HIPAA Risk Assessment

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Know Your Risks

Cybersecurity threats are on the rise like never before, and healthcare organizations are more vulnerable than ever. There are news stories every day on latest breaches – but how do you keep your organization out of the headlines? The first step is finding out where your risk truly lies in accordance with HIPAA guidance. With a HIPAA Risk Assessment, you'll get a full view of your organization's risks as well as a recommended action plan on the best way to remediate each risk or vulnerability.

Not Just Identification

During a HIPAA Risk Assessment, our experts will identify the threats to your assets as well as the impact and probability of those threats occurring within your IT environment. We evaluate not only the existence of controls, but also the effectiveness of the controls used to mitigate threats to your IT security program. We will also identify any residual risk that may still be there after you implement the proper controls to combat threats to your organization. After your engagement, you will have access to our Risk Management platform to streamline your remediation process.

Next Steps

Risk never completely goes away, so it's important to perform regular risk assessments, especially when you have any significant changes to your IT environment. The fact of the matter is that risk is constantly growing, which means your cybersecurity program needs to grow too. Once completing a risk assessment, you'll have a cybersecurity roadmap to help you through your security journey.

A Risk Assessment is a great way to understand what areas of your IT environment need your attention. Once completing a Risk Assessment, you'll understand what controls and patches you need to implement and learn about your other IT areas that may need additional testing. Don't waste time and resources on solutions you don't truly need – use the results from your Risk Assessment to truly know what areas need your attention so you can make the most of your budget.

After a HIPAA Risk Assessment You Will:

- **Understand your security posture and risk level present**
- **Have a recommended action plan for remediation**
- **Have a starting place for your cybersecurity roadmap**

Frequently Asked Questions

What is the difference between a risk assessment and an IT audit?
A Risk Assessment reports the resulting residual risk after evaluation of threats to your assets and current mitigating controls, whereas an Audit proves/tests that you have implemented the prescribed and asserted controls.

Will this make me HIPAA compliant?
Risk Assessments are an essential part of your information security program and are required by HIPAA. However, a HIPAA Risk Assessment is not designed to report compliance. Compliance can be verified by an independent audit or HIPAA compliance gap analysis.

What is included in "IT security?"
Information technology is one element of your information systems, but there are usually physical, procedural, technical, and personnel-related elements too. Combined, these encompass your Information Security program, which includes IT Security.

I have a vendor who manages my IT, and they assure me that they are HIPAA compliant. Do I still need a Risk Assessment?
An organization can outsource services, including management of information systems, but you cannot outsource the "responsibility" for protection of your data. Organizations must have a means to verify the vendor or service providers compliance with prescribed security controls. This is typically achieved through independent audits, monitoring, and periodic vendor/provider reviews.

Will this Risk Assessment look at both ePHI and PHI?
This Risk Assessment will look at information protection in both physical and electronic form.

Will this Risk Assessment cover personal employee devices brought to work?
This depends on if these devices are used to access business information and systems.

How much disruption will this cause in my day-to-day operations?
Aside from interviews with key stakeholders, this service causes little to no disruptions in normal business activities.

What kind of physical access do you need?
No type of physical access is necessary. We can perform Risk Assessments remotely or onsite depending on your preference.

How many times should I get a Risk Assessment and how often?
Risk Assessments should be done upon major changes to the processes or information systems, or at least once per year.

Who do you need to talk to in my organization?
Any stakeholder with knowledge of the technical, procedural and physical controls employed by the organization to protect information.

Are you going to look at my policies?
A policy document may be reviewed at your request in order to gain insight into any particular policy, process, or control.