WHAT ARE THE ELEMENTS OF A HIPAA SECURITY RULE RISK ASSESSMENT?

1

COLLECTING DATA

To begin the security risk analysis, an organization must identify where its ePHI is stored, received, maintained, or transmitted. A covered entity or business associate may do this in several ways, which include:

REVIEWING PAST OR EXISTING PROJECTS

PERFORMING INTERVIEWS

REVIEWING DOCUMENTATION

2

IDENTIFYING AND DOCUMENTING POTENTIAL THREATS AND VULNERABILITIES

Next, the covered entity or business associate 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.

3

ASSESSING CURRENT SECURITY MEASURES

- Covered entities' and business associates' documenting the security measures they currently use to safeguard ePHI.
- Covered entities' and business associates' assessing and documenting whether the security measures required by the Security Rule are already in place.
- Covered entities' and business associates' assessing and documenting whether their current security measures properly configured and used.

4

DETERMINING THE LIKELIHOOD OF THREAT OCCURRENCE

Covered entities and business associates must next assess the likelihood of potential risks to electronic protected health information. The results of this assessment, combined with the list of threats identified in element 2, above, will reveal what threats the covered entity or business associate should regard "reasonably anticipated."

5

DETERMINING THE POTENTIAL IMPACT OF THREAT OCCURRENCE

After the covered entity or business associate determines the likelihood of threat occurrence, it must then, as part of the HIPAA risk assessment, assess the impact of potential threats to confidentiality, integrity, and availability of ePHI.

This assessment is performed by evaluating the severity of the impact resulting from a threat that triggers or exploits a vulnerability. The evaluation 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").

6

DETERMINING THE LEVEL OF RISK

The final risk analysis step of the HIPAA risk assessment consists of determining the level of risk. The level of risk is determined by evaluating ALL threat likelihood and threat impact combinations identified in the risk analysis to this point.

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 an organization's network is completely unsecured, and that network stores all of the organization's ePHI, there is a high level of risk both that:

- *A threat will occur; and*
- *The occurrence of the threat may have a sever impact on the organization*

When threat likelihood and severity are both high, the level of risk should be classified as "high." Conversely, 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 for each level.

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.

WILLETTS TECH
I.T. FOR HUMAN SERVICE
301-722-5800
www.willettstech.com