COASTAL NETWORKS

HIPAA Compliance Guide

This document provides an overview of the Health Insurance Portability and Accountability Act (HIPAA) compliance requirements. It covers the relevant legislation, required procedures, and ways that your business can achieve compliance.

Important Terms

Covered Entities (CAs)

The HIPAA Privacy Rule refers to three specific groups as covered entities, including health plans, healthcare clearinghouses, and health care providers that transmit health information electronically.

Business Associate (BAs)

A person or organization that conducts business with the covered entity that involves the use or disclosure of individually identifiable health information.

Electronic Medical Records (EMRs)

Digital versions of the paper charts in a clinician's office. An EMR contains the medical and treatment history of the patients in one practice.

Electronic Health Records (EHRs)

EHRs focus on the total health of the patient—going beyond standard clinical data collected in the provider's office and inclusive of a broader view on a patient's care. EHRs are designed to reach out beyond the health organization that originally collects and compiles the information. They are built to share information with other health care providers, such as laboratories and specialists, so they contain information from all the clinicians involved in the patient's care.

Medical Practice Management Software (PMS)

A category of Healthcare Software that deals with the day-to-day operations of a medical practice. Such software frequently allows users to capture patient demographics, schedule appointments, maintain lists of insurance payers, perform billing tasks, and generate reports.

Subcontractor

A person or organization to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Safe Harbor Provision

MSPs and VARs are absolved from risk due to any data breach if the health data handled is adequately encrypted. The encryption processes tested and approved by the National Institute of Standards and Technology (NIST) may be found here; http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

6601 Memorial Highway Suite 309 Tampa, Florida 33615
support@coastal-networks.com
813-434-4819

The new HIPAA rules specifically defines cloud service providers (CSPs) as business associates:

"...document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold."

HIPAA

The United States requirements for securely managing Information Systems in Health Care are substantially governed by federal regulations, specifically HIPAA. The detailed requirements and responsibilities are covered by the HIPAA Omnibus Rule, which was revised in 2013. Initially, these regulations for safeguarding health information applied primarily to health care delivery providers and insurers known as "covered entities".

However, the 2013 additions to the HIPAA Omnibus rule require that "business associates" of these "covered entities" must now also be HIPAA compliant. All existing and new business associates must achieve compliance by September 23rd, 2013. The data covered under this requirement is known as Protected Health Information (PHI).

The new HIPAA rules specifically defines cloud service providers (CSPs) as business associates:

"... document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold."

Thus MSPs and VARs of cloud based services and products are also "business associates" and must also achieve HIPAA compliance. While health care demand for information technology and especially secure storage is vast, MSPs and VARs must have a clear strategy and plans for reducing potential liability.

A summary of the HIPAA Security Rule may be found here: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Electronic Protected Health Information (ePHI)

Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

Under HIPAA, PHI that is linked based on the following list of 18 identifiers must be treated with special care:

- Names
- Dates
- Geographic Identifiers
- Social Security Numbers
- Health Insurance Beneficiary Numbers
- Face Numbers
- Phone Numbers
- Email Addresses

- Medical Record Numbers
- Account Numbers
- Certificate / License Numbers
- Vehicle Indentifiers & Serial Numbers
- Device Identifiers & Serial Numbers
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) Address Numbers
- Biometric Identifiers
- Unique Numbers, Characteristics, or Codes
- Fullface Photographic Images

Business associates must comply with the final rule beginning September 23, 2013.

HITECH Act

Covered entities are liable under the final rule for violations resulting from the acts or omissions of a business associate if that business associate is an agent of the covered entity and the business associate is acting within the scope of the agency arrangement. If the business associate is not acting within the scope of that agency arrangement, the business associate is therefore liable.

A business associate is liable for violations resulting from the acts or omissions of a subcontractor if that subcontractor is an agent of the business associate and the subcontractor is acting within the scope of that agency arrangement.

Business associates must comply with the final rule beginning September 23, 2013. However, there is a special one-year transition period for implementing business associate agreements that comply with the final rule.

Civil penalties for willful neglect are increased under the HITECH Act. These penalties can extend up to $250,000, with repeat/uncorrected violations extending up to $1.5 million.

HIPAA Omnibus Rule

Business associates now include any of the following types of entities:

- A health information organization, e-prescribing gateway, or any other entity that provides data transmission services to a covered entity and requires access on a routine basis to PHI.
- An entity that offers a personal health record on behalf of a covered entity. However, if the personal health record is not offered on behalf of a covered entity, then the personal health record vendor is not a business associate.
- A subcontractor of a covered entity as well as any subcontractor of a business associate, if the subcontractor accesses PHI of the covered entity.
- An individual who creates, receives, maintains, or transmits PHI on behalf of a covered entity.

This rule change also includes subcontractors of business associates and requires the Covered Entity's (CE's) Business Associates to enter into Business Associate Agreements (BAA's) with their own subcontractors who will receive, create, or transmit PHI on their behalf.

HIPAA Safeguards

Under HIPAA, all covered entities and business associates must secure health information data under a prescribed controls framework that provides adequate safeguards for physical facilities, administrative requirements (e.g. adequate security policies), and technical infrastructure.

While health care demand for information technology and especially secure storage is vast, MSPs and VARs must have a clear strategy and plans for reducing potential liability. Steps that need to be taken include:

MSPs and VARs must have a clear strategy and plans for reducing potential liability.

- Ensuring the confidentiality, integrity, and availability of all electronic PHI (ePHI) they create, receive, maintain or transmit
- Identifying and protecting against reasonably anticipated threats to the security or integrity of the information
- Protecting against reasonably anticipated, impermissible uses or disclosures
- Ensuring compliance by internal workforce and sub-contractors

If MSPs are handling or have access to unencrypted ePHI they must also conduct a security risk analysis process to include the following activities:

- Evaluating the likelihood and impact of potential risks to ePHI
- Implementing appropriate security measures to address the risks identified in the risk analysis
- Documenting the chosen security measures and the rationale for adopting those measures
- Maintaining continuous, reasonable, and appropriate security protections

This risk analysis should be an ongoing process where it reviews its records to track access to ePHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to ePHI.

The following sections provide a more in depth scope of the administrative, physical, and technical safeguard requirements needed to be met to protect MSPs, VARs, from liability. Use the checklists to see if your organization meets the necessary standards.

Administrative

Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

- ☐ Risk Analysis: Risk analysis must be an ongoing process to review its records to track access to covered entity ePHI and detect security incidents, periodically evaluate the effectiveness of security measures and regularly reevaluate risks to ePHI. Regular analysis must document the following:
    - Evaluate the likelihood and impact of potential risks to ePHI;
    - Implement appropriate security measures to address the risks identified in the risk analysis;
    - Document the chosen security measures and, where required, the rationale for adopting those measures; and
    - Maintain continuous, reasonable, and appropriate security protections.

  NIST 800-30 details how to conduct a security risk analysis: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

- ☐ Risk Management: Implement measures sufficient to reduce these risks to an appropriate level.
- ☐ Sanction Policy: Implement sanction policies for employees who fail to comply.
- ☐ Information Systems Activity Reviews: Regularly review system activity, logs, audit trails, etc.
- ☐ Officers: Designate HIPAA Security and Privacy Officers.
- ☐ Employee Procedures: Implement procedures to authorize and supervise employees who work with PHI, and for granting and removing PHI access to employees.
- ☐ Business Associate & Sub-Contractor Agreements: Have special contracts with business partners who will have access to PHI to ensure that they will be compliant.
- ☐ Organizations: Ensure that PHI is not accessed by parent or partner organizations or subcontractors that are not authorized for access.
- ☐ ePHI Access: Implement procedures for granting access to ePHI and which document access to ePHI or to services and systems which grant access to ePHI.
- ☐ Security Reminders: Periodically send updates and reminders of security and privacy policies to employees.

- ☐ Protection against Malware: Have procedures for guarding against, detecting, and reporting malicious software.
- ☐ Password Management: Ensure there are procedures for creating, changing, and protecting passwords.
- ☐ Login Monitoring: Institute monitoring of logins to systems and reporting of discrepancies.
- ☐ Reporting: Identify, document, and respond to security incidents.
- ☐ Contingency Plans: Ensure there are accessible backups of ePHI and that there are procedures for restore any lost data.
- ☐ Contingency Plan Updates and Analysis: Have procedures for periodic testing and revision of contingency plans. Assess the relative criticality of specific applications and data in support of other contingency plan components.
- ☐ Emergency Mode: Establish procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

EHRs are designed to reach out beyond the health organization that originally collects and compiles the information.

Physical

Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

- ☐ Contingency Operations: Establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- ☐ Maintenance Records: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security.
- ☐ Facility Security: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- ☐ Access Control: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
- ☐ Workstations: Implement policies governing what software can/must be run and how it should be configured on systems that provide access ePHI. Safeguard all workstations providing access to ePHI and restrict access to authorized users.
- ☐ Media Movement: Record movements of hardware and media associated with ePHI storage. Create retrievable, exact copies of electronic protected health information, when needed, before movement of equipment.

- ☐ Devices and Media Disposal and Re-use: Create procedures for the secure final disposal of media that contain ePHI and for the reuse of devices and media that could have been used for ePHI.

Technical

- ☐ The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
- ☐ Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.
- ☐ Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
- ☐ Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- ☐ Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information when deemed appropriate.
- ☐ Emergency Access: Establish procedures for obtaining necessary electronic protected health information during an emergency.
- ☐ Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- ☐ Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is transmitted over an electronic communications network.
- ☐ ePHI Integrity: Implement policies and procedures to Protect electronic protected health information from improper alteration or destruction.