HIPAA Compliance and Privacy Concerns

Marisa McGinley
Staff Neurologist
Cleveland Clinic
3-10-22

Outline

- HIPAA and amendments
- COVID-19 related changes
- Telehealth challenges
- Future directions

The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual.”- Justice Earl Warren (1963)

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- The law encompasses many aspects of care with the main goal of assuring “portability” and continuity of health insurance coverage and privacy was initially a minor portion (Title II).
- HIPAA’s scope is limited to covered entities (such as health plans and health care providers) who transmit PHI in electronic form in relation to health care treatment and transactions
- HIPAA’s application to covered entities requires them to take responsibility with respect to using compliant technologies.

Edemekong PF, et al In: StatPearls. StatPearls Publishing, Treasure Island (FL); 2021.; Berwick D et al. JAMA. 2018 Jul

HIPAA Amendments

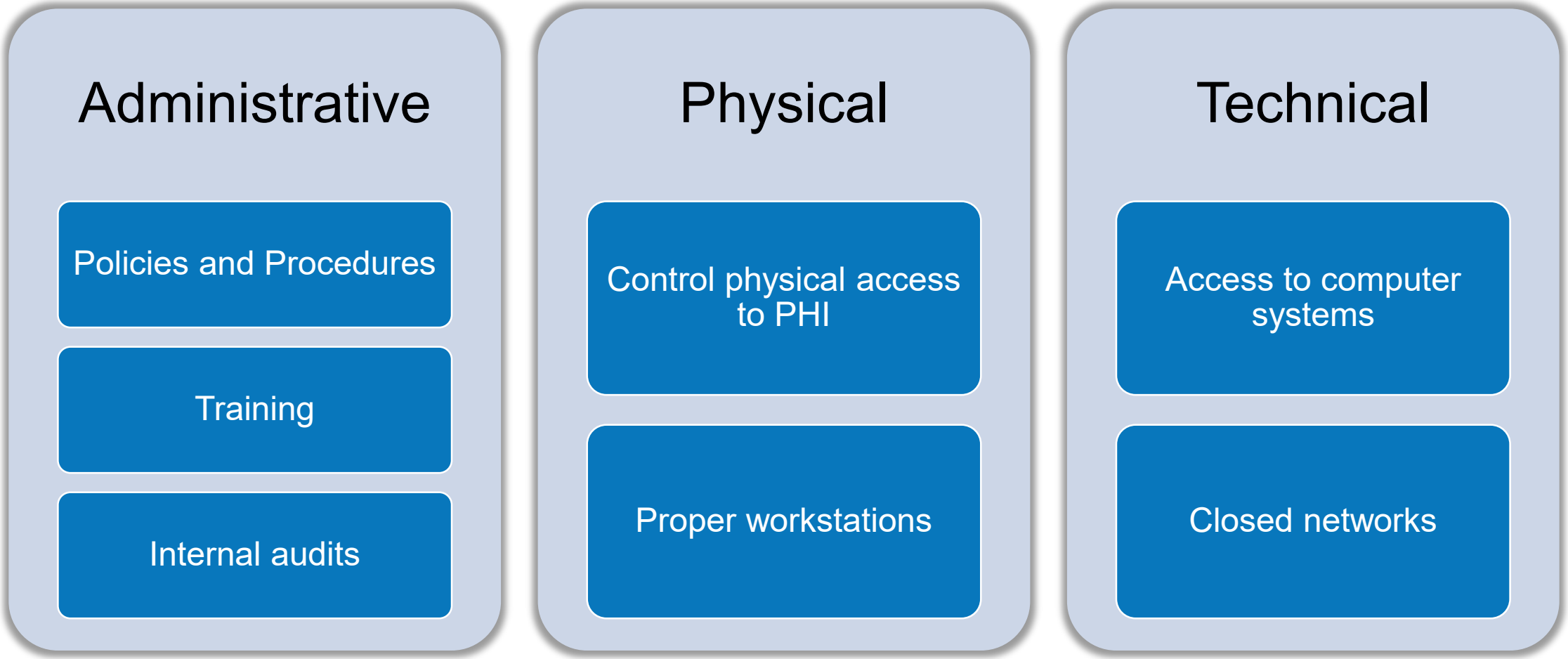
- Major amendments have since occurred to further define privacy rules
- The Security Rule Amendment of 2003
  - Technical Safeguards
  - Physical Safeguards
  - Administrative Safeguards
- The Privacy Rule Amendment of 2003
- The Breach Notification Rule of 2009
- The Final Omnibus Rule of 2013
  - modified HIPAA, GINA, and the HITECH Act to improve their workability, effectiveness, and flexibility.

Why is PHI valuable?

- Medical records often contain
  - Date of birth
  - Insurance
  - Health provider information
  - Genetic data—information that cannot be easily altered,
- This information is particularly lucrative for hackers because a patient's health information can be sold for 10-20 times more than the amount for credit card information or social security number.

Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity Risks in a Pandemic. J Med Internet Res. 2020;22(9):e23692. Published 2020 Sep 17. doi:10.2196/23692

Security



Edemekong PF, et al In: StatPearls. StatPearls Publishing, Treasure Island (FL); 2021.

Telehealth provider concerns

81%	•Telehealth providers are concerned about data leakage
52%	•Telehealth providers reported patient dissatisfaction or refusal to engage with a virtual visit because they distrust it.
>70%	• said that they use legacy operating systems, largely because of the costs associated with updating them •Legacy systems may pose risks to security because they often cannot be patched or updated, exposing them to security vulnerabilities.
4/10	• Four in ten surveyed telehealth providers agreed that the majority of clinicians do not have clear insights into how patient data is protected.
71%	•of respondents agreed that telehealth services would add the most value to the healthcare sector in the next five years compared to any other technology.

Kruse CS, Frederick B, Jacobson T, Monticone DK Technol Health Care. 2017; 25(1):1-10.; Arlington Research and commissioned by Kaspersky

Security Concerns

- Prior to the pandemic, cyber-attacks targeting medical information has increased 22 percent a year with 112 million compromised records back in 2015
- Since the pandemic, more breeches have occurred:
  - 7% were the result of deliberate hacking
  - 75% of the breaches were tied to business associates of providers or third parties, suggesting that non-providers need to ramp up their security as much if not more than the rest of the healthcare community.

COVID-19 related changes

- Office of Civil Rights (OCR) will exercise its **enforcement discretion** and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency.
- A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any **non-public** facing remote communication product that is available to communicate with patients.
- Under this Notice, covered health care providers **may use popular applications that allow for video chats**, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 nationwide public health emergency.

https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

Telehealth unique HIPAA challenges: Physical space

What happened early in the pandemic?

- Many adopted video conferencing applications, independent of electronic medical record systems, as essential patient care tools.
- Most electronic medical record systems did not offer these services or they were inefficient or expensive, or both.
- Inherently, when using third party there is a greater risk of data leakage, especially with video conferencing platforms originally used for social events.
- One example is the Facetime Group bug where third parties were able to listen in to a conversation without having to join the conference call.
  - This is something that is prevented in applications such as TEAMs and Zoom who have authentication protocols in place to prevent a monitoring situation.
- Because providers are often trying to find the easiest solution for the patient, this had become a common tool during the COVID-19 pandemic and opens up liability to data leaks.

Business Associate Agreements (BAA)

- Requirements for covered entities with respect to their business associates (e.g., lawyers, accountants, billing companies, and other contractors) if their relationship entails creating or sharing PHI.
- Liability for business associates' HIPAA violations has led to efforts to develop comprehensive contracts known as Business Associate Agreements (BAA).
- The purpose of a BAA is to obtain a written assurance that business associates protect health information through compliance with HIPAA.
- Some technology vendors have previously entered into BAAs, and, if they are familiar with the Security Rule, may have enhanced security capabilities. Others have not. The Notification includes vendors that market HIPAA-compliant video communication products, such as Skype for Business, Microsoft Teams, Zoom for Healthcare, and Google G Suite. However, OCR clarifies that it has not reviewed BAAs offered by these vendors, and this list does not constitute an endorsement of specific technology, software, applications, or products.

Audit Trail Requirement

- System administrators must be able to record and follow audit trails whenever protected health information is created, modified, accessed, shared, or deleted.
- Conventional audit control rules require health care workers or their organizations to enter into a Business Associate Agreement with the third party handling protected health information
- The HIPAA audit protocol was prepared for security and privacy compliance officers, not for telehealth providers who typically have no formal training in information security and privacy.
- Third party apps may use less than secure practices when developing an application to bring timeline to market sooner thanks to the rapid changing environment of COVID-19. Some software development kits used in popular platforms were found to have Zero Day flaws or weakened encryption, or third party monitoring to other platforms, meaning a review must be in place before a decision is made to implement.

HIPAA Privacy rule. 45 CFR parts 160 and 164, Subparts A, C and E.; Bhate et al. JAAD 83, 4, 10 2020. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html).

Avoiding the “Code of Silence”

- Patient care may be compromised when health care providers disproportionately fear the consequences of HIPAA violations
- Did the easing in HIPAA enforcement improve communication among clinicians and patients?
- Should the ongoing use of agile teleconferencing software, independent of electronic medical records, be embraced in the provider-patient relationship?

Shachar C, Engel J, Elwyn G. Implications for Telehealth in a Postpandemic Future: Regulatory and Privacy Issues. *JAMA*. 2020;323(23):2375–2376. doi:10.1001/jama.2020.7943

Future considerations

- Privacy concerns should not interfere with the actual need of patients to receive care on a timely basis.
- Revisions to audit controls in HIPAA could allow for the protection of privacy while also permitting patient and caregiver to exercise judgment in making decisions about the provision of health care.
- Guardrails, such as periodic audits, would be needed to ensure security. Perhaps, similar to systems in the financial sectors (ie, personal access to bank accounts and investment accounts), a more user-friendly approach to privacy may be possible for personal health care delivery.
- To maintain the impetus for change and the momentum for telehealth services that have resulted from the COVID-19 pandemic, the US cannot revert to prepandemic telehealth regulations. Neither can the US simply adopt the recent changes, because they lack nuance to support clinicians while ensuring safety and privacy for patients.

Berwick DM, Gaines ME. How HIPAA Harms Care, and How to Stop It. *JAMA*. 2018;320(3):229–230.; Bhate et al. JAAD 83, 4, 10 2020.; Anita Allen. NEJM.2021; 384:2169-2171; Shachar C, Engel J, Elwyn G. Implications for Telehealth in a Postpandemic Future: Regulatory and Privacy Issues. *JAMA*. 2020;323(23):2375–2376. doi:10.1001/jama.2020.7943