Keeping Up With HIPAA

Reducing HIPAA EPHI Risk Profiles And Addressing Evolving Cyber Threats

White Paper
Executive Summary

The Affordable Healthcare Act and new HIPAA mandates for electronic patient healthcare information (EPHI) protection have placed additional security burdens on the healthcare industry. As healthcare providers, exchanges, and third-party payers increasingly rely on data communications and electronic means for transmitting and storing EPHI, HIPAA compliance now requires greater IT security from end-to-end. More regulations may be forthcoming. Cyber threats to healthcare records are on the rise. Therefore, the healthcare industry should adopt underlying IT security measures that not only provide compliance today, but also are agile enough to quickly respond to any new security threats or regulations.

Unisys Stealth™ enhances HIPAA compliance from both outside and inside an organization. It is an agile, software-based solution for addressing outside threats as well as a broad-based tool for addressing government-mandated standards, secure access, and enabling auditing requirements. Because it is software based, and works below the application layer, it can be non-disruptively deployed and easily adapted to the changing needs and applications of healthcare IT infrastructures.

The Health Insurance Portability and Accountability Act (HIPAA) is a moving target. The law has had three major revisions since its inception in 1996 and many other amendments along its over 15-year tenure. One of the chief complications for healthcare providers was the enactment of the HITECH mandate in 2009 for the complete conversion of health records to electronic format, which expanded the reach and scope of HIPAA.

HIPAA has changed yet again. In a press release issued by the U.S. Department of Health and Human Services on January, 17th 2013 regarding a further omnibus rule, HHS Secretary Kathleen Sebelius said, “Much has changed in health care since HIPAA was enacted over fifteen years ago. The new [omnibus] rule will help protect patient privacy and safeguard patients’ health information in an ever expanding digital age.” A few important aspects of the omnibus rule include:

- Increased penalties for noncompliance based on the level of negligence, with a maximum penalty of $1.5 million per violation
- Strengthened ability of the HHS to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a healthcare provider, or one of their business associates
- Expanded many of the requirements to business associates of entities that receive protected health information, such as contractors and subcontractors

Despite the $24 billion dollars in funds paid out for electronic record conversion and security under the 2009 HITECH Act, healthcare IT lags behind industries that have significant security experience, such as the financial and retail sectors.

In a July 13th 2014 article in Politico, Robert Wah, the head of the American Medical Association, said, “What I think it’s going to lead to, if it hasn’t already, is an arms race between the criminal element and the people trying to protect health data. I think the health data stewards are probably a little behind in the race. The criminal elements are incredibly sophisticated.”

In fact, large medical record breaches have recently been reported. Malicious software introduced into Community Healthcare IT systems resulted in the theft of 4.5 million patient records, including Social Security numbers. According to a survey conducted by the Ponemon Institute in September 2013, some 1.84 million Americans were victims of medical identity theft during that year.

The ramifications of insecure records for patients, healthcare organizations, and even financial organizations are enormous in terms of fines, identity theft, and institutional reputation. For example, the theft of a single patient’s identity—through a complete medical record—can fetch as much as $500 on the black market.

---


v Ibid. Politico.
Potential Healthcare Attack Surfaces

Healthcare IT systems are incredibly diverse, and span many locations in most instances. A variety of applications, storage devices, and operating systems must all work in concert for seamlessly providing patient care and accurately recording and storing patient data. For these reasons, healthcare IT infrastructures may be more vulnerable to attack than traditional business or industrial enterprise systems as they present more vulnerabilities or “attack surfaces” for hackers and/or malicious code to enter their system(s).

• Healthcare Provider and Partner Networks
  The more network applications, shared resources, and connections with provider partners, the more attack surfaces hackers can exploit. As healthcare mandates and requirements require more shared EPHI information, security implementations are rarely uniform. For example, a clinic or doctor’s office may have an entirely different security system than a hospital or healthcare system it must connect with to retrieve or store patient data. Each of these intersections and interconnections are subject to attack.

• Affordable Care Act and Federal and State Exchanges
  Although the roll-out of the Affordable Care Act online exchanges was problematic at first, many problems appear to be remediated, with millions of Americans signing up for coverage online. However, some security analysts are concerned over the lack of consistent or effective security measures across the federal as well as many state-run ACA online exchanges.

• Mobile Healthcare Data
  One unintended consequence of the HITECH Act is the proliferation of mobile computing devices in healthcare environments. Tablets, wireless PCs and laptops, and even smartphone applications are routinely used in doctor’s offices, hospitals, and treatment facilities to quickly record or retrieve electronic data. Despite using secured wireless, many sophisticated hackers have the tools and techniques for intercepting mobile data and/or introducing malicious code over hacked wireless devices and networks.

Patients’ health, identity, and an organization’s financial well-being are at stake. But how can healthcare organizations provide compliant yet agile security without major disruptions to their complex IT infrastructures? How can partners safely and reliably share data? What does it take to more fully secure mobile devices and electronic records?
Unisys Stealth for Preventing EPHI Cyber-Attacks

Unisys Stealth is an innovative, software-based solution that adds proactive security measures to healthcare transactions and data not found in most security solutions today. Stealth takes an active, three-pronged approach to reducing potential attack surfaces and thereby greatly reduces the chance of cyber-attacks. The fewer the vulnerabilities a hacker can see, the less likely healthcare data would be compromised.

The following are ways Stealth strengthens security protection and improves HIPAA compliance:

Cloaking of Systems that Contain EPHI

Devices, such as healthcare PCs, terminals and mobile medical devices, can be cloaked by Unisys Stealth technology—making them invisible to insiders and outsiders who are unauthorized to access, or even see them. IP addresses are the “toe-hold” that virtually all hackers and malicious code need to break into systems. In short, hackers can’t hack what they can’t see. Connections to and from trusted third-party providers, mobile devices, and exchanges are masked.

Connections to and from trusted third-party providers, mobile devices, and exchanges are masked and undetectable to hackers and unauthorized users. By cloaking these potential attack surfaces, sensitive electronic EPHI is better protected from compromise and provides HIPAA compliance.

Encryption of EPHI data in motion

Stealth applies AES-256-bit encryption to all data in motion, both within a healthcare provider’s premises, and most importantly, to and from trusted partners, such as insurance providers and healthcare exchanges. With Stealth, communications between campus-based and remote clinics, for example, is completely encrypted in transit—so even if a hacker stumbled upon a Stealth-cloaked network, or hacked into a network connection, the data would be unreadable, unusable, and useless. In addition, using Stealth encryption/decryption, if hackers attempted to introduce malicious code into the encrypted Stealth data stream, the code would be discarded by the Stealth cryptography because it does not contain Stealth-assigned IP headers. Viruses and malicious code have nothing to attack in the encrypted stream. In this way, encrypted data communications improves any healthcare provider’s HIPAA compliance by making it unreadable to all but trusted parties and partners.

Encrypted data communications improves any healthcare provider’s HIPAA compliance by making it unreadable to all but trusted parties and partners.

Isolation of EPHI records

As an additional measure to its cloaking and encryption, Stealth allows the healthcare industry to deploy highly secure Communities of Interest (COIs) for greater user authentication security. Stealth COIs link endpoints and network connections/interconnections into secure, trusted groups. Stealth COIs are used in conjunction with existing authentication systems with no disruption or conflict. Now healthcare providers can connect with third-party partners, remote offices and devices, and know that they have an additional and consistent COI security layer for sharing sensitive patient data.

Healthcare providers and exchanges can connect with third-party partners, remote offices and devices, and know that they have an additional and improved HIPAA-compliant security layer for sharing sensitive patient data.
Stealth Application to Specific HIPAA Standards

While providing innovative protection against outside attacks and masking potential IT attack surfaces from outsiders, Stealth also supports a number of HIPAA-specific standards for internal operations. Stealth’s inherent attributes, particularly in encryption and data segmentation, can isolate data center strategic assets from unauthorized users within organizations. However, trusted COI users—or groups of users—can be added or deleted with a few simple commands.

Workstation Security and Access Control

Stealth’s unique Community of Interest (COI) network segmentation leverages existing Active Directory, LDAP, or even smart-card technology already in place at organizations. In this way, Stealth adds another layer of security to individuals using workstations to access EPHI. Since Stealth does not work on the application layer, changes in user authentication and access levels are easily changed.

Workstation security, especially in modern healthcare environments where mobile workstations and portable devices are used, is potentially more vulnerable to EPHI data exposure. Stealth, through its Community of Interest authentication, provides an additional layer of user authentication to devices that may be found in public or common areas, such as mobile devices and mobile workstations. While “normal” logons would provide workers with access to generic or system-wide application access, Stealth is designed so that only trusted individuals within a Stealth EPHI COI would have access to patient records. This makes workstations and other devices more secure yet more agile—allowing both generic and EPHI-specific access on one machine/device without the need for expensive physical isolation from the overall healthcare infrastructure or the requirement for multiple logins.

Unisys Stealth provides a broad-based, underlying security framework to meet the following HIPAA demands for security and access control:

Safeguards for workstations: easily assign, review and update authorized users

Because Stealth works with current ID systems, COIs can be easily attached to existing authorized users and their application workloads. Meanwhile, unauthorized users never see data they are not meant to access. Stealth leverages existing authentication and identity management systems, avoiding multiple IDs and logins.

New user access, changed privileges, or even deleted user access across single or multiple applications are handled through a centralized, easy to manage interface. Stealth logs all COI activity, which IT administrators can easily examine to make certain user accesses are appropriate or need updating. User credentials from a Stealth COI can easily be removed or modified for individual applications or from the entire system from one centralized management system with just a few clicks.

Establish an Emergency Access Procedure

Stealth is “disaster recovery aware.” If a system fails, its COI control can recover information from recovered ID sources. In addition, unlike many other systems, Stealth supports multiple secure remote access capabilities, including laptops, remote workstations, or even Stealth-enabled mobile devices. In addition, during the disaster recovery or failover process, Stealth securely encrypts data transmitted during the recovery process.

Automatic Logoff and use of Encryption and Decryption

Stealth, as mentioned, provides FIPS 140-2 certified AES-256-bit encryption. Stealth COI encrypted tunnels can be configured to shut down after a specific period of time.
Audit and Controls
An important requirement of HIPAA compliance is mandatory assessment and auditing of EPHI security. Many third-party assessment and auditing tools are available. But all depend on the quality of audit control log data to provide the necessary mandated HIPAA reporting. Stealth is uniquely suited in helping organizations capture access and audit information and integrate it with multiple analysis and forensic toolsets.

Stealth logs the following information for forensic analysis:
- Opening and closing of every Stealth tunnel
- IP source and IP destination addresses of connections
- Usernames and their COI identification
- Non-COI member access attempts/failures

All log information is aggregated locally, and then forwarded to an organization’s audit repository where it is available for review by audit and forensic analysis teams and tools.

EPHI Data Integrity
Stealth, with its use of encryption and highly secure segmentation, provides a greater level of data integrity than may be found in many organizations. These Stealth attributes protect organizations against the capture of EPHI data during transmission to and from trusted providers, users within a network, or during the use of mobile workstations, devices, or secured, off-site workstations.

Stealth tunnels can only open between Stealth-enabled endpoints, eliminating man-in-the-middle type interceptions. Because Stealth-protected systems are also cloaked from non-COI members, they are non-discoverable by unauthorized sources, significantly reducing the organization’s cyber-attack risk.

Because Stealth is software defined security, as technology and operational environments change, it is easy to adapt Stealth protection. As the infrastructure changes, Stealth will continue to provide a defense-in-depth approach to the evolving network and application topology.

Transmission Security
One of the key components of HIPAA compliance is transmission security, which is especially important in the evolving landscape of ACA exchanges, third-party contractors, and increased use of remote and mobile access to EPHI. Encryption of data in motion and secure segmentations of access to EPHI data and applications are two ways in which Stealth protects data transmission. Stealth executes on any IP network (LAN, WAN, wired, and wireless, over the Internet, etc.) to protect EPHI resources regardless of transmission channel. Any incoming attempt to open a path to a Stealth-protected resource from a non-COI member is discarded, with no acknowledgement. To an intruder, the transmission does not exist. Additionally, all data in motion between two communicating Stealth resources (client-to-server, server-to-server, VM-to-VM, etc.) is encrypted.

Conclusion
HIPAA has changed, and no doubt will continue to evolve in the years to come. With data moving from a doctor’s examining room, to central record storage, to insurers, and many places in-between, it is essential that potential vulnerabilities are protected from compromise. The rise of mobile computing and wireless data distribution must also be tightly secured.

Unisys Stealth, with its innovative cloaking, encryption, and isolation of EPHI data provides a solid foundation for building agile security infrastructures for HIPAA compliance with minimal disruption. If and when HIPAA compliance mandates change, healthcare providers may experience fewer wholesale IT infrastructure reconfigurations if they implement the broad-based security underpinning that Stealth delivers.

Stealth is non-disruptive, works hand-in-hand with existing security solutions healthcare providers and partners may already have deployed, yet adds a critical layer of security protection for patient health information—from both outside threats and internal non-compliance. Cloaking, encryption, and isolation provide a solid foundation for compliance and protection against outside attacks now—and in the future. In essence, Stealth helps healthcare organizations significantly reduce their long-term risk profile in a cost-effective manner.