Health Information Compliance Alert

Checklist: Have These Documents Handy for a HIPAA Audit

Get ahead by knowing exactly what auditors will expect.

Sure, HIPAA auditors will want you to show them a heaping mountain of documents to prove that you're complying with the Privacy and Security rules. Instead of scrambling to amass all these documents at the last minute, prepare ahead of time with a helpful checklist. Here's the specific documentation that auditors can ask for, according to an issue brief by Susan A. Miller, JD of Malvern, PA-based Malvern Group Incorporated.

HIPAA Security

- Security Officer contact information (name, email, phone, address, and admin contact info)
- Administrative Safeguards:
- Entity-Level Risk Assessment
- Organization Chart
- Information Security Policies, specifically those documenting security management practices and processes such as:
    - Access control
    - Data protection
    - Acceptable use
    - Workstation security
    - Workforce/HR security
    - Sanction procedures
- Security Incident Management Plan
- Business Continuity/Disaster Recovery Plan
- Data backup and recovery procedures
- Physical security policies and procedures
- Data destruction and media reuse procedures

Technical Safeguards:

- Encryption policies and procedures
- Management's internal control/internal audit policies and procedures relative to monitoring IT safeguards
- System-generated user access listing of all individuals with access to systems housing ePHI
- System-generated listing of all New Hires within the past year
- User authentication policies and procedures

HIPAA Privacy

- Privacy Officer contact information (name, email, phone, address, and admin contact info)
- Privacy Policy and Notice of Privacy Practices
- Privacy practices documentation including:

    - Use and Disclosure
    - Rights to Request Privacy Information
    - Right to Request Privacy Protection of PHI
    - Access of Individuals to PHI
    - Denial of Access to PHI procedures
    - Amendment of PHI

CPT® 2023 American Medical Association. All rights reserved.

- Accounting of Disclosures of PHI
- Administrative Requirements
- Transition Provisions

- Training documentation for employees over Privacy Practices and organization training policies
- Policies and procedures in place over administrative, technical and physical safeguards over all forms of PHI
- Complaint handling policies and procedures
- Population of complaints over Privacy Practices made within the past year (Complaint Log)
- Sanction and disciplinary policies and procedures over privacy violations
- Mitigation and disciplinary policies and procedures for when a breach occurs
- Anti-intimidation/anti-retaliation policies and procedures
- Policies and procedures over Uses and Disclosures of PHI, including:
  - Deceased individuals
  - Personal representatives
  - Confidential communication
  - Business associate contract requirements
  - Health Plan documentation requirements
  - Treatment, payment, and/or operation
  - Consent and authorization requirements
  - Judicial or administrative proceeding requirements
  - Research requirements
  - Approval or waiver requirements
  - De-identification/re-identification of PHI procedures
  - Restriction of PHI
  - Minimum necessary requirements
  - Limited information provided for fundraising purposes
  - Healthcare underwriting requirements
  - Identity verification procedures of individuals requesting PHI.

HITECH

- Breach notification processes and capabilities
- Entity-level risk assessment documentation

Source: Susan A. Miller, JD, Malvern Group: "Issue Brief: OCR Audit Documentation Requests What We Know Now." www.malverngroup.com/uploads/OCR_Audit_Document_Request_Brief_20120424_v_2.pdf.

CPT® 2023 American Medical Association. All rights reserved.