Lippincott NursingCenter

March 2019
www.nursingcenter.com

Guide to Privacy and Security of Electronic Health Information

About the Guideline

This guide is published by The Office of the National Coordinator for Health Information Technology (ONC) and is intended to provide health care providers, including Health Insurance Portability and Accountability Act (HIPAA) covered entities (CEs) and Medicare eligible professionals (EPs) the tools and resources to integrate federally mandated health information privacy and security requirements into practice. Updates regarding the Medicare and Medicaid Electronic Health Record (EHR) incentive program requirements are detailed in the text of this review.

Key Definitions

- In 2011, the Center for Medicare and Medicaid Services (CMS) initiated the Medicare and Medicaid EHR Incentive Programs, known as "EHR Incentive Programs" or "Meaningful Use" Programs which are intended to encourage adaptation of EHR by incentivizing healthcare providers and organizations to adopt EHR into their practice in a staged approach while meeting the security and privacy requirements (CMS, 2019).
- The HIPAA Privacy, Security, and Breach Notification Rules, most recently updated in 2013, set forth how certain entities, including most health care providers, must protect and secure patient information. They also address the responsibilities of Business Associates (BAs), which include EHR developers working with health care providers.

Key organizations

Centers for Medicare and Medicaid services (CMS)

- Oversees the meaningful use programs

Office for Civil Rights (OCR)

- Administers and enforces HIPAA privacy, security, and breach notification rules
- Conducts HIPAA investigations, compliance reviews, and audits

The Office of the National Coordinator for Health Information Technology (ONC)

- Supports adoption and promotion of EHRs and health information exchange
- Provides educational resources and tools to assist providers in maintaining private and secure Protected Health Information (PHI)

National Institute of Standards and Technology (NIST)

- Establishes computer security standards for the federal government
- Publishes reports on topics related to IT security, available to the public, and used to assist providers in developing strong security practices

Key Clinical Suggestions/Recommendations

The guide is arranged in 7 chapters, the highlights of each chapter are summarized here.

Chapter 1: Why Do Privacy and Security Matter?

- Digital health information can improve overall health outcomes by allowing access to timely and accurate patient health records. Access can improve both the quality of care by the healthcare provider and overall health of the patient.

- The likelihood of patients' withholding medical history from healthcare organizations and providers increases when there is a lack of trust in the security of electronic health information which can negatively affect health outcomes (Agaku et. al, 2014).
- Standardization and rules should be established to protect medical record privacy and security.
- To develop trust, the following recommendations are made:
    - Maintain accurate, secure information in patients' records and ensure that patients have access to their EHR as requested.
    - Access patient medical records only as requested or as necessary.
    - Be sure medical records are accessible only to authorized entities.
    - Ensure all members of the healthcare organization are trained in safe handling of records and are committed to maintaining privacy and security.
    - Ensure breaches of security are dealt with serious consequences.
    - Implement a system to prevent and protect against cyber-attacks.

Chapter 2: Your Practice and the HIPAA Rules

- HIPAA rules were developed to protect patient healthcare information and patients' rights to their health care information held by CEs and BAs.
    - CEs: Doctors, clinics, hospitals, nursing homes, pharmacies or any healthcare provider that bills electronically, including health plans and health clearinghouses
    - BAs: Any entity or individual, other than employee of provider/healthcare organization, who has access to or disclosure of PHI by means of services they provide to the healthcare provider or organization; may include, but isn't limited to, claims processing, billing, data analysis, quality assurance, certain patient safety activities, or utilization review
    - BAs act on behalf of CEs
- HIPAA Regulations include:
    - Privacy Rule – national standards for protection of individual identifying information, including how PHI is used and disclosed; includes standards on how patients may obtain and correct information in their medical record
    - Security Rule – national standards for the security of health care information and electronic protected health information (ePHI)
    - Breach Notification Rule – establishes rules for CEs and BAs to follow in response to a breach of privacy or security in PHI
- In addition to HIPAA regulations, healthcare providers and organizations may have further rules and regulations on EHR and PHI mandated at the local, state or federal level regarding security and privacy of PHI.

Privacy Rule

Protects PHI which is any information (written, electronic, or oral) that is individually identifiable health information (with reasonable belief that it could identify this patient) including demographics related to past, present or future, physical or mental health conditions, provision of heath care, or past, present or future payment for provision of health care to said individual.

- Notice of privacy practices (NPP) should be posted, distributed, and made available for patients to see how information specific to PHI is used and disclosed.
- NPP must include a description of patient rights and right to complain if there is concern that rights have been violated with process and point of contact to do so.

- CEs may disclose PHI to another CE **without authorization from patient** if both CEs have a relationship with the individual, PHI pertains to relationship, and PHI requested is the minimal amount of PHI necessary to accomplish a purpose (also referred to as **minimum necessary standard**).

A CE may disclose PHI **without patient authorization for**:

- Their own treatment or treatment by another healthcare provider
- Their own payment or payment of another CE and any health care provider
- Health care operations (quality assessment/improvement activities, quality or competence of healthcare provider, fraud abuse detection or compliance)
- Information sharing needed for treatment
- Disclosure to family, friends and others involved in the care of the individual and for notification purposes; information permission required by asking individual or by determining that the individual doesn't object outwardly (i.e. discussing health information while person is in the room and they don't object)
- If individual is incapacitated, in an emergency situation and provider determines through professional judgement that PHI disclosure is in the best interest of the patient and that minimal disclosure is necessary to achieve intended goal
- PHI is needed to ensure public safety
    - Immunization records (with oral agreement by parent or guardian for minor or individual)
    - Release to public health authority authorized by law to collect particular PHI with goal to prevent or control disease, injury or disability (i.e. births, deaths, public health surveillance, interventions, or investigations)
    - To a foreign government agency as directed by public health authority
    - To persons at risk of contracting or spreading a disease or condition if other law, such as state law, authorizes the CE to notify such individuals as necessary to prevent or control the spread of the disease
- Information necessary to prevent or lessen imminent danger or threat to person or public, with disclosure minimized only to person judged suitable to prevent or lessen this threat
- Disclosures in healthcare facility directories where patient contact information is maintained (with oral permission by patient)
- Individuals who have been deceased for more than 50 years isn't PHI, so information may be used without authorization

Patients' written authorizations ARE required in the following situations:

- Any disclosure not for treatment, payment, or healthcare operations
- Psychotherapy notes (although the CE that originated the notes may use them for treatment)
    - Note: PHI pertaining to substance abuse and behavioral health are included in PHI with the specific exception of psychotherapy notes; individual states or other federal regulations may have more stringent regulations regarding substance abuse and behavioral health disclosure
- Marketing activities
- PHI sales and licensing
    - The following activities aren't considered "sale of PHI":
        - Public health reporting
        - Sale or merger of practice

  - Treatment and payment
  - Due diligence
  - Payment made to BA for service BA supplied
  - Research, if compensation is reasonable and cost based
- Research - special rules apply to clinical research, bio-specimen banking and all other research not involving psychotherapy notes

De-identified PHI: Doesn't identify or provide reasonable information to identify an individual. Information de-identified under HIPAA guidance isn't considered PHI.

Chapter 3. Understanding Patients' Health Information Rights

- Healthcare providers have a responsibility to provide patients with NPP that describes how the practice shares the individual's PHI and the patient's rights to complain to their practice and the U.S. Department of Health and Human Services if they believe their privacy has been violated.
- The CMS EHR Incentive Program provides rights for patients who want the healthcare provider to transmit their electronic HPI to themselves or other caregivers.
- Patient Rights to Information:
  - Right to access information – copy of PHI available to inspect in a **designated record set** (a group of records that a practice or BA retains to make decisions about the individual's healthcare, including the patient's medical and billing records); must grant or deny request within 30 days and must be provided in format as requested by patient
  - Right to amend patient information – must be honored unless deemed PHI is accurate and complete; must be completed in 60 days or less after receipt of request
  - Right to receive an account of disclosure – includes the listing of names of persons or entity, date, description, and purpose for which PHI was disclosed (for 6 years prior to the date on which the account was requested)
  - Right to restrict information – request to restrict uses and disclosure for treatment, payment and healthcare operations, persons/individuals involved in healthcare or payment for health care, family members on individual's general condition, location or death
  - Right to confidential communications (i.e. information on phone voicemail)

Chapter 4: Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity

- Every ePHI storage location is at risk for cyber-attacks, therefore all systems that maintain or contain ePHI must be protected.
- Safeguards of the HIPAA Security Rule:
  - Administrative Safeguards – Development, implementation, and maintenance of policy and procedures to prevent, detect, contain and correct security violations. Organizations should ensure that risk is assessed, and security measures take place to reduce any identified risks.
  - Physical Safeguards – Physical measures, policy and procedures to protect electronic systems, buildings and equipment from environmental hazards and unauthorized access. Policies and procedures should be in place to protect and control ePHI.
  - Organization Safeguards – CEs must have arrangements or contracts with BAs that access the CE's ePHI. The standards provide criteria for written contracts or other arrangements.
  - Policies and Procedures – Mandate that CEs must have appropriate policies and procedures to comply with the provision of the Security Rule. All PHI must be maintained until six years after the date of creation or last effective date (whichever is later). A CE must maintain

written security policies and periodically review and update its documentation in response to environmental or organizational changes that could affect the security of the ePHI.
    - Security risk assessment: Chapter six discusses security risk analysis to identify potential security weaknesses and flaws, with steps to reduce risk and comply with HIPAA Rules and meaningful use requirements. Properly configured and certified EHRs can provide more protection to ePHI than paper files provided (ONC, 2015).

Key measures in keeping PHI secure with an EHR:

- Goal is to protect confidentiality, integrity and availability of ePHI in the EHR.
- Regular maintenance and knowledge of your EHR's built in security features including regular software updates and installation of available patches.
- Ensure proper encryption of text to reduce risk of unauthorized access as guided by NIST.
- Consider the following when working with the EHR and the health IT developer:
    - ePHI encryption
    - Auditing functions
    - Backup and recovery routines
        - Where is the documentation?
        - Where is the backup stored?
        - How often does the recovery system need to be tested?
    - Unique user ID and strong passwords
    - Role or user-based access controls
    - Auto time out
    - Emergency access
    - Amendment and accounting of disclosures
    - How the health IT developer will train staff on the features and maintenance of the system as well as the privacy and security awareness, requirements and functions
    - How much support will be provided by the health IT developer
    - How staff and health IT developer will authenticate themselves for communication purposes
    - How much remote access the health IT developer will have to provide support and ascertain if access will be secure
    - Secure email system for patient and staff that complies with the HIPAA Security Rule

Cybersecurity:

- Refers to a method to prevent, detect and respond to either unauthorized access or attacks on a computer system's information, digital memory device, or cloud server. This is necessary to comply with the HIPAA Security Rule and must also be provided for mobile devices (smartphones, tablets, and laptops).
- All online exchanges of PHI are at risk for cyberattacks including exchanging patient information or submitting claims electronically, generating records for patients' request, and e-prescribing.
- The ONC provides specific tools to reduce the risk of cyberattacks, including security standards and required protections for ePHI under the HIPAA Security Rule which can be found on the HIPAA Security Rule web page https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
- The HIPAA Security Rule must be followed if a provider is emailing a patient. Information becomes protected once the provider receives information from a patient. An encrypted email system should be used with appropriate Security Rule safeguards.

Chapter 5: Medicare and Medicaid EHR Incentive Programs Meaningful Use Core Objectives that Address Privacy and Security

- The Medicare and Medicaid EHR Incentive Programs or "Meaningful Use" Programs are CMS set staged requirements for providers to comply with over time to integrate use of EHRs and receive incentive payments for compliance.
- Meaningful Use must be demonstrated by:
    - Using Certified EHR Technology (CEHRT) as standards, implementation specifications, and certification criteria
    - Meeting CMS-defined criteria through a staged approach, based on anticipated technology and capabilities development
- Goal is improving health care quality, encouraging widespread EHR adaptation, promoting innovation, and avoiding excessive or unnecessary burdens on healthcare providers (ONC, 2015).
- Meaningful Use Stage 1 and Stage 2 require providers to "attest" that they have met specific objectives and measures regarding the use of the EHRs for patient care.
    - Stage 1 focuses on:
        - Capturing electronic health information in a structured format
        - Tracking key clinical conditions and communicating PHI for coordination of care
        - Utilizing clinical decision support tools to support management of disease and medication
        - Using EHR to involve patient and families
        - Reporting clinical quality measures and public health information
    - Stage 2 is a continuation of stage 1 with a focus on:
        - Use of health IT for continuous quality improvement
        - Point of care and exchange of information in a structured format
        - Examples: electronic transmission of orders, electronic transmission of diagnostic test results (labs, radiology, etc.)

Chapter 6. Sample Seven-Step Approach for Implementing Security Management Process

This chapter provides an approach to implementing a security management system in your healthcare organization or practice. It includes addressing requirements of the Medicare and Medicaid EHR Incentive Programs which are grounded in the HIPAA Security Rule.

<u>Step 1: Lead your culture, select your team, and learn.</u>

- Designate a security officer.
- Discuss HIPAA security requirements with your EHR developer.
- Consider using a qualified professional to assist with your security risk analyses.
- Use tools to preview your security risk analysis.
- Update your knowledge base of HIPAA Rules.
- Promote a culture of protecting patient privacy and securing patient information.

<u>Step 2: Document your process, findings, and actions.</u>

This step is required by both the HIPAA Security Rule and EHR Incentive Programs to comply and support meeting the measures of the program. It includes providing documentation of security risk analysis,

copies of HIPAA-related policies, procedures, reports and activities. It is recommended that the organization keeps a master file of security findings, decisions and actions.

Step 3: Review existing security of ePHI (perform security risk analysis)

- Consider creating a workplace culture that makes security a high priority.
- Have an action plan that assigns responsibility for each risk analysis component.
- Involve an EHR developer in the process.
- Be aware of potential threats to ePHI which include: human, cyberattacks, theft, workplace member errors, natural disaster threats (i.e. earthquakes, etc.), or environmental threats (i.e. pollution, power loss).
- Stratify each risk as high, medium, or low based on probability of occurrence and likelihood that threats would exploit vulnerabilities.
- Recognize that there are differences in risk to office-based (local host) or internet-based (remote host) EHR systems (Examples can be found on Page 43 at https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf)

Step 4: Develop an Action Plan

- Focus on high priority threats and vulnerabilities.
- The action plan needs to be feasible, affordable and tailored to the characteristics of your practice. Five components of an action plan include:
  1. Administrative safeguards –perform security risk analysis periodically.
  2. Physical safeguards- lock offices, screen shields.
  3. Technical safeguards – secure user IDs and passwords, routine audits, anti-hacking and anti-malware software installed, encrypted data; regular backup and testing of backup system.
  4. Organization standards – review agreements with BAs regularly, update as needed.
  5. Policies and procedures – implement written policy and procedure with appropriate staff training and update regularly.
- Other suggested low-cost, highly effective safeguards include:
  - Don't allow staff to take home laptops containing unencrypted ePHI.
  - Remove hard drives before discarding old computers.
  - Don't email ePHI unless encrypted.
  - Servers should be kept in rooms accessible to authorized staff only.
  - Ensure office staff members understand that passwords shouldn't be shared.
  - Inform office staff that access is monitored randomly.
  - Maintain fire extinguishers.
  - Regularly check EHR server for malware or viruses.
- When developing the plan:
  - Identify simple actions that can reduce the greatest risks.
  - Review the OCR Security Rule Guidance (https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html) for specific HIPAA requirements.
  - Seek security risk professional or legal counsel for help if needed.
  - Meet with the team as needed to coordinate actions and track progress.

Step 5: Manage and Mitigate Risks

- Implement your action plan (which includes applicable EHR security settings and updating your HIPAA-related policies and procedures).
  - Certified EHR systems have a core package of technical security functions.

  - Practice should be aware of security functions within the EHR system.
- Prevent breaches by educating and training your workforce.
- Communicate with patients.
  - Provide information of measures to protect privacy and security of their health information.
  - Patients should be made aware of any breaches of information that may take place.
- Update your BA contracts; BAs must comply with relevant safeguards your practice has set for PHI, they must train their workforce and adhere to any additional requirements for patient rights and breach notification.

Step 6: Attest for Meaningful Use Security-Related Objective

Once you have met the requirements for the EHR Incentive Program, attest for Meaningful Use by utilizing a technical legal statement that your organization has met the necessary requirements and standards to protect electronic health information. The goal of the program is to provide incentive payment as EPs demonstrate adoption, implementation, upgrading, and meaningful use of their certified HRT.

Step 7: Monitor, Audit, and Update Security on an Ongoing Basis

- Determine who will be responsible for monitoring and conducting audits, as well as what will be audited.
- Identify triggers for audits (a sign that ePHI could have been compromised and requires further investigation).
- Determine both a schedule for routine audit and guideline for random audits.
- Must have ability to investigate any breaches which includes who, what, when, where and how patient ePHI was compromised.
- State law requires medical records to be stored for a set number of years. These laws are found in the state's licensing laws. If one of your BAs is a Health Information Exchange (HIE), your written requirement with the HIE should require it to return or securely dispose of the ePHI it creates, maintains, receives, or transmits on behalf of the practice.

Chapter 7: Breach Notification, HIPAA Enforcement, and Other Laws and Requirements

- Providers should examine if there are additional laws or requirements based on their state, state board of medicine, state associations, and the Regional Extension Center.
- Any CEs or BAs that fail to comply with HIPAA Rules can receive both civil and criminal penalties.
- A breach is defined as an impermissible use or disclosure under the Privacy Rules that compromises security or privacy of PHI (ONC, 2015).
- Breach Notification Rule
  - Requires HIPAA CEs to notify individuals and the Secretary of HHS of any loss, theft, impermissible use or disclosure of unsecured PHI (ONC, 2015).
  - Promptly notify the Secretary of HHS if it affected 500 or more individuals.
  - Notify the media if it affected more than 500 members of a state or jurisdiction.
  - Notify the Secretary of HHS and the affected individuals if there were less than 500 individuals involved.
- Risk assessment process for breaches:
  - First, conduct a risk assessment to determine if PHI has been compromised.
  - If there is low probability of compromised PHI, it isn't considered a breach and no notification is necessary.
  - If there is probability of compromised PHI, breach notification is required.

- Visit the OCR webpage for details on how to submit a breach notification form to the Secretary of HHS.
- Once notified, HHS reports the breach on the OCR website if it affects 500 individuals or more.
- The HIPAA Enforcement Rule provides different monetary penalties for four levels of culpability:
    - Violations the entity didn't know about and wouldn't have known about by exercising reasonable diligence
    - Violations due to "reasonable cause"
    - Violations due to "willful neglect" that are corrected within 30 days
    - Violations due to "willful neglect" that are or aren't corrected within 30 days

- Civil Penalties
    - Carried out by the OCR; state attorney general may also carry these out
- Criminal Penalties (overseen by the U.S. Department of Justice) can be issued for:
    - Knowing misuse of health identifiers
    - Knowing and unpermitted acquisition or disclosure of PHI

References:

Agaku, I., Adisa, A., Ayo-Yusuf, O., & Connolly, G. (2014). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association, 21*(2). doi: 10.1136/amiajnl-2013-002079. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3932467/

The Center for Medicare and Medicaid Services (CMS). (2019). Promoting interoperability. Retrieved from https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html

The Office of the National Coordinator for Health Information Technology (ONC). (2015). Guide to privacy and security of electronic health information, version 2.0. Retrieved from https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

U.S. Department of Health & Human Services. (n.d.) Summary of the HIPAA Security Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Link to Practice Guideline:

https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf