Five Ways to Create a More Dynamic HIPAA Security Program

1. Document your Security Program in Comprehensive & Detailed HIPAA Security Policies

HIPAA covered entities and their business associates must have HIPAA security policies. Each policy should:

- List the specific HIPAA standard you are implementing;
- Identify the "why" for the policy (i.e., preventing unauthorized users from accessing ePHI");
- Outline very specifically how the organization is implementing the standard;
- If the HIPAA Security Rule makes the implementation specification for a specific standard "addressable" and you're not implementing the addressable specification, make sure your policy details the specific alternative you've chosen to implement instead; and
- Identify the specific person or people within the organization responsible for each policy and/or each component of the policy.

Importantly, your HIPAA security policies should track the HIPAA Security Rule and you should have a specific policy and documented processes for each HIPAA standard and implementation specification within that standard, including alternative specifications if you have decided the addressable specification is not reasonable and appropriate for your organization. Ideally, an outsider could pick up your HIPAA security policies and understand everything your organization is doing at that moment to safeguard protected health information and the totality of your security practices.

2. Establish an Ongoing & Robust Risk Analysis

Make sure you have a risk analysis policy that requires the organization to conduct a comprehensive risk analysis and specifies how frequently you review and update it. At a minimum, your risk analysis should be done once every three years but consider whether that's often enough or whether annually or every two years may be more reasonable for your organization. Even though you'll set the cadence for the frequency of your comprehensive risk analysis, you should think of your risk analysis as "ongoing". Your risk analysis policy should outline when the risk analysis or portions of it will be repeated in response to a change in circumstance or significant event.

If you haven't done a risk analysis previously or if you're not sure you're conducting an adequate risk analysis, review OCR guidance and **recommended resources here**.

Your risk analysis should include:

- Preparing by conducting a technology asset inventory and determining whether ePHI is transmitted to external parties, such as cloud service providers;
- Ensuring all ePHI your organization creates, receives, transmits, or maintains is considered in the risk assessment;
- Creating an assessment of the documented security measures you use to ensure your policies protect your ePHI;
- Identifying reasonably anticipated threats, potential vulnerabilities, and pre-disposing conditions and assigning a likelihood value to each threat by determining the likelihood that a threat would exploit a vulnerability and result in an adverse effect so that you have documentation of all threat and vulnerability combinations with associated likelihood estimates;
- Determining the impact of a threat exploiting a vulnerability, including assessing the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability so that you have documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities;
- Determining the level of risk to ePHI while considering the information gathered and determinations made during the previous steps so that you have documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level; and
- Documenting the risk assessment results.

Consider creating a "network map" to inform your risk analysis. A network map builds on your technology asset inventory to illustrate the movement of ePHI through your electronic information system.

3. Develop a Cadence for Evaluating your Security Policies & Procedures

Review your HIPAA security policies and procedures on a regular cadence, including:

- On an annual basis;
- As part of your risk analysis, making sure each policy ties back to and cites to anything in your most recent risk analysis the policy is aimed at addressing; and

- In response to changes, both internally and externally.

To ensure your policies get timely evaluated and updated when needed, consider an index that identifies which policies need to be updated in light of specific events. For example, if the organization implements new hardware, identify which policies will need to be reviewed and revised. Or, consider assigning responsibility to various policies within your compliance or IT teams.

4. Implement Testing and Auditing to Assess your Security Program and Identify and Resolve Weaknesses

Conducting periodic testing of your security measures, contingency plans and incident response procedures as well as auditing compliance with your HIPAA security policies can ensure that you identify and correct problems before those problems lead to costly security breaches. Routine testing and auditing can help identify weaknesses, non-compliance and security measures that don't work as intended. Adopt an annual audit and testing plan informed by your risk analysis, emerging threats, or recent enforcement actions. Rotate through your security measures and policies to ensure over time all aspects of your security program are audited or tested.

For any identified weaknesses, non-compliance, or ineffective security measures, determine how these issues will be resolved in a manner that's reasonable and appropriate for the organization and update your policies to reflect these changes.

5. Review Existing and Emerging Technology Available to Safeguard Data and Document Your Decision-Making Process and Rationale

The tools available to regulated entities to secure data are rapidly evolving. Any HIPAA security program needs to routinely evaluate the technology available to safeguard data and determine what is reasonable and appropriate for the organization. This process should be part of your comprehensive risk analysis but also something you're doing on an annual basis. By conducting a deliberate, thoughtful review of the technology available to safeguard data that considers and documents the benefits, the cost and other drawbacks, and the organization's ultimate decision on implementation, you can help ensure the organization is implementing reasonable and appropriate security measures.

Questions to ask yourself as part of this annual process include:

- What technology is available to safeguard sensitive data such as protected health information which our organization is not using or has not fully embraced?
- What are the benefits of this technology?
- What are the costs or other downsides of using this technology?

- Is the decision not to utilize or fully embrace this technology still reasonable and appropriate and why?
- What would need to change for us to reconsider this decision?
- What alternatives are we using instead?

OCR doesn't expect providers to implement any available technology regardless of the cost; however, it does expect that you'll implement reasonable and appropriate security measures. Whether something is reasonable and appropriate likely changes over time and it is important the organization is routinely evaluating and documenting its decisions.