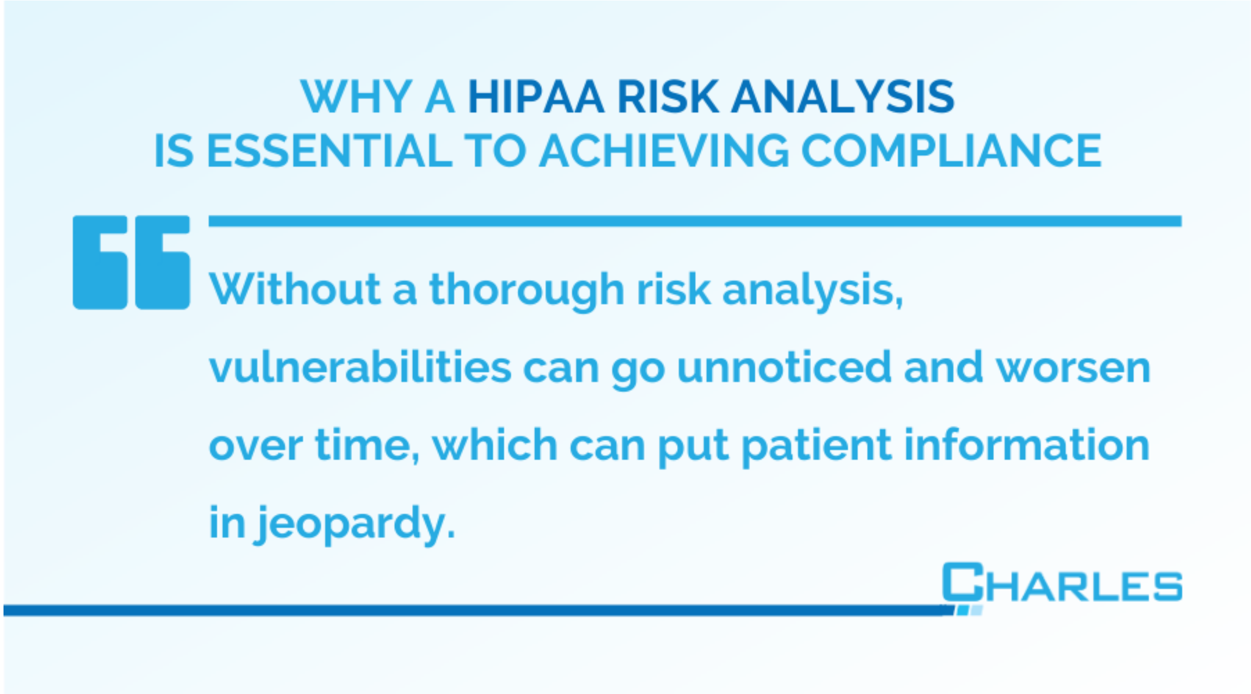
Why a HIPAA Risk Analysis is Essential to Achieving Compliance

Meta description: Learn the importance of a HIPAA risk analysis and steps on how to do it to achieve compliance.
Meta tags: HIPAA, compliance, cybersecurity, healthcare, phi, risk analysis



WHY A HIPAA RISK ANALYSIS IS ESSENTIAL TO ACHIEVING COMPLIANCE

Without a thorough risk analysis, vulnerabilities can go unnoticed and worsen over time, which can put patient information in jeopardy.

CHARLES

Cyberattacks on healthcare organizations are nothing new. In fact, there has been a 45% increase in the number of cyberattacks on healthcare companies since November 2020. Since then, the weekly attacks rose from 430 in October to 626 per organization in November. This is why the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires all entities handling protected health information (PHI), including HIPAA hosting providers, to perform a risk analysis as a first step in achieving HIPAA compliance.

What Is a HIPAA Risk Analysis?

A HIPAA risk analysis provides healthcare providers and their business associates with a clear road map on how to achieve compliance. It identifies vulnerabilities and potential risks to the integrity, confidentiality, and availability of PHI. A risk analysis also provides recommendations on how covered entities can strengthen their cybersecurity defenses to prevent cybercriminals from stealing patient information.

Without a thorough risk analysis, vulnerabilities can go unnoticed and worsen over time, which can put patient information in jeopardy. Also, organizations that have not performed a risk analysis can face serious financial penalties.

Who Needs a HIPAA Risk Analysis?

According to the HIPAA Security Rule, covered entities and their business associates are required to conduct a thorough risk analysis. Covered entities refer to healthcare providers, healthcare clearinghouses, and health plans, while business associates are individuals or organizations that use and disclose PHI on behalf of covered entities.

How to Conduct a HIPAA Risk Analysis

A risk analysis is only effective if it is done thoroughly and correctly. But because it evaluates every inch of a healthcare provider's infrastructure, the process can be challenging. This article provides guidelines on how to conduct a risk analysis the proper way.

1. Review HIPAA's updated regulations

HIPAA regulations went through some major changes in 2020, mostly due to the effects of the pandemic. These include changes to the HIPAA Privacy Rule, updated penalties for noncompliance, modifications to HIPAA enforcement, and the Notice of Enforcement Discretion, to name a few. Reviewing these updated regulations will ensure you understand the requirements your organization needs to meet before conducting a risk analysis.

2. Choose a HIPAA risk analysis tool

The Office of Civil Rights (OCR) recommends two tools that can assist you in conducting a risk analysis. They are:

- **Security Risk Assessment Tool (SRA)**
  Created by the Office of the National Coordinator for Healthcare Information Technology (ONC), the SRA features 156 questions that will lead you through each HIPAA requirement. It will then provide you with corrective actions you need to take based on your answers. The SRA also comes with resources to help you understand the context of the questions and the potential risks if HIPAA requirements are not met.

- **Risk assessment toolkit**
  This toolkit was developed by members of the Health Information Management Systems Society (HIMSS). It comes with Excel workbooks that contain National Institute of Standards and Technology (NIST) risk analysis references, HIPAA Security Rule standards, hardware and application inventory workbooks, implementation specifications, and a PDF user guide. This toolkit was designed to help a risk assessor perform a standards-based security risk analysis.

3. Determine the frequency of the risk analysis

The HIPAA Security Rule stipulates that risk analysis should be an ongoing process of documenting and updating your organization's cybersecurity measures as needed. However, the Security Rule does not specify how often a risk analysis should be performed. Some healthcare providers conduct a risk analysis as necessary depending on their current circumstances (e.g. every three years or bi-annually), while others do it annually.

4. Conduct the risk analysis

HIPAA does not specifically state who should conduct the risk analysis. Some healthcare providers outsource the task to third-party providers, others do it internally, and some do both. For instance, a covered entity may hire an external assessor to perform the risk analysis every other year, and perform an internal analysis during the off year. However, to ensure an impartial analysis, it's better to have a third-party assessor perform the risk analysis. The risk analysis should identify:

- Systems that store and access PHI
- Personal devices with access to PHI
- How PHI is stored, used, and transmitted
- Who has access to PHI
- When is PHI accessed
- Internal and external threats
- Current cybersecurity measures in place

5. Document your risk analysis

Documentation will prove that your organization has performed a complete risk analysis. This document must include a list of potential threats and vulnerabilities detected, a risk management plan, and your progress in addressing the issues identified during the analysis.

Conducting a risk analysis can be overwhelming, which is why you should partner with a managed IT services provider familiar with HIPAA regulations like Charles IT. We'll assess and evaluate your current cybersecurity policies and infrastructure to identify any vulnerabilities that can put patient data at risk. Call us today to learn more.