Compliancy Group

How to Complete Your Security Risk Assessment

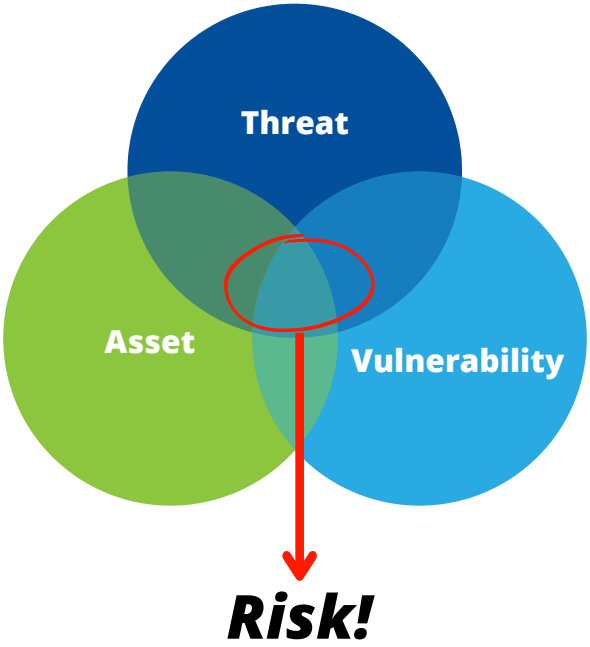
A COMPREHENSIVE GUIDE.

What is a Security Risk Assessment?

The HIPAA Security Rule requires that covered entities and business associates implement security safeguards.

These security safeguards must protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). ePHI is any protected health information that is created, stored, transmitted, or received in any electronic format.

Performing a security risk assessment (SRA) is the first step in identifying and implementing these safeguards.



What is the Scope of a Security Risk Assessment?

According to guidance issued by the Department of Health and Human Services (HHS), the scope of security risk assessment includes potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that an organization:

- Creates;
- Receives;
- Maintains; and
- Transmits

This includes ePHI in all forms of electronic media. Types of electronic media include hard drives, CDs and DVDs, smart cards, personal digital assistants, and portable electronic storage devices.

The term “electronic media” is defined broadly, to include something as small as a single workstation, up to something as large complex networks connected among multiple locations.

Security risk assessments must take into account all ePHI, regardless of the medium in which it was created, received, maintained, or transmitted, and regardless of its source or location.

Did you know: A security risk assessment is an annual requirement.

The Elements of a Security Risk Assessment

Security risk assessments include six elements:

- Collecting Data
- Identifying and Documenting Potential Threats and Vulnerabilities
- Assessing Current Security Measures
- Determining the Likelihood of Threat Occurrence
- Determining the Potential Impact of Threat Occurrence
- Determining the Level of Risk

Element 1: Collecting Data

To begin the security risk assessment, an organization must identify where its ePHI is stored, received, maintained, or transmitted. It can do this in several ways, by:

- Reviewing past or existing projects
- Performing interviews
- Reviewing documentation.

The data gathered on the ePHI gathered during data collection must be documented.

Element 2: Identifying and Documenting Potential Threats and Vulnerabilities

An organization must then identify and document threats to ePHI that are reasonably anticipated. Organizations must also identify and document vulnerabilities, which, if triggered or exploited by a threat, would create a risk of improper access to or disclosure of ePHI.

The Elements of a Security Risk Assessment Continued

Element 3: Assessing Current Security Measures

For this part of the security risk assessment, organizations should address their "state of security." They should do so by:

- Assessing and documenting the security measures they use to safeguard ePHI.
- Assessing and documenting whether security measures required by the Security Rule are already in place.
- Assessing and documenting whether current security measures are configured and used properly.

Element 4: Determining the Likelihood of Threat Occurrence

Organizations must then assess the likelihood of potential risks to ePHI. The results of this assessment, combined with the list of threats identified in element 2, will reveal what threats should be regarded as "reasonably anticipated."

Element 5: Determining the Potential Impact of Threat Occurrence

After an organization determines the likelihood of threat occurrence, it must assess the impact of potential threats to confidentiality, integrity, and availability of ePHI. This can be done by assessing the severity of the impact resulting from a threat that triggers or exploits a vulnerability. The assessment should be documented.

A useful way to document impact severity, is by describing the severity numerically (i.e., assigning a number to how severe an impact is, on a scale of 1 to 10, with 10 being "most severe").

The Elements of a Security Risk Assessment Continued

Element 6: Determining the Level of Risk

The level of risk is determined by evaluating ALL threat likelihood and threat impact combinations identified in the risk assessment so far. The level of risk is highest when a threat 1) is likely to occur; AND 2) will have a significant or severe impact on an organization.

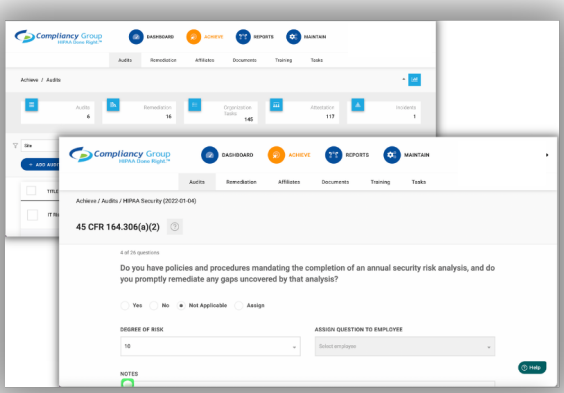
For example, if a network is completely unsecured, and that network stores all of the organization's ePHI, two things are likely to happen: A threat will occur, and its occurrence may have a severe impact on the organization. When threat likelihood and severity are both high, the level of risk should be classified as "high."

On the other hand, if there is a low risk of a threat occurring, AND the threat's occurrence will have little to no impact on the organization, the level of risk is relatively low.

Once the organization has assigned risk levels, it should document those levels, and document what corrective actions are needed.

Finally, once all six elements have been addressed, all documentation should be finalized. In addition, the security risk analysis should be periodically reviewed, and updated, as needed.

Compliance Software & Coaching



Compliancy Group Simplifies HIPAA Compliance

Overwhelmed by all you have to do for your security risk assessment? Covered entities and business associates can address their security risk assessment by working with Compliancy Group to address federal HIPAA security standards. Completing a security risk assessment is **required** to become HIPAA-compliant and we make it easier!

Our live coaching and web-based compliance app, The Guard™, gives health care organizations the tools to address HIPAA Security Rule standards so they can get back to confidently growing their business.

Contact Us

888-979-8880

kaizenHIPAA.com

wgordon@kaizenHIPAA.com