

Ensure HIPAA Compliance

Solution Brief

Health information has become a priority of the new administration in Washington as President Barak Obama seeks to digitize and make health records available to caregivers in an easy to access, easy to use manner. HIPAA, the Health Insurance Portability and Accountability Act, was created to regulate health providers, insurers and employers by imposing standards for identifying procedure codes and record keeping requirements. The HIPAA Privacy Rule identifies patient health, treatment, and payment records as Protected Health Information (PHI.) The Office for Civil Rights (OCR) is responsible for HIPAA Privacy Rule compliance. The Security Rule establishes requirements for guarding Electronic PHI (ePHI.) It essentially requires any organization that creates, stores, or transacts ePHI to safeguard and control all access to the information. Through 2008 the OCR has investigated 35,788 HIPAA complaints.

by **Richard Stienon**

Chief Research Analyst, IT-Harvest

On July 15 2008, Seattle-based Providence Health & Services reached an agreement with Health and Human Services (HHS) in the first stringent enforcement action spawned by HIPAA. They agreed to adopt a corrective action plan (CAP) and pay \$100,000 in fines for loss of patient data. And in January, 2009, CVS agreed to pay \$2.25 million and implement a detailed corrective action plan in response to an investigation by HSS of the loss of records of millions of health care consumers.

To remain HIPAA compliant, which imposes fines for health organizations not in compliance, strict control over access to patient records must be demonstrated.



Not only are the patient records being protected highly sensitive, but many of the users who have access to them are high-risk as well. High-risk users in health care environments include doctors, pharmacists, and care givers who have legitimate access to individual records but should not be able to access unauthorized systems, databases or files. Additionally, it is important to note that high-risk users also consist of IT operations staff which have administrative access to systems in hospitals and clinics and pose a potential threat to compliance. Vendors of medical equipment, software and even network services also traditionally have unrestricted access to the systems and networks on which ePHI reside and also pose a threat to compliance. The most common scenario is for these operational users to be granted access at a gateway if they are external or at the system level internally. Credentials are often shared as they are assigned to a help desk, vendor support teams, or superusers such as administrators, database analysts, or developers.

To be completely in compliance with the Security Rule provisions of HIPAA all access to systems that contain or process ePHI must be controlled and audited. Best practices dictate that unauthorized access to these systems be prevented proactively.

Service and Network Providers

The system administrators responsible for applying patches, installing software, and maintaining the operating system configuration on hospital, clinic, or medical billing equipment may also have direct access to ePHI. They are not care givers and any exposure of protected health information to technical personnel would result in an incident that could kick off a HIPAA complaint and investigation. Separation of duties and compensating controls that provide a complete audit trail are required.



Vendors and Third Parties

Hospital equipment represents some of the most sophisticated technology in use today. Life support monitors, MRI machines, ultrasound imagers, and even health care administration applications are controlled by computers that require periodic support, maintenance, and updates, often provided by vendors who access the machines remotely or onsite. These systems are password protected but vendors are often granted network access allowing them to see internal systems and potentially access ePHI.

Internal IT Staff

The system administrators responsible for applying patches, installing software, and maintaining the operating system configuration on hospital, clinic, or medical billing equipment may also have direct access to ePHI. They are not care givers and any exposure of protected health information to technical personnel would result in an incident that could kick off a HIPAA complaint and investigation. Separation of duties and compensating controls that provide a complete audit trail are required

"Connections in and out of the enterprise are now managed and insulated by Xceedium, and there is no longer direct access into our network via standard VPN methodology. The granular control over user access minimizes the threat of data being destroyed or tampered with and helps us automate HIPAA compliance cost-effectively."

— Arch Beard, information security officer, Bert Fish Medical Center

Xceedium GateKeeper

Access to these systems must be strictly controlled, contained to authorized areas, and all activity must be logged; and ultimately, an audit trail must be in place. Xceedium's GateKeeper provides this functionality in a hardened appliance that can be deployed in front of these critical systems. With the Xceedium GateKeeper deployed these high-risk privileged users login to the GateKeeper with unique credentials that are bound to the identity of the individual and completely integrated with existing authentication and directory systems. Based on identity each account is limited to only specific back-end resources and applications and, at a granular level, only explicitly defined actions.

By deploying the Xceedium GateKeeper a health care provider can limit access and contain each vendor to specific machines and specific applications on those machines. Administrators, whether remote or local, also would be restricted to only those machines they were authorized to manage. They would be limited to specific administrative tasks or tools and constrained from accessing ePHI systems or databases.

A third party's technical support person's access to an MRI device would allow changes to the operations of that machine but not the reading of any patient data residing on it. All access and activities would be logged, recorded and audit reports would be generated to demonstrate compliance with HIPAA's Security Rule for ePHI.

Network administrators and managed services providers for a health care facility would be granted specific access to firewalls, routers, switches, and IPS devices under their purview. But their access to the network would be controlled and contained to those authorized devices. They would not be able to access systems containing ePHI or penetrate further into the network.

Of the key features of the Xceedium GateKeeper one to note is the ease of deployment with a zero-footprint restrictive access methodology to control all access to internal systems be they network devices or specific applications running on particular servers.

The Xceedium GateKeeper appliances deployed at each location provide the centralized control, tracking of activity, and audit reports that allow a health care organization to impose measures that ensure they are in compliance with HIPAA.

Key Features		Benefits
Controls access with a secure appliance-based platform for high-risk users		Lowers cost of controlling and auditing high risk users
Centrally defines policy and controls access via a single point of ingress		One point of control and management requires less resources
Creates a secure, zero-footprint channel for accessing all components of the IT infrastructure		Fast and effective deployment
Enforces granular authentication and authorization policy		Works with existing directories and identity management infrastructure
Compartmentalizes and contains activities of high-risk users (LeapFrog Prevention™)		Enforces best practices for access control
Monitors and alerts about violations in real time		Monitors and alerts about violations in real time
Remediates by terminating access for the offending party		Includes high risk user monitoring in existing alerting infrastructure
Centrally records all activities in every session		Enforces policy and provides complete audit trail
Easily creates compliance reports for testing of controls		Provides an end-to-end audit trail ensuring accountability
Certifications	CLI	Supported GUIs
FIPS 140-2 Level 2	Telnet, Serial	Windows, Mac, X-Windows
JITC PKI/CAC	Secure Shell (SSH)	HTTP, Citrix, VNC, IP KVM
CC-EAL2, CC-EAL3, CC-EAL4 (In process)	CLI Session Recording	Terminal Services / RDP Graphical Session Recording

