Questions for Data Collection for a HIPAA Compliance Review

Overview

Things you need to know include:

- What do you do at your office? What services do you provide?
- How many offices do you have, and how big a staff?
- What systems do you use that may touch PHI?
- Where is PHI saved?
- How does PHI move around?
- What policies and procedures do you have, documented or otherwise?
- How do you use or disclose PHI?

You will need to speak with at least three people at your office:

- The Business/Department Manager (who is supposed to know what's going on)
- IT person familiar with systems (who thinks he knows what's going on)
- The person who really knows what's going on (who has the most real experience)

The questions you want to ask them about include questions like:

- What are the policies and procedures for HIPAA?
- What happens if someone asks for a copy of all their records, or wants to make a change in their records, or otherwise wants to exert their rights under HIPAA?
- What systems are used?
- Are we using new technologies like e-mail, mobile devices, and texting?

There are three areas of inquiry:

- First, there are questions that would apply to the **organization as a whole**, such as hiring and termination practices, various policies on uses, disclosures, and patient rights, management practices, and identification of the information systems in use in the office.

- Secondly, there are questions that pertain to **each site** where services are offered. These are questions you ask at each site about office practices in privacy and security, including a physical review of security.
- Finally, there are questions that pertain to **each information system** in use, for the details of operation, access, and security.

Organization-wide Questions

The organization-wide questions fall into two categories: those pertaining to the Privacy Rule (including policies and practices regarding uses, disclosures, and patient rights), and those pertaining to the Security and Breach Notification Rules.

Privacy Rule Questions

Obtain the following information:

1. Identification of the HIPAA Privacy officer and contact information.
2. Privacy Policy (s) and Notice of Privacy Practices Privacy Practices Documentation including:
    a. Use and Disclosure
    b. Rights to Request Privacy Information
    c. Right to Request Privacy Protection of PHI
    d. Access of Individuals to PHI
    e. Denial of Access to PHI Procedures
    f. Amendment of PHI
    g. Accounting of Disclosures of PHI
    h. Administrative Requirements
3. Training documentation for employees over Privacy Practices, and organization training policy(s)
4. Policies and procedures in place over administrative, technical and physical safeguards over all forms of PHI
5. Complaint handling policies and procedures
6. Sanction and disciplinary policies and procedures over Privacy violations
7. Mitigation and disciplinary policies and procedure for when a breach occurs
8. Anti-intimidation/anti-retaliation policies and procedures

9. Policies and procedures over Uses and Disclosures of PHI, including:
    a. Deceased individuals
    b. Personal representatives
    c. Confidential communication
    d. Business associate contract requirements
    e. Health Plan documentation requirements
    f. Treatment, payment, and/or operation
    g. Consent and authorization requirements
    h. Judicial or administrative proceeding requirements
    i. Research requirements
    j. Approval or waiver requirements
    k. De-identification/Re-identification of PHI procedures
    l. Restriction of PHI
    m. Minimum necessary requirements
    n. Limited information provided for fundraising purposes
    o. Health care underwriting requirements
    p. Identity verification procedures of individuals requesting PHI

Security and Breach Notification Questions

Obtain the following information:

1. Identification of the HIPAA Security officer and contact information.
2. Overall organization-wide Entity-Level Risk Assessment
3. Information Security Policies, specifically those documenting security management practices and processes such as:
    a. Access Control
    b. Data Protection
    c. Acceptable Use
    d. Workstation Security
    e. Portable Device Policy
    f. Texting Policy
    g. Social Media Policy
    h. Workforce/HR Security: Are new employees subject to a background check? Are confidentiality agreements in place for all staff?

   i. Sanction Procedures: Are policy violations enforced with sanctions, and have any ever been applied?
4. Security training program for all staff, including annual refresher sessions. Does the training program include:
   a. Periodic security reminders
   b. Protecting systems from malicious software
   c. Log-in procedures and monitoring
   d. Password management
5. Security Incident Management Plan
   a. Is there a process in place for reporting and information security incidents, including breaches?
6. Business Continuity/Disaster Recovery Plan Data backup and recovery procedures
   a. Are there procedures to enable access to PHI in the event of an emergency?
7. Physical Security Policies and Procedures
8. Data destruction and media reuse procedures
9. Encryption policies and procedures
10. Management's internal control/internal audit policies and procedures relative to monitoring IT safeguards
11. User authentication and access control policies and procedures
   a. Is there a documented process followed when staff are terminated?
   b. Are access lists reviewed to ensure terminated staff accounts are closed, and how often?
   c. What is the process for requesting and approving access to systems?
   d. Are changes in access documented?
   e. Are there minimum password standards, and are they enforced?
   f. Are password-protected screen savers set to lock workstations automatically, and after how long?
12. For all PHI, identify the name of the system and/or the types of documents:
   a. EHR System:
   b. Practice Management System:
   c. Claims Management System:
   d. Excel Spreadsheets (list by name):
   e. Word Documents (list by type of communication):

f. Access Databases (list by name):
g. Web-based Systems (list all systems accessed over the Internet using a Web browser):
h. E-mail (identify all e-mail systems used):
i. File Server for saved documents:
j. Voicemail System:
k. Printers, Copiers, and Faxes:
l. Mobile Device Management:
m. Other systems:

13. Are there any privacy or security issues at the practice that need to be addressed?

Site-specific Questions

If you have more than one site where services are provided, these questions should be asked for each site. For each of the sites handling PHI, complete the following:

1. Name of Site (e.g., main office, satellite site X, radiology office, etc.)
2. Address:
3. Services Offered:
4. Security Observations (enter observations about any observed Security issues, such as physical or environmental vulnerabilities):
5. History of Security Issues at this site (break-ins, fire/water damage, incidents needing police, etc.):
6. Known Security Issues:
7. Who has keys to open the building/offices, and are they well-controlled, and changed when a key-holder leaves the organization?
8. Is there a facility security plan (such as how the site is secured in off-hours, reviews of any security tapes, planning for increased security, etc.)?
9. Is there a burglar alarm and/or recorded video surveillance?
10. Are all entrances monitored in-person by staff or by monitored video cameras?
11. Is there a plan for accessing the facility for purposes of disaster recovery following an emergency, perhaps as part of an overall disaster recovery plan?
12. Do staff, visitors, and vendors wear identification while on premises?

13. Are repairs and modifications to physical security documented? Is there a record of changes to locks, windows, and doors?
14. Are workstations, printers, and fax machines in protected areas and used securely? Are computer screens turned so others can't see them, or do they have view-blocking screens? Can people other than staff access or see what's in a printer or fax machine easily?
15. Where are all on-site servers and network hardware located; is it routinely kept secured?
16. Any other site-specific privacy or security issues?

System-oriented Questions

For each of the information systems handling PHI identified in the organization-wide listing, detail information on each system needs to be collected.

1. System Identification
    a. Name of System and current installed version number:
    b. Informal System Name:
    c. How long system has been in use:
    d. Type of Information:
    e. Type of System (select letter from the key below):
        A: Access control/management
        B: Internally hosted systems and interconnections (like a major, central EHR)
        C: Externally hosted systems and interconnections
        D: Locally used spreadsheets, documents, and databases
        E: Office systems (e-mail, servers, workstations, etc.)
    f. Primary Location of System (local, at a Business Associate, in the cloud):
    g. Primary Location of Data Storage (server, local drive):
    h. System Technical Manager (and phone/e-mail):
    i. System Responsible Manager (and phone/e-mail):
    j. Contractor/Vendor Involved with System (and phone/e-mail):
    k. Is a Business Associate Agreement in place with contractor/vendor?
2. System Description (one or two sentences about the function and purpose of the system, how it is normally used, the organizational business processes supported, and related systems)
3. Information Flow Description (narrative about how information is used and moves around)

4. Incoming or Imported Information (enter list of incoming or imported information here, also network or system interconnects, also whether or not transmissions are encrypted, and how)
5. Information Created In This System (enter list of information created in this area used by the subject system)
6. Exported Information (enter list of information exported from this system, also network or system interconnects, also whether or not transmissions are encrypted, and how)
7. Stored Information (enter list of information stored by this system, also whether or not stored data are encrypted, and how)
8. Remote Access Permitted? (yes/no; if yes, who and how)
9. Is Portable Data used (USB stick, smart phone, CD, DVD, etc.)?
10. Is portable data encrypted? (y/n/na; if yes, how)
11. Any Security Incidents?
12. Any security issues or concerns?
13. Information Security Level (choose Moderate or High)
14. Criticality of PHI retained by the system (choose Low, Moderate, or High)
15. Are all accesses authenticated to an individual, and are logons NOT shared?
16. What are the means in place to ensure PHI has not been inappropriately altered?
17. Does this system track log-ons, and how?
18. How long is the audit log retained?
19. Who reviews the audit logs of this system?
20. How often are audit logs reviewed?
21. Which of the following activities may be audited for this system?
    A. Date and time of significant activity
    B. Origin of significant activity (workstation)
    C. Identification of significant activity
    D. Description of attempted or completed significant activity
    E. Documents printed
22. Who supervises the staff using this system?
23. Does this system automatically disable unused accounts?
24. Is the list of active users reviewed regularly?
25. Is there regular, secure, tested backup of this system's information?
26. Is there a tested disaster recovery plan in place for this system?

27. Does this system have an automatic time-out or log-off?
28. Are old media destroyed or cleared before re-use?
29. Who is responsible for maintaining records of the movement of hardware and software?
30. Information Flow Diagram (attach, optional)

Questions About Business Associates

If you hire contractors who create, receive, maintain, or transmit PHI on your behalf, or need your PHI to do their job for you, they act as HIPAA Business Associates. You must establish proper HIPAA Business Associate Agreements (BAAs) with those vendors who act as Business Associates.

Business Associates must abide by the HIPAA Security and Breach Notification rules, and limit their uses and disclosures to only those allowed in the agreement, according to your policies in support of the Privacy Rule. You need to document who your HIPAA Business Associates are, what they do, how they interact with you, and the HIPAA Business Associate Agreements you have with them.

In addition to the requirements spelled out in a BAA, for some Business Associates it will be a good idea to ask additional questions similar to those laid out by NIST in their guidance on HIPAA and Mobile Devices, SP 1800-1e[1]. A set of questions for a BA who provides information system services based on that guidance can include the following:

1. Vendor Agreements
    a. Is the vendor willing to sign a comprehensive business service agreement?
    b. Is the vendor willing to confirm compliance with HIPAA Privacy and Security Rules, and willing to be audited, if requested?
2. Third-party Application Integration
    a. Does the health care organization need to integrate the system with other in-house products, such as practice management software, billing systems, and e-mail systems?
    b. If integration of the system to in-house applications is needed, what are the implementation procedures and techniques used? What security features protect the data communicated among different systems?

[1] https://nccoe.nist.gov/sites/default/files/nccoe/NIST_SP1800-1e_Draft_HIT_Mobile-Risk.pdf

3. Personal or Device Authentication and Authorization
    a. Does the vendor restrict the type of mobile devices that can access the system?
    b. Are mobile devices subject to some kind of mobile device management control for enforcing device security compliance?
    c. Are there security compliance polices for using a personal device to access the system?
    d. If a portable device is lost, stolen, or found to be hacked, are there any countermeasures in place to avoid protected data from becoming compromised?
    e. Does the system require a user to be authenticated prior to obtaining access to PHI?
        i. What authentication mechanisms are used for accessing the system?
        ii. Are user IDs uniquely identifiable?
        iii. Is multifactor authentication used? Which factors?
        iv. If passwords are used, does the vendor enforce strong passwords and specify the lifecycle of the password?
    f. Does the system offer a role-based access control approach to restrict system access to authorized users to different data sources?
    g. Is the least privilege policy used? (A user of a system has only enough rights to conduct an authorized action within a system, and all other permissions are denied by default.)
4. Data Protection
    a. What measures are used to protect the data?
    b. What measures are used to protect the data from loss, theft, and hacking?
    c. Does the system back up an exact copy of protect data? Are these backup files kept in a different location, well protected, and easily restored?
    d. Does the system encrypt the protected data while at rest?
    e. What happens if the vendor goes out of business? Will all clinical data and information be retrievable?
    f. Does the vendor have security procedures and policies for decommissioning used IT equipment and storage devices that contained or processed sensitive information?
5. Security of Data in Transmission
    a. How does the network provide security for data in transmission?
    b. What capabilities are available for encrypting health information as it is transmitted from one point to another?

   c. What reasonable and appropriate steps are taken to reduce the risk that PHI can be intercepted or modified when it is sent electronically?

6. Monitoring and Auditing
   a. Are systems and networks monitored continuously for security events?
   b. Does the vendor log all the authorized and unauthorized access sessions and offer auditing?
   c. Does the system have audit control mechanisms that can monitor, record, and/or examine information system activities that create, store, modify, and transmit protected health information?
   d. Does the system retain copies of its audit/access records?
   e. How does the vendor identify, respond to, handle, and report suspected security incidents?
7. Emergencies
   a. Does the vendor offer the ability to activate emergency access to its information system in the event of a disaster?
   b. Does the vendor have policies and procedures to identify the role of the individual responsible for accessing and activating emergency access settings, when necessary?
   c. Is the system designed to provide recovery from an emergency and resume normal operations and access to protected health information during a disaster?
8. Customer and Technical Support
   a. What is included in the customer support / IT support contract and relevant service level agreements?
   b. Can the vendor provide a written copy of their security and privacy policies and procedures (including disaster recovery)?
   c. How often are new features released? How are they deployed?

