HIPAA INSTITUTE

Achieve | Maintain | Inculcate | Track

HIPAA DOCUMENTATION CHALLENGES:

How to Ease the Burden of Compliance

www.hipaainstitute.com

Content:

Introduction

What is HIPAA?

- To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 was enacted by Congress.
- HIPAA sets standard for protecting sensitive patient data
- Covered entities and business associates need to protect the privacy and security of protected health information (PHI)

Part 2: HIPAA Rule

What steps need to be taken in order to become HIPAA compliant?

Covered Entities and their Business Associates need to protect the privacy and security of protected health information (PHI).

There are 4 rules one need to dissect:

1. HIPAA Privacy Rule
2. HIPAA Security Rule
3. HIPAA Enforcement Rule
4. HIPAA Breach Notification Rule

The Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires

appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The security rule is made up of 5 parts:

1. Administration Safeguards
2. Physical Safeguards
3. Technical Safeguards
4. Organizational Requirements
5. Policies and Procedures and Documentation Requirements

1. Administrative Safeguards

A. **Security Management Process.** As explained in the previous section, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

B. **Security Personnel.** A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

C. **Information Access Management.** Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).

D. **Workforce Training and Management.** A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

E. **Evaluation.** A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule

2. Physical Safeguards

A. **Facility Access and Control.** A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

B. **Workstation and Device Security.** A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

3. Technical Safeguards

A. **Access Control.** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

B. **Audit Controls.** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

C. **Integrity Controls.** A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

D. **Transmission Security.** A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

Required and Addressable Implementation Specifications

Covered entities are required to comply with every Security Rule "Standard." However, the Security Rule categorizes certain implementation specifications within those standards as "addressable," while others are "required." The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.28

4. Organizational Requirements

A. **Covered Entity Responsibilities.** If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.

B. **Business Associate Contracts.** HHS is developing regulations relating to business associate obligations and business associate contracts under the HITECH Act of 2009.

5. Policies and Procedures and Documentation Requirements

A. A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.

B. **Updates.** A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI).

The HIPAA Enforcement Rule

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings. The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E.

Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Part 3: HIPAA Omnibus Updates

On Jan. 25, 2013, the Department of Health and Human Services (HHS) published the "HIPAA Omnibus Rule," a set of final regulations modifying the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement various provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Highlights of HIPAA Omnibus Final Rule:

- Patients can ask for a copy of their electronic medical record in an electronic form.
- When patients pay out of pocket in full, they can instruct their provider to refrain from sharing information about their treatment with their health plan
- There are new limits on how information can be used and disclosed for marketing and fundraising purposes, and it prohibits the sale of an individuals' health information without their permission.
- Penalties for noncompliance with the final rule are based on the level of negligence with a maximum penalty of $1.5 million per violation.
- Health Plans also have changes related to the Genetic Information Nondiscrimination Act (GINA) that must be reflected in their policies and NPPs

BIGGEST HIPAA breaches

	Covered Entity	#People
01	Anthem, Inc. Affiliated Covered Entity	4 Million
02	Premera Blue Cross	11 Million
03	Excellus Health Plan, Inc.	10 Million
04	Science Applications International Corporation:	5 Million
05	University of California, Los Angeles Health:	4.5 Million
06	Community Health Systems Professional Services Corporation:	4.5 Million
07	Advocate Health and Hospitals Corporation, d/b/a Advocate Medical Group:	4 Million

Compliance

- Number of people in U.S. affected by publicly reported **HIPAA** breaches since 2009: 159.3 Million
- 74% are due to Hacking/IT Incident
- 40% top 10 are business associates
- 60% of top 10 are due to Hackers

(Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)
(From: 2009 to 2015)

Part 5: HIPAA Penalties

The High Cost of HIPAA Violations

Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5).

Civil Penalties for HIPAA violations

HIPAA violation	Minimum penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by state attorneys general regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect, but violation is corrected with the required time	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Part 6: What HIPAA wants you to do?

A breakdown of above rule will show that HIPAA is asking for 6 Things:

- **Choose HIPAA Privacy and Security Officer** - appoint a privacy and security officer. This could either be the same or different individuals. They will be responsible for implementation of compliance in the organization
- **Conduct Risk Assessment** - review your workplace and electronic devices to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI)
- **Assess Risks** - review risks identified in risk assessment and plan control measures.
- **Develop HIPAA Privacy and Security Policies and Procedures** – develop and implement HIPAA Privacy and Security policies and procedures
- **Train Employees** - train all employees who use or disclose protected health information
- **Monitor Compliance** – monitor compliance regularly.

Part 7: Closing the Gaps in HIPAA Compliance

Achieving HIPAA compliance is the responsibility of everyone involved in the practice. Building a culture of compliance in organization depends on 4 important components.

Organizational Requirement

1. Risks Assessment
2. Creating HIPAA policies
3. Training the Team
4. Monitoring

Part 8: HIPAA Documentation Challenges

HIPAA documentation is only as good as its accuracy.

Proper Documentation is Crucial in Achieving HIPAA Compliance

A healthcare organization HIPAA compliance program will be considered directionless without proper documentation. Documentation creates a baseline security standard for every process, workforce member, and system. It includes retaining written or electronic results of a risk analysis, documenting the results of an audit, developing and implementing comprehensive privacy and security policies and procedures, and documenting staff training and security incident responses.

Meeting HIPAA Documentation Requirements

HIPAA Documentation means “recording the Who, What, When, Where, How, and Why of everything relating to Protected Health Information (PHI) in the healthcare spectrum”

Part 9: How HIPAA Institute can help?

HIPAA Institute developed this comprehensive suite of best-in-class solutions designed to make HIPAA compliance faster, easier, and cheaper. It offers a set of Templates, Checklists, eLearning Modules, and easy to refer and implementable action items to help organizations achieve compliance.

HIPAA Institute offers:

Templates:

HIPAA Institute's customizable templates can be easily altered to meet the unique requirements of healthcare organization. The template help professionals comply with all of the areas of the HIPAA Privacy, Security and Breach Notification Rules, while staying up-to-date with new regulations. The templates are reviewed by renowned HIPAA specialists such as Jim Sheldon-Dean, Barbara Cobuzzi, and Kristine Cuddy.

Ask an Expert

Have a compliance question? Ask an Expert has the answers. This forum allows users to submit their question(s) and a HIPAA compliance specialist will respond with the answer, supporting information, and explanation—within 48 hours.

Education/ eLearning

Violations of regulations such as the HIPAA Privacy and Security Act have the potential to cost practices thousands of dollars in fines. Therefore, educating staffs on these compliance related guidelines is always a priority. HIPAA institute's interactive e-learning courses help organization drive awareness about the subject. The eLearning modules also help generate Continuing Education Units (CEU) for Training and Education, and Auditing and Monitoring for Compliance, approved by AAPC, HCCA, AHIMA, PAHCOM, etc.

Plus, one can also print the CEU certificates with one quick online test.

Checklists

HIPAA Institute checklists are created to provide a complete walkthrough of HIPAA privacy and security rule for organizations, thus highlighting the policies, processes and different mechanisms required to effectively implement HIPAA compliance.

Online Tools

In an environment of ever-changing regulations, the online tools help manage compliance, understand the gaps, mitigate the risks and achieve HIPAA compliance.

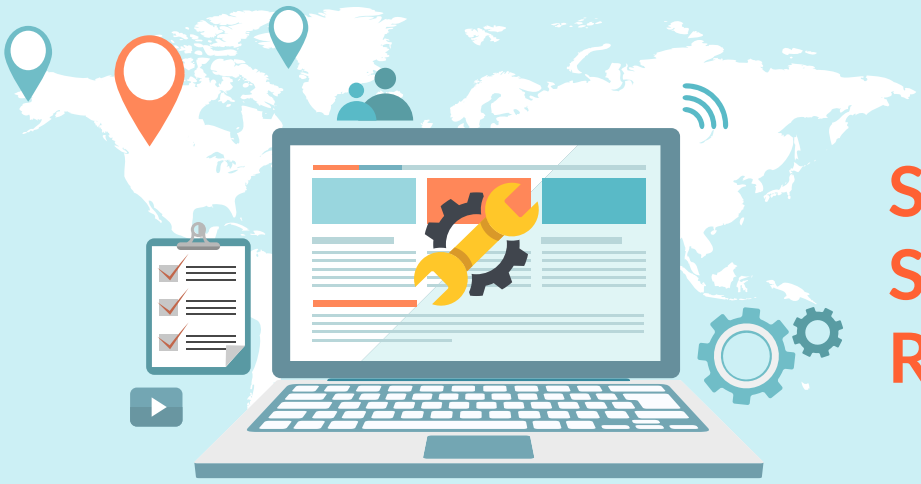
Violations of regulations such as the HIPAA Privacy and Security Act have the potential to cost practices thousands of dollars in fines. HIPAA Institutes best-in-class web-based solution provides valuable guidance to help organizations establish the policies, procedures and trainings to achieve HIPAA compliance in an easy way.

Part 10: Conclusion

According to the healthcare data breach reports submitted to Office of Civil Rights, Department of Health and Human Services 113,267,174 of Americans medical records data was exposed in 2015. This increase in cybersecurity attacks, employee data theft, and negligence shows a gap in HIPAA compliance training in healthcare organization which needs to be corrected.

Implementing best practices for HIPAA, conducting ongoing risk analysis, workforce training and HIPAA policy awareness will go a long way in protecting any organization's PHI and ensuring privacy and security. As per the OIG, implementing an ongoing training program for staff isn't just a good idea, it's actually a requirement in order for covered entities and their business associates (healthcare providers, hospitals, individual clinics etc.) to stay HIPAA and HITECH compliant.

HIPAA Institute offers a wealth of compliance training resources on HIPAA, HITECH, OSHA, OIG and other compliance regulations for staff members, including updated regulations and court rulings for maintaining compliance.



SERVICE & SOLUTION RESOURCES

✓ Policy Management Tool:

Create and manage your policies and procedures and be audit ready. Web-based system and no local installation requirement allows the use of preferred web browser for easy secure access anytime, anywhere.

✓ Customizable Policy and Procedure Templates:

Policy and procedure templates you can customize to fit the needs of your practice. Downloadable forms to help you establish a comprehensive compliance program.

✓ E-Learning:

HIPAA Institute eLearning modules help you to generate Continuing Education Units (CEU) for Training and Education, and Auditing and Monitoring for Compliance, approved by AAPC, HCCA, AHIMA, PAHCOM, etc. You can also print your CEU certificates with one quick online test.

✓ Compliance checklist:

HIPAA Institute's checklists provide you with a complete walk-through of the HIPAA Privacy and Security Rules, highlighting the required policies, processes, and mechanisms you need to effectively implement HIPAA compliance in your organization.

Contact Information

ADDRESS

2222 Sedwick Road, Durham, NC 27713

PHONE NUMBER

1-800-262-8146

EMAIL

help@hipaainstitute.com

HIPAA INSTITUTE

Achieve | Maintain | Inculcate | Track