HIPAA Training

Covered Entity

Privacy Rule – Who Is A Covered Entity (CE)?

Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity.

These transactions include **claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule**.

Using electronic technology, such as email, does not mean a health care provider is a covered entity; *the transmission must be in connection with a standard transaction***.**

PHI - Protected Health Information

Information that identifies a patient and any health condition.

ePHI – Electronic Protected Health Information

Protected health information (PHI) that is stored electronically.

As a staff member, you cannot **DIVULGE** any PHI.

This includes intentionally or unintentionally sharing patient information with:

- Family
- Spouse
- Friends of patient
- Friends of staff
- Malpractice attorney (Injury attorney is authorized of represented)
- Business associates who have not signed a Business Associate Agreement (BAA)

The only exception is when the patient has signed an authorization form.

HIPAA Office Rules

- Speak in quiet voices.
- Get permission to speak in open therapy areas.
- Offer private rooms to all patients.
- Tag patients who have sensitive conditions.
- Turn computer screens away from public.
- Use screen protectors.
- Log off computer after one minute.
- Do not autosave or share passwords.
- Do not use generic (unencrypted) email.
- Find out if office is using encrypted hard drives.
- Get Business Associate Agreements signed.
- Only send records when authorized.
- Send all records within 15 days of request.
- Report all breaches to Security Risk Official.

Communicating With Patients

- Do not discuss health condition when other patients can hear.
- This applies to when you're in/out of the office.
- Get permission to speak in common areas.
- Speak in quiet voices in the office.
- Offer private rooms to patients.
- Tag files with sensitive health information.
- Use encrypted email only.
- Never use personal email with patients.
- Inform patients to delete all emails.
- Be careful when talking on the phone.
- Do not text PHI unless written permission.

EHR – Computer, Tablet and Phones

- Turn screens away from patients.
- Use privacy screen protectors.
- Use strong passwords to logon.
- Do not save passwords on computer.
- Do not share passwords.
- Use auto log off after one minute.

Notice of Privacy Practices (NPP)

- Give all new patients an NPP.
- Us the most current DHHS version of the NPP.
- Must include office name and contact info.
- Send to patients via email.
- Must be kept in lobby.

Policies and Procedures (PNP)

- Written policies and procedures for HIPAA.
- Ask the Security Risk Official (SRO).
- Report any breaches to SRO.

Records

- Records need to be accessible to all patients.
- Must provide within 15 days of request.
- Cannot decline release of records (copies).
- Best to use EHR and open patient portal.
- Paper records should be securely stored.
- All hard drives should be encrypted.

Business Associate Agreements (BAA)

- All non-employees who have access to PHI.
- Includes all staff who are not employees.
- Billing agencies
- X-ray technicians
- Copier repair persons
- Landlords
- Attorneys – lawsuit, malpractice
- Do not need for referrals or patients attorney.

Breaches

- Report immediately to SRO immediately.
- Take immediate corrective action.
- No penalty if corrected within 30 days.
- Encrypted drives do not need to be reported.
- Over 500 people – report to HHS, patients and local media within 30 days.
- Under 500 people – report to patients and local media within 30 days. DHHS yearly

Staff Training

- Initial training - Within 60 days of employment
- As needed – breach, change in PNP's.
- At least every 2 years after initial training.
- Document when and how trained.
- Contingency/Disaster recovery plan
    - Natural disasters/Acts of terrorism
    - Post information on office website
    - Social media posts
    - Email patients
    - Contact media