



HIPAA and HITECH Network Assessment and Compliance

360 GRC
Whitepaper



Audit IT, Trend IT, Solve IT

What is the history behind HIPAA/HITECH compliance?

The Health Insurance Portability and Accountability Act (HIPAA) was passed on August 21, 1996. It included rules covering administrative simplification, and making healthcare delivery more efficient. Portability of medical coverage for pre-existing conditions and the underwriting process for group medical coverage were key provisions of the act. It also provided standardization of electronic transmittal of billing and claims information.

Congress recognized that standardizing the electronic means of paying and collecting claims data increased the potential for the abuse of people's medical information. A key part of the act also increased and standardized the confidentiality and security of health data. HIPAA privacy regulations require that access to patient information be limited to authorized personnel, and only the information necessary for a task/procedure be made available to them.

HIPAA/HITECH -- What is it?

HIPAA:

This act, passed in 1996, helps ensure that privacy is maintained in regards to patients' medical records. It also created a set of standards to which all electronic medical records must adhere to.

HITECH:

On February 13, 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), as part of President Obama's stimulus package (The American Recovery and Reinvestment Act of 2009). The HITECH Act made important changes to the Health Insurance Portability and Accountability Act (HIPAA), particularly with regards to the privacy provisions. Part of the HITECH Act is entitled "Improved Privacy Provisions and Security Provisions."

HIPAA/HITECH: What does it mean to you?

Under HIPAA if you are a covered entity (all entities that handle, maintain, store, or exchange private health or patient-related information, regardless of size, including healthcare organizations; employers maintaining health records; health plans; life insurers; most doctors, nurses, pharmacies, hospitals, clinics, nursing homes; and many more) then you are required to comply fully with the standards and requirements of HIPAA.

What is at stake if you don't follow the rules?

Compliance for a covered entity under HIPAA/HITECH is **mandatory**, with violations carrying severe penalties. New enforcement provisions indicate that any approach to meeting the compliance via a strategy of "quick fixes" through technology is unacceptable. Organizations subject to HIPAA must become proactive in their compliance efforts and understand that "voluntary compliance" is no longer the state of the regulatory environment. Specific actions involving comprehensive business process and technology efforts must be undertaken to achieve and maintain compliance in the future. Non-compliance with HIPAA brings risks of FINES, JAIL & LAWSUITS impacting either individuals or corporate entities.

HIPAA HITECH Compliance

A covered entity that is found to be non-HIPAA-compliant will face stiff penalties from the Federal and State government, regardless of whether the network has been compromised. Such penalties can include:

Hefty Fines - Fines apply to persons that willfully neglect to comply with HIPAA. They range from \$10,000.00 per violation to \$50,000.00 per violation. A fine of up to \$1.5 million per calendar year for one “identical violation” can be assessed if corrective action is not taken in the case of willful neglect to comply with HIPAA.

Sole Liability - New rules give Attorney Generals (AG) in every State the ability to sue on behalf of residents of their State against “any person” violating HIPAA in a Federal District court. The rules provide for statutory damages and State AG’s will be able to utilize private law firms to assist in carrying out their obligations under this section of the new rules. New rules significantly increase civil monetary penalties that eliminate previous defenses for non-compliance. For example, a tiered penalty structure is outlined that enables fines to be levied against “persons” that did not know about the need for compliance, up to and not to exceed \$25,000.00 for one calendar year for one “identical violation.”

Criminal Offense - New mandates provide clarification on “wrongful disclosures” and make it a criminal offense of up to one year in prison if one violates the Privacy rule’s authorization requirements.

Loss of client confidence - The loss of business due to an unforeseen confidential data loss or a security breach can be permanent. Data that is destroyed is seen within any industry as a poor business process and the loss of consumer confidence is evident as well.

Data Breach Notification Laws - If the data that was lost is considered confidential and consumer related, it is also classified as a Security Data Breach. That may require a company to conform to any number of Data Breach Notification Laws or risk Federal and/or State penalties. The notification process is very expensive. Current estimates are over \$200.00 per account lost. Also, penalties and fines are starting to increase to unrecoverable amounts.

Increased Compliance Audits - New rules mandate audits for organizations that are subject to HIPAA. The rules enable the Office of Civil Rights within the Department of Health and Human Services on the Federal level to monitor “corrective action plans” in order to enforce HIPAA.

So what are you required to do to comply with HIPAA/HITECH mandates?

Below are specific mandates that covered entities and business associates must satisfy relating to network controls:

- **164.308(a)(1)(ii)(B) - Risk Management** (i.e. verifies that security measures are implemented to reduce the risk of security breaches).
- **164.308(a)(3)(ii)(A) - Authorization and/or Supervision** (i.e. verifies that authorization/supervision are adequate for Personal Health Information [PHI] access).
- **164.308(a)(4)(ii)(B) - Access Authorization** (i.e., verifies that policies and procedures are in place to authorize access to PHI).
- **164.308(a)(5)(ii)(C) - Log-in Monitoring** (i.e., verifies that procedures and monitoring of log-in attempts host IDS).
- **164.308(a)(5)(ii)(D) - Password Management** (i.e., verifies that there is strong password management).

- **164.312(a)(2)(i) - Unique User Identification** (i.e., verifies that a unique ID is assigned to support tracking)
- **164.312(a)(2)(iii) - Automatic Logoff** (i.e., verifies that session termination mechanisms are in place).
- **164.312(a)(2)(iv) - Encryption and Decryption** (i.e., verifies that there is a mechanism for encryption of stored PHI).
- **164.312(b) - Audit Controls** (i.e., verifies that there are procedures and mechanisms for monitoring system activity)
- **164.312(d) - Person or Entity Authentication** (i.e., verifies that there are procedures to verify identities).
- **164.312(e)(1) - Transmission Security** (i.e., verifies that there are measures to guard against unauthorized access to transmitted PHI).
- **164.312(e)(2)(i) - Integrity Controls** (i.e., verifies that there are measures to determine that integrity controls are configured for PHI on transmission).
- **164.312(e)(2)(ii) - Encryption** (i.e., verifies that there are mechanism for encryption of transmitted PHI).

Can an audit be performed on the network to ensure HIPAA/HITECH compliance?

Unfortunately, most HIPAA/HITECH covered entities are not placing much emphasis in complying with the requirements on the network. A minority of covered entities are trying to comply by manually auditing their network configurations or using a home grown script to inspect individual device settings. To ensure 100% compliance, the Information Risk Professional should review each line of every network device's configuration file and try to ensure that it matches the applicable HIPAA/HITECH mandates.

There are several potential risks and problems with these approaches:

- The process can be tedious and time consuming, even in small IT environments. Audits are not performed or only in a minimum number of network devices which can expose non-compliance with the remaining devices.
- This leaves much room for error. It is easy to overlook a device or setting due to the technical nature in which the review is conducted.
- Performing routine audits can be costly and difficult (especially in large environments) in which changes are frequent and thousands of devices must be examined.

Summary

Although some vital differences exist among the various regulations, all share one unifying factor: they all deal with fundamental issues of data security and privacy. In IT, an optimal way to address regulations is first to understand the potential threats and vulnerabilities of the data and the network then create an effective and secure technology solution built on a well-designed infrastructure.

This approach enables an organization to easily deal with any new regulations that become law. Many organizations have invested in well-designed network infrastructures, but they still need an upgrade or a technology refresh to achieve a comprehensive solution to meet their regulatory compliance challenges.

About 360 GRC

360 GRC is headquartered in Manhattan, New York. 360 GRC's management team includes over 100+ years in global enterprise Architecture and over 50+ years in IT Audit and IT Security field in top global organizations.

To learn more, visit www.360grc.com

© 2010, 360 GRC Inc.

The information contained herein is subject to change without notice. The only warranties for 360 GRC products and services are forth in the express warranty statement accompanying such products and services. 360 GRC shall not be liable for technical or editorial errors or omissions contained herein.