Grow Your HIPAA & Security Training

Megan Maddocks, MBA
PCC People and Culture Champion

PCC Pediatric EHR Solutions

UC 2026

Session Objectives

1. Get your “hands in the weeds” (via pen and paper) and make notes

2. Gain insight into the minimum necessary elements of HIPAA and Security training

3. Make it fun!

Training Outline

- When it should occur
- What it should include to begin
- What is PHI?
- Privacy Rule
- Security Rule
- Breach Notification Rule
- Practical Examples
- Build a Positive Compliance Culture

When should it occur?

- First day of employment (or shortly thereafter)
- Annually for all (administrative, clinical, and support staff)
- Ad hoc, i.e., after an incident
- Additionally:
  - Keep records of training
  - Ensure everyone knows who your Privacy Officer is

To begin, include:

- ➔ HIPAA overview and purpose
- ➔ Common language (PHI, designated record set, etc.)
- ➔ Covered Entity and Business Associate definitions

What is PHI? (18 identifiers)

- ➔ Electronic, paper, and oral
- ➔ Minimum necessary rule
- ➔ Designated record set
- ➔ Consequences for non compliance (legal, financial, reputation)

Privacy Rule

- ➔ HHS Overview page
- ➔ Responsibilities when handling PHI
- ➔ Patient rights: access, amendment, accounting of disclosures, and authorization requirements
- ➔ Permitted uses and disclosures of PHI

Security Rule

- ➔ HHS Overview page
- ➔ Administrative, Physical, Technical
- ➔ Reporting suspicious activity
- ➔ Culture of it being OKAY to say I am unsure and/or I did something wrong

Security Rule: Administrative

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness training
- Security incident procedures
- Contingency planning
- Evaluation
- BAAs

Security Rule: Physical

- ➔ Facility access controls
- ➔ Workstation use
- ➔ Workstation security
- ➔ Devices and media controls
- ➔ Data backup and storage

Security Rule: Technical

- ➔ Access controls (access to ePHI)
- ➔ Audit controls (monitor access)
- ➔ Integrity (not deleted or altered)
- ➔ Authentication (person/entity is valid)
- ➔ Transmission (data encryption)

Security Basics

- Security awareness
  - Password management
  - Phishing and social engineering
  - Device security
- Top Ten Data Security Best Practices for a Pediatric Practice - PCC Learn

Breach Notification Rule

- HHS Breach Notification Rule Overview
- Breach definition
- Procedures to report a breach
- Understanding impacts of a breach

Share Examples

- Share a common and uncommon (egregious) HIPAA violation
  - **no snooping**, only look at what you need to look at
  - UCLA fired 13 people for accessing Britney Spears PHI without consent
- Share how to minimize risk

Positive Compliance Culture Tips

- ➔ Speaking up is welcome
- ➔ We all want to succeed
- ➔ Protecting patient trust
- ➔ Preventing identity theft
- ➔ Avoid penalties

Discussion

What stuck out to you the most?

Sources

- Adler, S. (2025). HIPAA Training Requirements. Retrieved from https://www.hipaajournal.com/hipaa-training-requirements/
- Apex Legal Publishing. (2020). A *concise guide to HIPAA compliance an easy-to-follow guide derived from official government sources*. Akron
- Additional links provided throughout the presentation

Session Takeaways

1. HIPAA training is an ongoing, never ending journey

2. Embrace positivity, it helps!

Please complete the course survey in the UC App.

PCC Pediatric EHR Solutions

UC 2026

Asking Questions:

Virtual attendees: Use the chat if you have a question that you want answered

In-person attendees: Go to the stationary microphone in your room.

CEUs:

You can request CEU codes for qualifying sessions using the form PCC shares out at the conclusion of the conference.

Do you have any questions?