HIPAA Security Audits: How to Get Your Organization Ready

Your organization is HIPAA compliant. Oh, really?

By Chad Peterson, CHC, CHP, CHSS, CISA, CISSP, CRISC, CSCS, ITIL-Foundation; and Derek Woo, MCP, CNE

Executive Summary

Is your organization compliant with the Health Insurance Portability and Accountability Act (HIPAA) Security regulations? Are you doing everything you are expected to do on a yearly basis to ensure patient data is protected? Who has access to patient data? Who is accessing data without authorization? What are your organization's biggest risks when it comes to patient data?

With an established and implemented HIPAA Security Audit plan for your organization, you will be able to confidently answer these questions and truly know what the organization's major risks are in protecting patient health information.

HIPAA Privacy and HIPAA Security are closely related; to successfully audit an organization for HIPAA Security, you need to understand HIPAA Privacy as well.

The HIPAA Privacy Rule addresses the use and disclosure of an individual's protected health information (PHI) by organizations that are subject to the Privacy Rule. Such organizations are referred to as Covered Entities. PHI refers to patient information in any form—written, electronic or even spoken.

Essentially, the Privacy Rule states that a Covered Entity must obtain written authorization from the patient to disclose to an entity any PHI that is not for treatment, payment or healthcare operations.

The HIPAA Security Rule is comprised of three areas that outline how PHI should be protected by the Covered Entity:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

The three areas stipulate safeguards that need to be in place to minimize the risk of PHI falling into the wrong hands in what is termed a "breach." A breach can occur when a device containing PHI, such as a laptop, is lost or stolen. Breaches also refer to information sent or provided to a wrong person in error. The HIPAA Security Rule's purpose is to ensure that measures are taken to protect the integrity of the patient information.

The difference between the Privacy and Security Rules is the Privacy Rule states *what needs to be protected* and the Security Rule provides *guidance on how to protect* information stored electronically.

HIPAA Security Rule

Before an audit plan can be created to assess how an organization is complying with the Security Rule, you need to understand what the Security Rule and the associated safeguards are addressing.

HIPAA Security provides a set of guidelines to protect PHI that is in an electronic format, known as Electronic Protected Health Information (EPHI). Each of the three safeguards has standards, and each standard has one or more implementation specifications. The implementation specifications provide the key areas upon which to base your audit plan.

> The Privacy Rule states *what needs to be protected* and the Security Rule provides *guidance on how to protect* information stored electronically.

The area of implementation specifications is a source of confusion. Each specification is categorized as either Required (R) or Addressable (A). The term "Required" is simple to understand—these specifications must be met as stated in the Security Rule. The term "Addressable" is often thought to be optional, but that is not the case. When an implementation is categorized as "Addressable," it means you have four options:

1. Assess whether the specification is "reasonable and appropriate" for your environment.
2. An alternative security measure can be substituted.
3. A combination of an alternative security measure and the addressable implementation specification can be used.
4. Choose not to implement the addressable implementation specification.

When an addressable implementation specification is put into place, if it is not based on the above options, there *must be documentation available for each specification stating why that decision was made.*

Additional information and specifics on each of the Security Safeguards is on the CMS website (cms.gov/hipaageninfo/).

The final Security Rule includes additional required areas of Risk Analysis, Risk Management and Sanction Policy to go along with the aforementioned safeguards.

When you create an audit plan for HIPPA Security, all of the above components need to be assessed.

How to develop a HIPAA security audit plan

As with any IT based audit, there are essential items that are a part of the audit checklist. The basic audit steps remain the same:

1. Contact key administration & IT director(s).
2. Schedule the fieldwork.
3. Send the pre-audit questionnaire.
4. Send the document request list.
5. Review questionnaire responses and documentation.
6. Perform fieldwork.
7. Interview key personnel.
8. Conduct a walkthrough.
9. Document observations and conclusions.
10. Write report.
11. Schedule exit conference.
12. Hold exit conference.
13. Issue report.

The following steps summarize the specifics for a security audit.

> *The term "Addressable" is often thought to be optional, but that is not the case.*

Contact key administration and IT director(s)

Baseline audit – Here is your opportunity to conduct an orientation with key organization administration and IT director(s) to ensure everyone is aware of the HIPAA regulations and has a basic understanding of what is required for both HIPAA Privacy and Security rules.

Now is the time to set the expectations of the audit. Share the audit plan as it pertains to each of the audit areas and to explain the overall audit process.

Follow-up audit – During conversations, review any changes to the regulations and the risk environment since the previous audit, share new audit tools and set the current audit expectations.

Schedule the fieldwork

Now is the time to meet with key contacts for interviews, shadowing and walkthroughs. Meetings should be scheduled with the key administration and IT personnel as well as others identified by area leadership.

Send the pre-audit questionnaire

Baseline audit – When the questionnaire is sent for the first time, some training with the recipients will be needed on what is expected and how the process works. You will often discover you need to start with basic training on HIPAA Security for some individuals and groups.

An example of a HIPAA Security questionnaire and a HIPPA Security Rule

Technical safeguards	
Access Control: "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308 (a)(4)[Information Access Management]."	164.312(a)(1)
Unique user identification: "Assign a unique name and/or number for identifying and tracking user identity."	164.312(a)(1) - R
Emergency access procedure: "Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."	164.312(a)(1) - R
Automatic logoff: "Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."	164.312(a)(1) - A
Encryptions and decryption: "Implement a mechanism to encrypt and decrypt electronic protected health information "	164.312(a)(1) - A
Audit controls: "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."	64.312(b) - R
Integrity: "Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."	164.312(c)(1)
Mechanism to authenticate Electronic Protected Health Information: "Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."	164.312(c)(1) - A
Person on entity authentication: "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."	164.312(d) - R
Transmission security: "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."	164.312(e)(1)
Integrity controls: "Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detections until disposed of."	164.312(e)(1) - A
Encryption: "Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."	164.312(e)(1) - A

Toolkit (HSR Toolkit) can be found at the NIST website (scap.nist.gov/hipaa/). The kit provides a documentation tool that can be used when conducting an audit.

Follow-up audit – For these audits, it is important to prepare the questionnaire with the responses from the previous year while including a column for the current year's responses. During the follow-up audit, a good practice is to remind everyone where the organization was a year ago and to gauge the progress made since.

Send the document request list

Baseline audit – The Document Request List (DRL) is a key tool for a successful audit. If the right documents are not requested, there is a risk that correct information might be missed.

The documents to collect include:

1. HIPAA policies and procedures
2. Security plan
3. Most recent risk assessment or risk analysis
4. Security incident reports
5. Organization charts
6. Business continuity and disaster recovery plans
7. Data back-up procedures

Follow-up audit – When conducting a follow-up audit, you should use the baseline DRL and request all updated documents or any additional documents required because of changes to the regulations.

Review questionnaire responses and documentation

Your review of the questionnaire responses, along with the information collected from the DRL, are the keys to a successful audit. At this point additional interview questions can be formulated and workflows and processes can be learned. The bulk of the information used to determine compliance is obtained at this step in the audit process. It is important to plan enough time to thoroughly read and understand all of this information.

Perform fieldwork

When conducting fieldwork, the information you received in the DRL and questionnaires needs to be verified. You can do this by observing workers, ensuring policies and procedures are followed as written, and by asking questions of employees. During this phase of the audit, it is common to request additional information to supplement the items requested in the original DRL and to ask follow-up questions about policies and procedures.

Interview key personnel

When conducting interviews, you should speak with all key personnel in the organization. It does not mean you need to speak with executive leadership and the board. It does mean that for each type of audit, the key individuals who have a vital role in the process being audited are included. CMS includes a list of key individuals to interview for a Security audit. The individuals include:

1. HIPAA Compliance Officer
2. Lead Systems Manager or Director
3. Systems Security Officer
4. Lead Network Engineer
5. Disaster Recovery Specialist
6. Facility Access Control Coordinator
7. Director of Training
8. Incident Response Team Leader

Conduct a walkthrough

During a walkthrough for a Security audit, your objective is to evaluate the presence of physical and logical HIPAA Security compliance requirements, as well as the workforce's awareness of security practices.

Items to include in the walkthrough observations:

- Data center safeguards
  - *Administrative* – policies and procedures (e.g., user access, system usage, policy and procedure enforcement, incident response, etc.)
  - *Physical* – facility security, securing equipment and media, procedure enforcement
  - *Technical* – firewalls/intrusion detection systems, virtual private networks (VPNs)/secure portals for remote devices (PCs, tablet computers, smartphones and other portable devices)
- Network closet safeguards
- Workstation security
- Mobile device security – Smartphones, tablets and other portable computing devices
- Computer-on-wheels (i.e., point-of-care mobile workstation) security
- Workforce awareness

Use the implantation specifications as a guide when conducting walkthroughs.

Document observations and conclusions

The documentation phase should include an evaluation of the responses to the HIPAA Security questionnaire with a

For a HIPAA Security Audit

Some help is provided by the Centers for Medicare and Medicaid Services (CMS) form *Sample Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews*. The document can be obtained on the AHIMA site at library.ahima.org/xpedio/groups/public/documents/government/bok1_039154.pdf.

score for each element. You will also want to include observations from the walkthrough compliance, including gaps, concerns and follow-up questions that need to be addressed.

The documents you create should be used as reference for future follow-up audits; therefore, it is critical these notes are clear and detailed.

Write report

Baseline audit – The report you create for the Security audit should describe the compliance gaps and concerns and include recommendations to address the gaps and concerns that have been noted. Your report should also include an action plan that includes suggested timelines for remediation, including ownership for the remediation.

Follow-up audit – Your follow-up report should include everything in the baseline report with respect to the current gaps, concerns and action plan. Include status updates from the previous year's findings.

Obviously, the purpose of your Security audit is to identify compliance gaps within the organization, but your report is also an excellent opportunity to include suggestions for program improvements. The suggestions should point out where the organization can improve on its compliance and where it can move to into areas of best practices.

Schedule exit conference

You should schedule the exit conference as soon as possible after the completion of the report. The audience for the conference should include the key stakeholders from compliance management, IT management and hospital administration. Other key individuals and functions should also be considered, as necessary.

> ***Compliance programs should include a combination of ongoing monitoring and periodic audits.***

Hold exit conference

The purpose of the exit conference is to review the findings of your audit report with the key stakeholders. Each finding and recommended remediation should be explained to the attendees' satisfaction.

The action plan should be discussed in detail and agreed upon by the attendees. At the conclusion of the meeting, all parties should agree on how to address compliance concerns, the necessary corrective action to be undertaken and the timeframe for doing so.

Issue report

After the exit conference, any amendments to the report should be made and the agreed-upon action plan and dates should be included. At this point, the report is considered final and should be issued to those who attended the exit conference and any other designated individuals. A copy of the report should also be retained for use in the next year's audit.

Conclusion

A formal HIPAA Security audit plan will assist the organization in recognizing where it stands from a compliance perspective. Audits are one tool that can be used to ensure everything is being done to protect EPHI and to ensure compliance with the HIPAA Security Rule.

Audits tell an organization where it is at a point in time and identify gaps and concerns. Audits, of course, cannot identify issues that occur after the fact. Therefore, all compliance programs should include a combination of ongoing monitoring and periodic audits.

Using the results of audits can provide a means for establishing an effective ongoing monitoring process for the organization. The combination of monitoring and audits will assure the organization will remain at a high level of compliance. **NP**

Authors

Chad Peterson, CHC, CHP, CHSS, CISA, CISSP, CRISC, CSCS, ITIL-Foundation, is a Senior Manager of Healthcare Information Technology at Sinaiko Healthcare Consulting. Chad and Derek work with organizations of all sizes on operations improvement strategies, regulatory compliance and healthcare technology solutions and architecture. Chad can be reached at Chad.Peterson@sinaiko.com or (310) 776-4500.

Derek Woo, MCP, CNE, is Managing Director of Revenue Cycle and HIT services at Sinaiko Healthcare Consulting. You can reach Derek at Derek.Woo@sinaiko.com or (510) 913-2534. For more information, please visit www.altegrahealth.com/sinaiko.

> ***We all need lots of powerful long-range goals to help us past the short-term obstacles.***
> **~Jim Rohn**