HIPAA: Securing Your Patients and Practice

Megan Maddocks, Privacy Officer

UC 2024

PCC
Pediatric EHR Solutions

Session Goals

1. Learn about recent updates to HIPAA
2. Learn about Security threats
3. Share security tips with each other

Agenda

- HIPAA: past, present & future
- Security
- Share time

UC 2024

PCC
Pediatric EHR Solutions

HIPAA

HIPAA Past...

- Almost turning 30!
- Its purpose is to improve portability, accountability, protection, and confidential handling of protected health information (PHI)

HIPAA Rules:

- Privacy
- Security
- Enforcement
- Breach Notification
- HITECH Act
- Omnibus
- FTC Final Rule

HIPAA Present...

Reminders for your to-dos:

- BAAs with all Business Associates
- Privacy & Security Policies for all staff (and ongoing training)
- Signed training forms for all staff
- Privacy Policy for Patients
- Visitor logs
- Disclosure and documentation protocols
- Audit logs & PHI access protocols
- Annual Security Risk Assessment
- PCC provides guidance here: HIPAA, Security Risk Assessments, and the Pediatric Practice - PCC Learn
- **Notice of Privacy Practices update required by **Feb 16, 2026****

UC 2024

PCC
Pediatric EHR Solutions

HIPAA Future…pending and new

- Data privacy protection proposed legislation
- Reproductive Health Privacy OCR Final Rule
- Breach Notification FTC Rule

National Data Privacy & Security Proposal

American Data Privacy and Protection Act (ADPPA)

- Introduced in 2022
- Stalled because it would have watered down existing state-level legislation , e.g., California

National Data Privacy & Security Proposal

The American Privacy Rights Act of 2024

- Introduced in April 2024
- Contains privacy and security standards for all consumer data
- Makes privacy a consumer right to control their personal information
- Sets security standards to protect data from being compromised

Legislation in draft as of late-May 2024

UC 2024

PCC
Pediatric EHR Solutions

OCR: Reproductive Health Care Privacy Final Rule

- Who: Department of Health and Human Services, Office for Civil Rights
  - *HIPAA Privacy Rule to Support Reproductive Health Care Privacy*
- When
  - Final rule published: April 26, 2024
  - Effective date: June 25, 2024
  - Compliance thereof if 180 days after: October 23, 2024
  - Compliance date for persons subject to regulation: Jan 1, 2025
  - Compliance date for persons subject to Notice of Privacy Practices (CFR 164.520): Feb 16, 2026 *To-do* for all of you!
- Why
  - Overturning of Roe v. Wade via Dobbs, gave pause and reflection to ensure that HIPAA still provided protection to reproductive health information (and those who provide it)

OCR: Reproductive Health Care Privacy Final Rule

- (changes) to HIPAA to protect women, their family members, and doctors by prohibiting the disclosure of PHI when it is sought to investigate or impose liability for seeking, obtaining, or providing legal reproductive health care
- This rule limits the circumstances under which an individual's reproductive healthcare information can be used for certain non-healthcare purposes
  - It "prohibits a regulated entity from using or disclosing an individual's PHI for the purpose of conducting a criminal, civil, or administrative investigation into or imposing criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care that is lawful under the circumstances in which it is provided."
  - The rule clarifies the definition of a "person"
  - The rule has adopted new definitions of "public health"
  - The rule adds a new category for prohibited uses and disclosures to clarify that a entities now need to recognize reproductive health care providers as a personal representative for an individual they provide such care for
  - New requirement that in certain circumstances regulated entities must first obtain an attestation that a requested use or disclosure for this information is not for a prohibited purpose.

FTC Final Rule: Breach Notification

- Who: Federal Trade Commission
- When:
  - Final rule issued April 26, 2024
  - Final rule take effect on June 25, 2024
- Why: Intent is to keep regulations up-to-date with technology

UC 2024

PCC
Pediatric EHR Solutions

FTC Final Rule: Breach Notification

- Breach Notification Rule Update to include health apps and other technologies that are not currently covered by HIPAA
    a. Modified the definition of "PHR Identifiable health information" and added two new definitions for "covered health care provider" and "health care services or supplies"
    b. Updated the definition of "PHR related-entity" to include entities that store personal health information other than personal health records (e.g. portals)
- FTC provides clarification regarding what they consider to be a security breach to mean "an unauthorized acquisition of identifiable health information that occurs as a result of a data security breach or an unauthorized disclosure."
- FTC is to be notified at the same time consumers are when the breach includes 500 or more individuals; both must be notified without undue delay and no later than 60 days from the date the breach was discovered
- Expansion of the permitted methods to notify consumers
    a. The entity or party that acquired the data will be named in the consumer notification

Security

University of Vermont Medical Center Cyber Attack

- Employee on vacation → UVM laptop used to open email and attachment from HOA *[HOA already attacked]* → Malware installed → Employee returns to UVM network →Malware installed again…
- Infrastructure rebuilt, and data restored from backups
- Cost estimate: $40 - $50 million, patient care impacted

Phishing

What is it? Social engineering to gain access to your device by getting you to click on a link or interact in some way

How does it work? Malicious software is downloaded to a device or network when the end users clicks a link, opens an attachment, or interacts with bad actor in some form or fashion

Who is at risk? Everyone

How to prevent it: Training, go straight to source (e.g., bank, company). Look closely at links: citibank.com and citib*a*nk.com.

Vishing (aka Voice Phishing)

What is it? Phishing over the phone/voice

How does it work? Robocall or automated message requesting a call back re: warranty related issues, IRS, banking, tech support, charities

Who is at risk? Everyone (older generations, and Gen Z 1996-2010)

How to prevent it: Don't answer calls from folks you don't know, or go straight to the source BEFORE providing any information

Credential Stuffing

What is it? Using stolen usernames and passwords from breaches

How does it work? Bad actors purchase in bulk and use automation to access sites

Who is at risk? Everyone

How to prevent it: Use unique passwords for each site and use a password manager, either a site such as Bitwarden, or a good old fashioned pen and paper to keep track of them

Money Mules (aka Employment Scams)

What is it? Common in the “work from home” ads; money is laundered transferred

How does it work? “Interview” for work from home job →provide personal information [e.g., bank, SSN] → $$ deposited to your band account →force you to wire money, buy gift cards….smaller wire transfers don’t trigger alerts

Who is at risk? Everyone, but most common targets are students, seniors/recently retired, under or unemployed, romance scams

How to prevent it: Research the company before providing any personal information

Share time

Ack! What Can I do? Learn, and then learn more....

Continuous learning

- We use knowbe4.com
- Training is done quarterly at PCC

Protect

- Via learning and awareness
- Tactical (keep those machines updated)

This is a never ending journey...

UC 2024

PCC
Pediatric EHR Solutions

Knowledge Sharing

Your office/your devices - what are you doing to secure your office, or what would you like to add to your list?

Session Takeaways

1. Enhanced protections for consumer data
2. Security: if it's too good to be true, it probably is. Always verify/go directly to the source.
3. Security is NOT a one an done; learn, learn more, and repeat

What Questions Do You Have?

References

General

New Legislation Aims to Upgrade HIPAA to Account for New Healthcare Technologies – Health Law Scan (morganlewis.com)

New HIPAA Regulations in 2023 (hipaajournal.com)

Healthcare Cybersecurity (hipaajournal.com)

Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2022 | HealthIT.gov

Legislation | Senate Committee on Health, Education, Labor and Pensions

References

UVM Case Study

UVM hospital 2020 cyberattack cause revealed: Malware and phishing (burlingtonfreepress.com)

Malware on employee's company computer led to cyber attack on UVM Medical Center - VTDigger

Statement from UVM Health Network on Cyberattack

References

Privacy legislation:

Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive... (senate.gov)
New Federal Data Privacy and Protection Legislation Introduced (hipaajournal.com)
American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf (d1dth6e84htgma.cloudfront.net)

New regulations

FTC Issues Final Rule Updating Health Breach Notification Rule (hipaajournal.com)
OCR Issues HIPAA Reproductive Health Care Privacy Final Rule (hipaajournal.com)
Federal Register :: HIPAA Privacy Rule To Support Reproductive Health Care Privacy

References

Vishing

https://www.proofpoint.com/us/threat-reference/vishing
https://consumer.ftc.gov/articles/robocalls
https://www.fortinet.com/resources/cyberglossary/vishing-attack
https://www.social-engineer.org/framework/attack-vectors/vishing/
https://www.donotcall.gov/

Credential Stuffing

https://owasp.org/www-community/attacks/Credential_stuffing
https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/
https://arstechnica.com/security/2023/10/private-23andme-user-data-is-up-for-sale-after-online-scraping-spree/
https://bitwarden.com/

Money Mules

https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules
https://www.cisa.gov/sites/default/files/publications/money_mules.pdf
https://krebsonsecurity.com/2020/03/coronavirus-widens-the-money-mule-pool/
https://www.theguardian.com/money/2023/jun/12/older-people-hired-as-money-mules-by-gangs-as-cost-of-living-crisis-bites