Do You Need a **HIPAA Gap Analysis,** a **HIPAA Risk Assessment,** or a **Security Frameworks Assessment?**

Lumen21

Ask any IT department what is **required to comply with the HIPAA Security Rule,** and you'll likely hear things like data encryption, unique user IDs, and strong passwords. You might even hear about documented policies, anti-virus software, and removable media controls. But you are less likely to hear about the first required specification in the HIPAA Security Rule, **a risk analysis.**

The **HIPAA Security Rule (45 CFR 164.308(a)(1)(ii)(A))** states companies complying with HIPAA must: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

The statement seems clear, but the implementation is not always so obvious. Identifying all the potential risks can be a daunting task, so many companies choose to hire experts to perform this work. But what are you really getting? Some companies may suggest a **HIPAA Gap Analysis, others may offer a HIPAA Risk Assessment or a Security Framework Assessment.** Each can provide value to your organization, but it is important to understand the differences.

HIPAA Gap Analysis

The HIPAA Gap Analysis is usually the least expensive of these options and is often appropriate as a starting point for a company trying to determine their current level of HIPAA compliance, but it is the one that is least likely to meet the requirements of 45 CFR 164.308(a)(1)(ii)(A). A gap analysis will provide a **review of your existing administrative, physical, and technical controls** to determine if they meet the requirements in the HIPAA Security Rule. The gap analysis usually **includes a mapping of the company's security policies, procedures, and security controls** against the HIPAA specifications. In addition to mapping the gap analysis should (but doesn't always) include a review of the policies, procedures, and controls for adequacy with recommendations for improvement. There also may be a **review of the vendor management documentation,** including the Business Associate agreements, as part of the HIPAA contracting requirements. A more in-depth gap analysis even identification of vulnerabilities and testing of controls.

Whether the gap analysis is limited to mapping existing policies, procedures, and controls against the HIPAA Security Rule, or some identification and control testing, the gap analysis is not "an accurate and thorough assessment of the potential risks and vulnerabilities" of protected health information (PHI) for one simple reason. The HIPAA Gap Analysis **assesses the company's compliance with the HIPAA Security Rule, rather than assessing the potential risks to the data.** Compliance with the HIPAA Security Rule **does not** address all potential risks to the data. **It is possible to be HIPAA compliant without being secure.**

HIPAA Risk Assessment

The HIPAA Risk Assessment **may include the features in the gap analysis,** but will expand beyond simple compliance with the HIPAA Security Rule to **concentrate on the company's ability to maintain the confidentiality, availability, and integrity of any protected health information.** Note that under this definition, a HIPAA Risk Assessment **may not assess all the risks to the company,** but is restricted to the systems that contain protected health information or have access to those systems. Determining risk can be boiled down to an equation:

Threat x Vulnerability x Impact = Risk

At the most basic level, **threats are anything that can cause harm to the company if they can exploit a vulnerability in the security controls.** Threats can be external, such as *a hacker, a virus, an earthquake, or a fire.* Threats can also be internal, such as *a failed upgrade, a disgruntled employee* or simply *an employee who circumvents the security controls* for the sake of convenience.

Vulnerabilities are weaknesses in the security controls that can be exploited by the threat.

There are obvious vulnerabilities such as *unpatched systems, uncontrolled removable media, and poorly configured firewalls.* But there are less obvious vulnerabilities as well. These can be *inconsistent processes for providing access to systems or for collecting and reviewing logs, insufficient policies, or lack of management oversight.*

The impact of a threat exploiting a vulnerability depends on the potential damage that can be caused.

The failure of an upgrade and resulting outage on a critical business system will have a much greater impact than the upgrade failure of a less consequential system. The potential loss of a single record will have a significantly lower impact than the potential loss of an entire database. Impact can be considered in numeric terms, such as time to recovery, amount of data loss, or dollar cost to the business. Impact can also be considered in qualitative terms, such as high, medium, or low impact if accurate numbers are not available.

Performing a HIPAA Risk Assessment is a time-consuming and resource-intensive undertaking in order to meet the Security Rule requirement for an accurate and thorough assessment.

Security Framework Assessment

A **security framework is a collection of controls that are designed to reduce the likelihood of a system having vulnerabilities that can be exploited by threats.** Common security frameworks include *ISO 27002 Code of Practice for Information Security Controls or NIST CyberSecurity Framework for critical infrastructure.* A security framework is based on a **comprehensive risk assessment that identifies the potential threat universe and potential vulnerabilities**, then develops a set of security controls that, if deployed effectively, will **reduce or eliminate the exploitation of vulnerabilities.** A Security Framework Assessment determines whether the correct controls have been implemented according to the framework, and whether are not they are being managed correctly. If the security framework is designed to address HIPAA compliance as well as protect against potential threats, **it will address both the elements of the gap analysis and the risk assessment.**

A company undergoing a Security Framework Assessment, if performed by an authorized assessor, can have their compliance with the framework validated. **This independent certification can provide customers with a level of assurance that the company can protect their data.**

A HIPAA Gap Analysis, a HIPAA Risk Assessment, and a Security Framework Assessment all can have a place in meeting HIPAA compliance. But it is important to know the differences to select the correct option for your company's situation.

Lumen21 is a company that specializes in the area of IT Security and Compliance. Lumen21 has a series of solutions and services for used by Healthcare organizations in order to leverage newer technology while meeting its regulatory and security responsibilities. Lumen21's Compliant Cloud Computing Solution is truly HIPAA compliant and also maps to NIST SP-800-144, NIST SP 500-299 standards as well as it complies with or exceeds the Cloud Security Alliance Framework (CSA). Lumen21 enables the process of compliance and allows a healthcare company the ability to measure, monitor, report and improve that process. Lumen21 offers its O365+ Compliance Service leveraging Microsoft products such as O365 Enterprise, Enterprise Mobility, Device management and Azure Storage, implementing the necessary controls that are configured and monitored to meet regulatory standards. That is why at Lumen21 we believe HIPAA compliance is not a statement, it's a continuous process that is vetted and certified. You can learn more about our solutions that can help you meet regulatory compliance in your It operations as well as enhance your security by reaching out to us at sales@lumen21.com or visit us at www.lumen21.com HIPAA compliance is not a statement, it's a continuous process that is vetted and certified. You can learn more about our solution by reaching out to us at sales@lumen21.com or visit us at www.lumen21.com