HIPAA Compliance White Paper

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPPA) requires national standards for electronic health care transactions and code sets, unique health identifiers, and security.

HIPAA is a U.S. federal standard, so it's only applicable to entities operating in the United States, but depending on the jurisdiction of your covered entity you may have to comply with other countries standards, such as Canada's PIPEDA.

Secondly, be wary of only achieving HIPAA compliance and assuming that compliance is finished. Many states have more stringent privacy rules for health information than the federal HIPAA. Finally, unlike some regulations, HIPAA compliance is not optional and failure to comply can result in expensive fines.

What is Protected Health Information (PHI)?

PHI is any identifiable information that a HIPAA covered entity collects, uses, or stores.

This includes: names, phone numbers, fax numbers, email addresses, Web URLs, IP addresses, Identifying photos, biometric identifiers, geographical data, dates (except year), social security numbers, vehicle identifiers, device identifiers, any unique codes or numbers (account numbers, health plan beneficiary numbers etc.)

The Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information") and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

The Privacy Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization.

The Privacy Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.

The Security Rule

The Security Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Covered entities need to implement security specific safeguards to protect the confidentiality, integrity, and availability of PHI.

Administrative Safeguards include policies and procedures that protect a covered entity against a breach. These safeguards ensure that physical and technical protections are working. They cover everything from training to documentation processes.

Physical safeguards include policies for physical access, locations of workstations and servers, among many others. These safeguards physically protect PHI.

Technical safeguards focus on technology and reducing unauthorized access to electronic PHI. Typically, a covered entity will conduct a risk assessment to determine which policies are relevant to them.

The Security Rule includes an evaluation standard requiring covered entities to perform periodic technical and nontechnical evaluations

Who must comply?

HIPAA-Covered entities include health insurers, health care providers, health plans, health care clearinghouses, and their business associates.

Risk Assessment & Management

Covered entities must ensure that they comply with HIPAA Standards. This includes the following annual self-audit requirements:

1. Security Risk Assessment
2. Security Standards Audit
3. HITECH Subtitle D Audit
4. Asset and Device Audit
5. Physical Site Audit
6. Privacy Assessment

Risk Assessments are a crucial part of countless cybersecurity certifications. The Security Risk Assessment helps evaluate your covered entity's specific risk level.

Next Steps

Following each audit, a remediation plan should be developed to address the gaps identified in your organization's system that leaves Protected Health Information unprotected and susceptible to data breaches. The remediation plan should assign roles and responsibilities to specific company staff, alongside a timeline for completion of the remediation efforts. The remediation process must be documented to ensure that compliance measures were addressed effectively.

Policies and Procedures

Covered entities industry must have policies and procedures that address the unique qualities of the organization. The goal of policies and procedures is to protect PHI from data misuse and cyber-attacks, as well as protect the organization from liability in the event of a HIPPA violation. Policies and procedures must address each HIPAA standard. If a covered entity's policies and procedures are not tailored to the needs of the covered entity, then the covered entity is left unprotected in the event of a HIPAA violation.

After policies and procedures are written and implemented across the covered entity, employees must be trained to comply with these policies and procedures. Employee training must occur annually.

Furthermore, a signature of attestation for each policy is required for all employees. When onboarding new employees, policy and procedures training must be part of the onboarding process.

Vendor Management & Business Associates

Covered entities must also ensure that their vendors have security measures in place to protect PHI. These vendors that access, transmit, or disclose Personal Health Information are considered Business Associates. As a result, the two organizations are required to have a specific Business Associate Agreement. This agreement involves an in-depth analysis and review of the vendor's security processes to determine any potential risks.

The covered entity must send vendor questionnaires to the Business Associate to assess their practices and identify any security gaps. It is suggested that covered entities mandate that Business Associates create and implement their own remediation plans to address any identified gaps before PHI is shared between the covered entity and vendors. Both parties are responsible for their own HIPAA compliance and could be held liable in the event of a data breach.

Breach Notification Rule

In the event of a data breach, covered entities must have incident management plans in place to minimize the impact of the data breach and properly report required information to the appropriate parties. The HIPAA Breach Notification Rule mandates that covered entities report breaches to the Department of Health and Human Services, along with affected individuals.

If a Minor breach occurs (affecting less than 500 individuals), the covered entity has until the end of the calendar year to report the incident. It is not required to report the incident to the media. If a Meaningful breach occurs (affecting more than 500 individuals), the covered entity has 60 days to report the incident to Health and Human Services and the media. In the event of a data breach, the Office for Civil Rights (OCR) may open an investigation. If a covered entity has outdated information for 10 or more affected individuals, they most post the notice on their webpage for at least 90 days or provide it in major print or broadcast media.

Enforcement & Fines

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR) is responsible for enforcing HIPAA. They do so by:

1. Investigating HIPAA violation complains that have been filed with it;
2. Conducting compliance reviews of covered entities to ensure compliance;
3. Educating and providing outreach to covered entities and promoting compliance with HIPAA requirements.

The OCR also publishes a list of entities online that they are currently investigating.

Fines

Violations range from $100 - $50,000 or more per violation. The cost is dependent upon when the violation occurred, whether the organization should have known about its failure to comply, and whether it was caused by willful negligence.

Corrective Action Plan

After fines, noncompliant covered entities must adopt a corrective action plan that brings policies and procedures up to HIPAA standards, which can be incredibly impactful to a covered entity's productivity and financial resources.

HIPAA + SOC 2

Because HIPAA is not an auditable framework, many covered entities request a SOC 2 report from vendors to ensure that security best practices are being followed.

Useful Resources:

https://www.hhs.gov/hipaa/index.html

Privacy Rule https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Security Rule https://www.hhs.gov/hipaa/for-professionals/security/index.html

Enforcement Rule https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html

Omnibus Rule https://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html

Breach Notification Rule https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html