5 KEY ELEMENTS FOR AN EFFECTIVE HIPAA PROGRAM

ISOutsource

A Modern Technology Consulting Firm

5 KEY ELEMENTS FOR AN EFFECTIVE HIPAA PROGRAM

TABLE OF CONTENTS

Introduction

A 1996 federal law created the Health Insurance Portability and Accountability Act (HIPAA). The new legislation created national patient record protection standards, protecting patient data from disclosure without the patient's consent or knowledge. Additionally, the US Department of Health and Human Services implemented the HIPAA Privacy Rule to protect a subset of information. Together HIPAA and the Privacy Rule protect patients' data through a series of laws, rules, and guidelines for covered entities and Business Associates.

Being HIPAA compliant can be tricky, costly, and overwhelming for covered entities (typically medical providers) or Business Associates. Functional, operational, and technical requirements are challenging to correctly implement, leaving patients' Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) exposed due to the complexity and costs associated with managing requirements. Daunting regulations mixed with constantly changing technical environments challenge even the most seasoned security professionals, compliance officers, and support teams.

A Strategic Approach

The internet abounds with HIPAA information and recommendations; the plethora of suggestions are overwhelming. A quick internet search of "HIPAA basics" reveals millions of search results, ranging from government requirements to implementation applications. Many of the top search results promise to "simplify HIPAA"; however, most don't answer the question "HOW?"

The HOW is answered by creating a balanced, strategic approach. The following five key elements address the primary components of HIPAA compliancy. Each element should align with organizational requirements, this applies to covered entities and Business Associates.

1 CREATE A FORMALIZED PROGRAM

A formal approach puts your organization on notice that you are serious about compliancy; formality leads to accountability. Your formal program should focus on enhancing operations while preventing HIPAA violations. Be intentional, seek improvements, and keep it up to date.

Documentation. Create a HIPAA and cybersecurity library with policies and supporting documentation.

Staffing. Staffing models differ between organizations; however, three basic guidelines exist. Shortcutting requirements and guidelines lead to incomplete programs placing PHI and your organization at risk.

- **Dedicated Roles.** Larger organizations often have specific HIPAA Security, Privacy, and IT Security Officers. The specific title and duties vary based on organizational structure and risk requirements.
- **Separation of Duties**. It is difficult to obtain compliancy if the same person is creating, implementing, and validating the HIPAA program. Even the smallest organization should separate tasks amongst different people.
- **Checks and Balances.** Create an internal audit program, testing and validating those activities that are occurring. If your organization does not assign people to dedicated roles completing separate and distinct duties, consider partnering with a third-party vendor to serve as your internal auditor.

Perform Periodic Self-Audits. Track your results and manage your deficiencies.

Validate all aspects of your technical environment. It is not enough to simply use technology-enabled solutions to store your ePHI, you need to ensure your entire environment is secure.

- Include all data, all solutions, all hardware, all networking, and all communication methods in your HIPAA program.
- Be strategic, right-size your program for your organization.

- Adopt a strategic approach to cybersecurity and technology.
- Focus on business/patient enablement, not a series of rules restricting systems.
- Prevent ePHI from leaving protected systems; it is common for users to save ePHI to local computers or unsecured shared files storage systems.

Ensure Patient Data Portability. Basic requirements establish the need to exchange data in the standardized format between systems, allowing for patient data exchange.

- Read beyond the definition to discover threaded requirements such as "need to know" rules and disclosures.
- Portability requirements include data in transit protections.

Strategic Partnerships – Do not attempt to create a strategic HIPAA program yourself. Align with HIPAA service providers that fully understand and practice HIPAA compliance.

- Partner with software or SaaS providers built for HIPAA purpose.
- Leverage a partner to conduct periodic technical and functional assessments.
- Leverage a third-party training partner that has specific HIPAA curriculum with the ability to add your specific training requirements, train constantly and consistently.

2

HIPAA REGULATIONS AND OTHER REGULATORY REQUIREMENTS

It is important to know, implement, and conduct periodic assessments to ensure that you are compliant with HIPAA regulations and other regulatory requirements. The following list outlines the general standards of federal requirements. Check with your local state, county, or city for local requirements.

ADMINISTRATIVE – 45 CFR §164.308 series – The active management and reporting of HIPAA programs.

PHYSICAL – Physical – 45 CFR §164.310 series – Physical protection for facilities, workstations, mobile devices, and other hardware.

TECHNICAL – Technical – 45 CFR §164.312 series – Technical mechanisms to manage access, authentication, encryption, and logging for ePHI data. Do not limit your technical controls to items listed in 45 CFR, include other relevant cybersecurity practices.

OTHER RECOMMENDED SAFEGUARDS ORGANIZATIONAL – 45 CFR §164.314 & §164.316 series – Business Associate management and operationalizing programs.

KNOW THE HIPAA LEGAL REQUIREMENTS – Failure to comply carries significant financial penalties based on severity, intent, and knowledge; fines range from a few hundred to almost two million dollars. Full rules and penalty criteria are documented in:

- The Enforcement Final Rule of 2006
- The Ominibus Rule of 2013
- HITECH (Health Insurance Portability and Accountability Act) of 2013.

3

MANAGE BUSINESS ASSOCIATES

The HIPAA Privacy Rule only applies to covered entities, which includes health care providers, clearinghouses, and health plans. The Privacy Rule allows covered entities to disclose HIPAA data to Business Associates.

Business Associates are organizations providing ancillary services outside of patient care that have access to protected PHI. This includes claims processing, administration, billing, benefits administration, legal services, practice management, and other support tasks.

Covered entities must obtain satisfactory assurances that the Business Associates use the PHI for the purposes stated in the contract. The covered entity is accountable for Business Associates' activities and is required to take reasonable steps to cure breaches or end violations. You must create and maintain contracts with all Business Associates; contracts must contain all requirements specified in 45 CFR 160.103, 45 CFR 164.502(e) and 164.504(e). Several exceptions and special situations may change your requirements for Business Associate contracts rules, see the rules for complete details.

Business Associate Contract

Covered entities must maintain a contract with all Business Associates. The HIPAA Security Rules includes the following paraphrased contract guidelines; refer to the regulation for the complete language.

1. Permitted and required uses and disclosures.
2. Prohibit future disclosure.
3. Implement safeguards.
4. Report any use or disclosure of the information not provided for by its contract, including breaches or exposure of PHI.
5. Disclose PHI upon patients request.
6. Follow HIPAA Privacy Rule.
7. Disclose HHS practices upon request.
8. Return or destroy all PHI upon contract termination.
9. Ensure all subcontractors agree to the same restrictions and conditions.
10. Contract will be terminated if the Business Associate violates material terms.

REFERENCES

- https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html
- 45 CFR 160.103
- 45 CFR 164.502(e)
- 45 CFR 164.504(e)

4 DOCUMENT

Standard 45 CFR §164.308(a)(1)(i) stipulates "Security Management Process. Implement policies and procedures to prevent, detect, contain, and correct security violations." The regulation contains implementation specifications addressing a myriad of written documentation, additional standards, and management standards.management standards.

Common Documentation includes

Policies – Document expected behaviors for users and IT staff members for the treatment of all IT, data, and cybersecurity systems.

Practices/Standards/Procedures – The expected implementation of policies.

Risk Assessments – Include identification, impact assessment, remediation planning, and reporting.

Self-Assessments – A method of internally validating all policies and procedures for effective implementation and operation.

Business Continuity – A program addressing an interruption in business processes, this expands beyond technology into business processes.

Disaster Recovery – Plans to recover technology systems after a failure or incident.

Incident Response – The response to technical or cybersecurity attacks or incidents.

Vendor Management – A method to identify, track, and manage all vendors.

Business Associate Program – A program to identify, track, and manage all Business Associates.

5

TRAINING

Programs, policies, and standards are not effective unless you teach your users about their rules and responsibilities. Do not try to force all learning into a single session; instead, create an effective training program that is constantly training and implementing your culture and programs. Consider all aspects of user roles and responsibilities, and tailor training to specific needs.

TRAINING TOPICS – The following list of common training topics illustrates:

General HIPAA Rules – Teach, refresh, and update users on personal and organizational HIPAA requirements and responsibilities.

Acceptable Use Policy – Create a policy stating how users may use your technology systems, applications, solutions, and ePHI. Ensure that they know the rules through periodic training and messaging.

Role Based Activities – Increase your training effectiveness by customizing training materials aligned to specific roles and responsibilities. Help users understand how the rules directly apply to them and their roles. Ensure that all users receive training on the applications and system related to their roles.

Cybersecurity – Train on specific cybersecurity topics that resonate with users, such as phishing, email fraud, and internet fraud.

Organization Specific – identify topics that are specific to your organization; ensure users understand how to protect ePHI, the organization, and themselves.

Bonus Tip: Do not attempt to develop and ensure HIPAA compliancy as a standalone organizational program; consider partnering with trade associations, professional peers, and third-party vendors.

AVOIDING COMMON HIPAA PROGRAM PITFALLS

The complexity of HIPAA rules creates pitfalls for organizations from the smallest covered entities and Business Associates to the largest enterprises. The introduction of the HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009 further complicates matters. Keep a keen eye on potential pitfalls, and implement common solutions to help you avoid potential pitfalls.

PITFALL – Creating non-HIPAA compliant Technical and Cybersecurity systems

SOLUTIONS

- Create and document specific HIPAA requirements; include checklists for period validation.
- Ensure that all devices are physically and technically secured.
- Implement encryption with Multi-Factor Authentication (MFA) controls, even on devices not leaving your facility.
- Create a robust Risk Assessment based on your current business and compliance requirements.
- Do not allow any non-controlled devices, especially personally owned devices, access to any system containing ePHI
- Do not rely on your cloud provider to be compliant; double check its HIPAA program. Many providers have methods to secure the environments, but still require you to complete the necessary HIPAA security setting.
- Remember, no organization is too small to audit.

PITFALL – Failure to manage data according to HIPAA requirements

SOLUTIONS:

- Create a comprehensive Vendor Management program; include due diligence activities such as data classification, HIPAA requirements, and technical requirements.
- Know, document, and classify all data, storage, and usage systems (data at rest, transit, and transaction).
- Digitally validate ePHI systems on all local system and end user devices.
- Respond to ePHI requests in a timely manner.
- Destroy physical and digital data in accordance with HIPAA requirements.
- Send data breach notifications in accordance with HIPAA requirements.

PITFALL – User activities that are not HIPAA compliant

SOLUTIONS:

- Ensure that staff are trained and prepared to handle ePHI.
- Conduct periodic training.
- Include topics such as
- System usage and cybersecurity hygiene
- Social Breaches – e.g. talking about patients outside of appropriate professional contexts
- Employee curiosity
- Password management
- Messaging ePHI
- Accessing and storing ePHI from and on unauthorized locations
- Periodically test your users on HIPAA and cybersecurity practices.
- Create a culture that encourages employee honesty and integrity.

PITFALL – Not managing Business Associates Agreements (BAA)

SOLUTIONS:

- Maintain an active roster of all Business Associates.
- Include elements specified at 45 CFR 164.504(e) in the contract or other written arrangement with Business Associates.
- Require all Business Associates to use appropriate safeguards to prevent the use or disclosure of the PHI other than as provided for by the contract.
- Periodically review BAAs.

PITFALL – Trying to be HIPAA compliant alone

SOLUTIONS:

Create a partnership of resources. This includes industry associations, professional peers, and third-party support vendors.

Include government resources in your program

- HIPAA for Professionals: https://www.hhs.gov/hipaa/for-professionals
- Security Rules: https://www.hhs.gov/hipaa/for-professionals/security
- NIST based HIPAA Security Rule Toolkit https://csrc.nist.gov/projects/security-content-automation-protocol/hipaa
- Business Associate Guidelines https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates

Summary

Becoming HIPAA compliant is not easy nor is it quick. It requires time, money, operational changes, and technical/cybersecurity improvements with executive sponsorship. Being HIPAA compliant requires cultural shifts and dedication by your entire organization (including Business Associates).

Be strategic, and create a HIPAA based program that aligns with business requirements. Constantly validate compliancy through self-assessment and train your users. And finally, do not attempt to do it alone; seek professional help to create and maintain your program. Following these steps will help ensure that your organization is HIPAA compliant, while protecting your organization from operational, financial, and reputational risks associated with a breach.

ISOutsource

A Modern Technology Consulting Firm

www.ISOutsource.com