Navigate the Compliance Universe

Compliance Today - August 2022
Back to basics: Privacy walk-throughs

By Jan Elezian, MS, RHIA, CHC, CHPS

Jan Elezian (jan.elezian@sunhawkconsulting.com) is a Consultant and Director at SunHawk Consulting LLC.

- linkedin.com/in/jan-elezian-30821011/

Jan Elezian

Is performing regular privacy walk-throughs required under HIPAA standards? Technically no, but to prove due diligence, a covered entity "must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information [PHI]" and have a HIPAA orientation for new employees and ongoing training for retained staff.[1] Walk-throughs create a venue for required administrative, physical, and technical safeguards to be accessed and any vulnerabilities identified and mitigated. Watching your staff in action is a great way to make sure your employees are following HIPAA standards and your facilities' privacy and security policies and procedures. A walk-through compares your privacy and security requirements with actual employee practices.

A walk-through begins by randomly choosing a physician front office, registration area, nursing station, etc. where PHI is accessed and/or stored. Carry a developed checklist with you. Mark areas assessed as compliant, partially compliant, noncompliant, or N/A (not applicable). You'll need this information for your post-assessment remediation plan. As you observe, talk to staff members, praise good practices, and teach best practices. Areas of interest to note may include:

- Notice of privacy practices:
  - Is required signage prominently posted where patient registration is performed?
  - Are notice of privacy practices acknowledgements obtained?
- Privacy/security in workstation/work areas:
  - Are patient schedules out of sight of patients or visitors?
  - Is PHI cleared from desktops?
  - Are documents securely stored in locked cabinets or boxes?
  - Are there physical restrictions to access areas containing PHI?
  - Are screen savers in use on front-facing computers?
  - Are IDs or passwords visibly written or attached to workstations?
  - Are restricted areas secured?

- Proper disposal of confidential information, PHI:
  - Are special collection bins provided and locked?
- General employee awareness:
  - Can phone calls be overheard?
  - Are all staff wearing name tags?
  - Are visitors monitored and escorted?
  - Are periodic privacy/security reminders posted and/or provided at staff meetings?
- Equipment privacy/security:
  - Are printers secured and located in a private area?
  - Are printers free from any documents waiting to be picked up?
  - Are there cover sheets on any faxes?
  - Does each user have a unique ID and password?

Take the opportunity during a walk-through to check environmental controls such as smoke, fire detectors, and presence of up-to-code fire extinguishers.

The questions provided above align with HIPAA standards that should be included in your facility's internal policies and procedures and reflect industry standards.

[1] 45 C.F.R. § 164.530(b)(c) .