HIPAA Enforcement, Training Requirements, Tips, and Resources

November 29, 2018

In 2003, the Office of Civil Rights (OCR) began enforcing the HIPAA *Privacy Rule*. In 2009, OCR began enforcing the HIPAA *Security Rule*. Every year, there is a steady increase in the number of complaints received and investigated by the OCR. Since 2003, the OCR has received over 186,453 HIPAA complaints, initiated over 905 compliance reviews and resolved 96% of these cases. As a result of these HIPAA complaints, OCR has imposed civil monetary penalties on violators totaling $79 million.[1]

Hospitals, private practices and outpatient facilities have been the most common types of covered entities required to take corrective action.

The compliance issues OCR most often investigates are:

- Impermissible use and disclosure of protected health information (PHI)
- Lack of safeguards of PHI
- Lack of patient access to PHI
- Lack of administrative safeguards of electronic PHI
- Use or disclosure of more than the minimum necessary PHI

Workforce Training

Workforce training is the key to HIPAA compliance and risk mitigation. Both the HIPAA *Privacy Rule* and *Security Rule* have workforce training requirements.[2]

Privacy Rule Training

Covered entities are responsible for ensuring that every member of its workforce (both new and existing employees) receives training in HIPAA privacy policies and procedures. If your organization has contract employees who come in contact with PHI and work routinely on the premises, these contract employees should also receive HIPAA training. The *Privacy Rule* requires that your organization maintain documentation that the training has taken place.[3]

Although the *Privacy Rule* does not specifically require annual training or a specified length of time for training, annual training is recommended because of the increasing risks of a privacy or security violation and the heightened liability associated with a violation.

Security Rule Training

The *Security Rule* requires security awareness training for your workforce as employees generally create the most significant risk to your organization's security. This training should be periodically updated to include any changes to the *Security Rule* and when your organization has new or upgraded hardware or software that impact security.

What Topics Should Be Covered in the Training?

Privacy

The *Privacy Rule* does not identify the specific topics that must be covered in workforce training. Rather, the *Privacy Rule* states that training must be "as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity."

Based on current industry guidance, the most important HIPAA privacy topics to train your workforce include:

- Identifying the organization's Privacy Officer
- What is PHI?
- Document retention and destruction
- The minimum necessary rule
- Rules about when and how PHI may be disclosed
- Disclosures that require a written authorization
- Disclosures that do not require an authorization
  - Treatment, payment, healthcare operations, public health and safety, research
  - Organ and tissue donations, work with a medical examiner or funeral director
  - Workers' compensation, law enforcement or other government requests
- The importance of confidentiality
  - Confidentiality policy
  - Social media policy
- Accounting of disclosures
- Patient rights
  - Obtaining a copy of their medical record
  - Requesting a correction of their medical record
  - Requesting confidential communications
  - Requesting limitations on their medical information
  - Requesting an accounting of disclosures
  - Obtaining a copy of the Notice of Privacy Practices
  - Requesting a representative
  - Requesting who information is shared with (family, friends, or others involved in the patient's care)

    - How to handle a patient complaint related to privacy

Security

Like the *Privacy Rule,* the *Security Rule* does not identify the specific topics that should be covered in workforce training.

Based on current industry guidance, the most important HIPAA security topics to train your workforce include:

- Organizational policy on security updates
- How to respond to a patient's request for electronic communication
- Physical safeguards of equipment and devices that contain PHI (laptops, flash drives)
- Procedures for guarding against, detecting, and reporting malicious software
- Procedure for guarding against, detecting and reporting social engineering attacks
    - Phishing
    - Dangers of certain websites
- Remote access procedures
- Procedures for monitoring login attempts and reporting discrepancies
- Procedures for creating, changing and safeguarding passwords
- Use and security procedures related to portable devices
- New or upgraded hardware or software or new technologies that impact security
- HIPAA Breach/Data Security Incident
    - Definition of breach
    - How to respond in the event of a potential breach or a security incident
- Procedures for destruction of sensitive information (hard copy and electronic)

Suggested Action Items

1. Make sure your organization's Notice of Privacy Practices (NPP) are updated. You can find sample forms in MagMutual's HIPAA Toolkit
2. Respond to patient's medical record requests as soon as possible, but no later than 30 days after the request is made
3. Limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. (The minimum necessary rule does not apply to disclosures for treatment purposes.)
4. Ensure that the HIPAA authorization form your organization is using includes all of the required components
5. Perform and maintain a current security risk analysis. A security risk analysis tool is available for download at www.healthit.gov/providers-professionals/security-risk-assessment [1]
6. Physically secure and encrypt data on laptops, thumb drives, DVDs, cellphones, and other forms of portable media
7. Regularly perform audits on your systems to prevent intrusions
8. Train your staff on the steps to take in the event of a HIPAA-related complaint

Training Resources

- MagMutual HIPAA Staff Training Learning Module [2] (requires login to account)
- MagMutual Patient Safety Institute's HIPAA Webinar [3] (requires login to account)
- HIPAA 101: The Basics of HIPAA Administrative Simplification [4]
- Worried About Using a Mobile Health Device for Work? Here's What To Do [5]

HealthIT.gov's Guide to Privacy and Security of Electronic Health Information [6] provides a beginner's overview of what HIPAA requires, and the page has links to security training games, risk assessment tools, and other aids.

[1] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html [7]. November 2018.

[2] 45 CFR § 164.530(b)(1); 45 CFR § 164.308(a)(5).

[3] 45 CFR 164.530(b)(2)(ii).

The information provided in this resource does not constitute legal, medical or any other professional advice, nor does it establish a standard of care. This resource has been created as an aid to you in your practice. The ultimate decision on how to use the information provided rests solely with you, the PolicyOwner.

Source URL: https://www.magmutual.com/learning/article/hipaa-enforcement-training-requirements-tips-and-resources

Links
[1] http://www.healthit.gov/providers-professionals/security-risk-assessment
[2] https://www.magmutual.com/learning/course/protecting-patient-privacy
[3] https://www.magmutual.com/learning/course/hipaa-privacy-and-security-preparing-increased-enforcement
[4] https://www.youtube.com/watch?v=ahEW1xEKz0Y
[5] https://www.youtube.com/watch?v=Vz1ddGJn1PM
[6] https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
[7] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html