and technologies are required up and down and across the entire IT stack. It is critical that an organization understand the risk they face by not being compliant, and should, in kind, take the time to understand and map out how they will meet each guideline.

CORE Security Vulnerability management solutions address key sections of HIPAA General Security Rule 164.306 which states Covered Entities must adhere to these guidelines:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

Additionally, IT security is addressed in HIPAA rules on Administrative Safeguards 164.308, 164.316 Policy and Documentation, as well as 164.318 Compliance, and 13401: Application of Security Provisions and Penalties to Business Associates of Covered Entities.

Annual Guidance on Security Provisions also calls for HIPAA IT security provisions to provide greater emphasis on enforcement across the entire health care ecosystem.
Experiencing security violations with a failure to adhere to the rules defined in section 13401 which extends the risk landscape to include business associates and covered entities, brings penalties and unwanted annual oversight via the Secretary of Health and Human Services.

The following describes how CORE Security solutions can help organizations become compliant with a number of these guidelines:

<table>
<thead>
<tr>
<th>HIPAA Requirement</th>
<th>How CORE Security Solutions Help</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security standards: General rules.</strong> Covered entities must do the following: § 164.306</td>
<td>CORE Security solutions embody an offensive, real-world approach to assessing the operational security posture, thereby helping security teams understand how actual attacks happen so they can pinpoint exploitable weaknesses in the entire environment before breaches occur. CORE Security solutions also span business-critical assets across multiple vectors—Web, network, client, and endpoints—to reveal chains of vulnerabilities across systems including patient Web portals; hospital or front-office sign-on systems; and back-office systems housing ePHI and EHR.</td>
</tr>
<tr>
<td>Security standards: General rules. (a) General requirements. Covered entities must do the following: § 164.306. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Analysis and Management</strong> Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity. § 164.308(1)(ii)(A)</td>
<td>CORE Security solutions reveal actual, exploitable security threats, allowing health care organizations to safely identify which vulnerabilities are critical, which are insignificant, and which are false positives. CORE Security solutions also add intelligence and prioritization to pinpoint data from scanners and incident logs—identifying what is real to enable informed decision-making. Security teams using CORE Security solutions have been able to reclaim up to 50 percent of their time and effort and redirect this time to remediation and change management.</td>
</tr>
<tr>
<td>Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the general requirements of the Security Rule] § 164.308(1)(ii)(B)</td>
<td></td>
</tr>
<tr>
<td><strong>Security awareness and training.</strong> Implement a security awareness and training program for all members of its workforce (including management). § 164.308(5)(i)</td>
<td>CORE Security solutions help security teams conduct security awareness testing through safe and controlled replication of social engineering threats. CORE offers user-less, client-side testing and risk reporting to test standard desktop builds and identify which groups are most likely for a client-side attack as well as what type of attack would be successful. The user-less and simulation aspect decreases sensitivity in health care organizations by directly testing end users while accomplishing the spirit of security awareness. In addition, CORE Security solutions offer enhanced scalability, enabling security teams to</td>
</tr>
</tbody>
</table>
### Incident management

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. § 164.308(6)(ii)

CORE Security solutions for vulnerability management integrate with industry-leading security incident and event monitoring tools as well as IT governance risk and compliance solutions. CORE Security solutions also combine vulnerability information with incident correlation and deeper risk context about both past and potential incidents. CORE’s risk- and goal-based approach allows security teams to prioritize incidents and vulnerabilities from incident logs in order to convey the business-continuity implication in addition to the compliance implication of an incident to the right stakeholders.

### Re-Evaluation

Perform a periodic technical and non-technical evaluation, ... in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of [the Security Rule] § 164.308(8)

Things change and so do IT infrastructures. New locations, mergers, and initiatives introduce new end points and applications. The typical stance is “we haven’t been breached, so our security is working” is in itself a risk, with validation of the security posture performed infrequently.

CORE Security solutions enable health care organizations to keep pace with vulnerabilities as new network infrastructures are deployed, as applications are upgraded and patched, and as new facilities are added. Continuous, regular and automated assessment helps evaluate the effectiveness of existing security measures while justifying proposed security investments.

### Documentation

If an action, activity or assessment is required by [the Security Rule] to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. § 164.316(b)(1)(ii)

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. § 164.316(b)(2)(ii)

CORE Security solutions generate clear, informative reports that provide data about the targeted network and hosts, audits of all exploits performed, and details about proven vulnerabilities. CORE Security solutions also distill vast amounts of security data into actionable information via heat maps and dashboards that communicate the risk in actual systems and care locations such as patient Web portals; hospital or front-office sign-on systems; and back-office data such as ePHI and EHR.

CORE Security also helps communicate both definitive answers and security trends over time in terms of business brand reputation, legal risks, and patient protection metrics—information CFOs can understand.

### Administrative Safeguards

CORE Security vulnerability assessments offer a
Implement policies and procedures to prevent, detect, contain, and correct security violations. § 164.308(1)(i)

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with guideline §164.306(a) – which essentially states that an organization must define a privacy policy to guard against data theft, implement security measures to protect against potential threats, implement security measures to protect against insider disclosure, and ensure that the workforce are abiding by the rules. § 164.308(1)(ii)(B)

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. § 164.308(1)(ii)(D)

If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. § 164.308(4)(ii)(A)

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. -§ 164.308(4)(ii)(B)

Best Practices to Ensure Compliance and Reduce Risk

While HIPAA and HITECH are clear on the sensitivity of ePHI and consequences of breaches, the security guidelines don’t address all the many different ways that ePHI may be compromised. CORE Security’s vast experience in vulnerability assessment and penetration testing across a wide variety of industries helps health care security teams think ahead so they can proactively take remedial and additional steps where necessary:
Insulate Networks from Unauthorized Mobile and other Devices

One of the most significant challenges faced by many health care organizations today—especially those organizations that operate semi-public facilities such as hospitals and outpatient care centers—is the requirement to support secure network access to a massive range of different computing devices. This includes wireless equipment used in the patient environment as well as mobile devices used by physicians and other staffers.

Organizations must work constantly to ensure that such bring your own device (BYOD) or other unauthorized devices cannot gain access to protected networks or applications without due discovery and similar technical safeguards applied as their traditional segmented network. They must also ensure that established access management solutions are in place and working correctly to prevent inappropriate data exposures.

CORE Security solutions offer comprehensive asset discovery, end-point testing and testing of security controls using a many-layered approach to systematically stay on top of changing and complex environments. CORE Security also helps health care institutions protect themselves against the reality of unauthorized devices coming into their environments by identifying exploitable vulnerabilities that may be open to attack before they can be compromised.

Proactive testing of vulnerabilities also allows organizations to understand and address root-cause issues that could lead to potential malware and botnet infections. This helps prevent sophisticated threats from making the leap from authorized devices onto organization networks.

Limit Unauthorized Insider Activities

Now more than ever, health care organizations are being forced to deal with the potential fallout of unauthorized, unintentional or intentional rogue access of PHI by privileged insiders and other connected staff. This trend is driven by the increasing financial value of such sensitive information on the underground market.

*Only 41 percent of organizations have implemented technical security measures designed to address insider threats.*

A single instance of an unauthorized insider gaining access to individual health records, whether to spy on a celebrity patient or merely check up on a family member, can now result in costly lawsuits, regulatory penalties and even unwanted public relations exposure. By incorporating more frequent, continuous assessment and validation of their IT security programs, health care organizations can limit the opportunity for insider attacks.

---

6 [http://i.zdnet.com/whitepapers/Apani_Aberdeen_Insider_Benchmark.pdf](http://i.zdnet.com/whitepapers/Apani_Aberdeen_Insider_Benchmark.pdf)
Diminish the Impact of Social Engineering

One of the most significant trends to emerge on the cybercrime scene in recent years has been the increasing use of targeted social engineering attacks carried out against specific end users in the name of gaining access to their devices and the protected networks that they access. Health Care organizations are no exception to this reality.

In attacks that have been carried out against everyone from government agencies to tech giants such as Google, cybercriminals have proven that by isolating specific individuals or groups of users, and by targeting them with custom threats that play on their trusted relationships, they can gain access to the most closely-guarded IT networks in the world.

With the increasing value of stolen PHI and electronic payment record information, and the massive, diverse workforces typically employed by large health care organizations, the end user has become a bigger target than ever for attacks that seek to circumvent IT security controls put in place to prevent unauthorized access to sensitive information. Using CORE Security social engineering assessments and scheduled end user testing, organizations can lower their related exposure to these social engineering threats.

Drive Down Web-Based Security Risks

Health Care companies and their business partners are under more pressure than ever to make their electronic data available to many different online applications in order to allow for smooth information-sharing throughout the entire health care ecosystem. This includes providing physicians with up-to-date patient records and enabling fulfillment within various provider payment-processing systems.

While these online applications offer tremendous value in helping health care organizations communicate with all of their varied constituents, Web applications have rapidly become the primary target for advanced hackers and malware programs seeking to infiltrate protected environments to disrupt operations and steal sensitive data.

CORE Security solutions not only test the security of Web applications, but also go deeper into analyzing application vulnerabilities. This allows organizations to take cost-effective remediation actions and to continue to roll out new systems without simultaneously expanding their risks.

Conclusion: Address the Real Risk: Go Beyond the Letter and Spirit of Compliance

Considering the economics of security and compliance, CORE Security understands the reality of IT budget pressures and the need to prove ROI based solely on “something that could happen.” As security leaders, providing justifications for investments in compliance and auditing can prove to be a challenge. To help address this challenge, CORE Security solutions reduce implementation and reporting costs,
enabling the organization to maximize their limited resources while offering actionable information and a more accurate indication of risk posture.

Ultimately, CORE Security solutions enable better risk assessment in the language of the business on assets and applications that matter. Security leaders can communicate that risk to the entire organization in order to drive better security awareness throughout the organization and reduce downtime. CORE Security solutions also offer insights that can position security leaders as partners vs. the naysayers and establish security as a key indicator in overall enterprise performance.