

Annual HIPAA & Security Training

2026 staff guide | Foot HealthCare Associates, P.C.

Complete this guide, then submit the separate quiz with your name, date, and signature to the practice HIPAA Compliance Officer. Ask when unsure. Report suspected incidents promptly.

1. What information do we protect?

Protected health information (PHI) is individually identifiable health information held or shared by the practice, whether in Athena, Phreesia, a paper form, a photograph, a fax, a conversation, or another medium. A name paired with care details is PHI; record numbers, appointment information, and identifying images can also be PHI. Electronic PHI (ePHI) has additional Security Rule safeguards.

- Access a chart only for a real work reason. Curiosity about a neighbor, coworker, family member, or public figure is not a work reason.
- Use information only for your assigned duties. Limit internal access and routine payment/operations disclosures to the information reasonably needed.
- The HIPAA minimum necessary standard has exceptions, including disclosures to or requests by another health care provider for treatment. Verify the purpose and recipient; do not withhold a clinically needed record because of a mistaken blanket rule.

2. When can information be shared?

Treatment, payment, and practice operations

The practice can generally use or disclose PHI for treatment, payment, and health care operations without a separate HIPAA authorization. A referral to another treating provider is a treatment disclosure. Follow practice procedures for verifying the recipient and documenting a release; escalate unusual requests.

Family, friends, and callers

When the patient is present and able to decide, ask about the patient's preference or give the patient an opportunity to object before sharing information relevant to another person's role in care or payment. Written authorization is not invariably required by HIPAA. When the patient is absent or incapacitated, the care team may use professional judgment about the patient's best interests. Follow any documented restrictions and practice identity-verification procedures. A caller knowing a patient's name is not enough by itself to justify a full chart disclosure.

Requests that need escalation

Send requests from attorneys, law enforcement, schools, media, employers, and other third parties to the designated records/privacy process. A subpoena is not an automatic instruction for front desk staff to release a chart. Marketing uses, testimonials, and public patient photos generally require a valid authorization unless a specific exception applies. Patient photos used solely for treatment are different from photos posted publicly.

3. Patient rights and sensitive records

- Route requests for access, corrections, confidential communication, restrictions, and an accounting of disclosures to the privacy/records team promptly. Do not promise an immediate denial or tell a patient that the doctor owns the record and they cannot see it.
- If a patient paid for a service in full and asks that it not be disclosed to the health plan for payment or operations, route the restriction request before billing; the practice generally must honor it unless law requires disclosure.

- Some records have additional legal protections. A diagnosis of substance use disorder does not by itself make every chart entry a 42 CFR Part 2 record. If records from a federally assisted Part 2 program are received or flagged, refer unusual release requests and any demand connected with proceedings against the patient to the privacy officer.

The 2026 Notice of Privacy Practices includes information about Part 2 records. The special 2024 HIPAA reproductive-health attestation rule was largely vacated by a court in June 2025; do not use an outdated attestation checklist as a routine disclosure rule. Ask the privacy officer about applicable current law and practice policy.

4. Everyday safeguards

- **Workstations:** lock your screen when stepping away; keep paper, labels, and fax trays away from public view. Dispose of PHI in the approved shred container, not regular trash.
- **Messages:** check the correct patient and destination before faxing, printing, scanning, or sending. Use only practice-approved systems and channels for patient information. Do not forward PHI to personal email or use unapproved personal messaging.
- **Accounts:** use your own login, keep credentials private, and follow the practice's password and multifactor authentication procedures. Do not approve an unexpected login prompt. Report suspicious links or attachments through the approved process.
- **Devices and remote work:** do not store patient files on personal devices or drives unless the practice has expressly approved and secured that workflow. Report lost devices immediately.
- **Conversations and social media:** use private spaces when practical. Do not post patient stories, images, or identifying details on social media, even if you omit the patient's name.

5. When something goes wrong

Immediately report a misdirected fax or email, the wrong chart opened, a missing paper record or device, a suspicious login or phishing interaction, ransomware, or a conversation overheard by an unintended person. Contact the practice HIPAA Compliance Officer, Joshua Fenn, at **248-258-0001**, or notify your supervisor so the report reaches him promptly. For active technical threats, also use the practice's IT escalation process.

- Preserve the basic facts: what happened, when, which information, and who may have received it. Do not delete evidence or independently promise a patient that a breach did or did not occur.
- The privacy/security team determines containment, risk assessment, documentation, and whether notice is legally required. Fast internal reporting gives them time to act.

Practice decision check

Before using or releasing PHI: (1) Is there a real work purpose? (2) Is this the correct patient and recipient? (3) Is the channel approved and the amount appropriate? (4) Is this a special request or sensitive record that requires escalation? If uncertain, pause and ask.

Sources: HHS HIPAA Privacy Rule, Security Rule, family/friends guidance, and 2026 Part 2 fact sheet. hhs.gov/hipaa/for-professionals/. This guide is staff education; follow the practice's approved policies for exact workflow.