HIPAA documentation isn’t something you can create overnight. Here are the top 5 pieces of documentation auditors look for.

## 1. Policies and procedures

Auditors want to see...

- Recently signed agreements for all business associate relationships
- Agreements updated to include Omnibus language
- Satisfactory assurance that each business associate safeguards patient data
- Business associate risk evaluation
- Annual reevaluation of contracts

## 2. Business associate agreements (BAA)

Business associate agreements are necessary to transfer responsibility to the business associate and allow the organization to be accountable for the protection of the information.

## 3. HIPAA risk analysis

A HIPAA risk assessment identifies potential security threats that put your patients’ data and your organization at risk.

- Lists of employees with access to PHI
- Flow diagram of PHI in your environment
- Lists of systems with access to PHI (e.g., servers, workstations, laptops)
- Identified vulnerabilities, threats, and risks to patient data
- Risks, prioritized based on likelihood of occurrence and potential impact
- Privacy Rule policies (e.g., use and disclosure of PHI, NOPP)
- Security Rule policies (e.g., password requirements, encryption)
- Breach notification policies (e.g., incident management, breach processes)
- Frequent updates to policies and procedures
- Where policies are stored and how they are disseminated to staff

## 4. HIPAA risk management plan

The main purpose of a HIPAA risk management plan is to help you address identified risks. The plan should:

- Identify HIPAA risks
- Identify controls to mitigate risks
- Schedule for conducting a risk assessment and reevaluating controls
- Establish a HIPAA awareness and training program

## 5. Employee training documentation

Training helps companies meet important security guidelines and ensure that employees are aware of the policies and procedures in place.

- Regular training for all employees
- Distribution notices to ensure training completion and keep records of training conducted
- Policies and procedures for each employee
- HIPAA risk analysis for each individual
- Training plan documents
- Incidents of noncompliance with HIPAA policies
- Documentation of conducted training programs

## Auditors want to see...

- Privacy Act requirements (e.g., use and disclosure of PHI)
- Security Plan policy (e.g., written policies and procedures)
- Breach notification policies (e.g., incident management, breach processes)
- Privacy and Security policies (e.g., consent, confidentiality)
- Written policies and procedures
- Ongoing training
- Communication to patients

## 5. HIPAA documentation

Using a checklist to go through all the necessary steps for preparing documentation can help you stay organized.

### Checklist:

- Employee training documentation
- Business associate agreements
- HIPAA risk analysis
- HIPAA risk management plan
- Employee training documentation

### Tips:

- Conduct annual HIPAA training sessions for all employees
- Share HIPAA guidelines and best practices with employees
- Keep a record of all training materials and sessions
- Review and update HIPAA policies and procedures regularly

---

**Need help preparing for a successful HIPAA audit?** We can help! [hipaa@securitymetrics.com](mailto:hipaa@securitymetrics.com)

**877.384.0183**

---

Image credits: FreeImages.com