HIPAA RISK ADVISOR

SAMPLE REPORT

FOCAL POINT
DATA RISK

HIPAA Security Analysis Report

The most tangible part of any annual security risk assessment is the final report of findings and recommendations. It's important to have an accurate risk analysis along with pragmatic and reliable recommendations so that organizations reduce real world risk while simultaneously demonstrating their due diligence to an auditor.

Our HIPAA Security Analysis Report achieves this goal. Based on industry-accepted standards as the basis for control assessment criteria and recommendations, our methodology provides a more defined baseline than alternatives that rely on a "check-box" approach and result in a false sense of security.

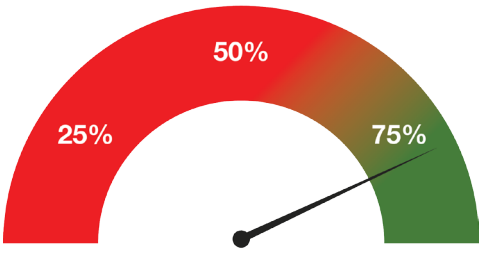
> The HIPAA Security Analysis Report exceeded my expectations. Even with all of the deficiencies that were discovered, I didn't feel overwhelmed because the recommendations are so straightforward.
>
> - Office Manager, dentist office

Dynamic Risk Score

Your level of risk is constantly changing, based on factors that are both within your control, and outside of it. With HIPAA Risk Advisor, we'll identify all of the possible sources for risk to your ePHI, assess the effectiveness of the controls you have in place to mitigate that risk, and make pragmatic recommendations on how to meet HIPAA Security Rule requirements as well as reduce overall risk.

Based on an analysis of the online Security Risk Assessment and through our consultative reviews, the Dynamic Risk Score reflects your current risk, and can be used to demonstrate your compliance with each specific HIPAA Security Rule requirement. Over the course of your HIPAA Risk Advisor subscription, your Dynamic Risk Score will continue to increase as you navigate through the Security Risk Assessment process, and implement our recommendations.

Dynamic Risk Score

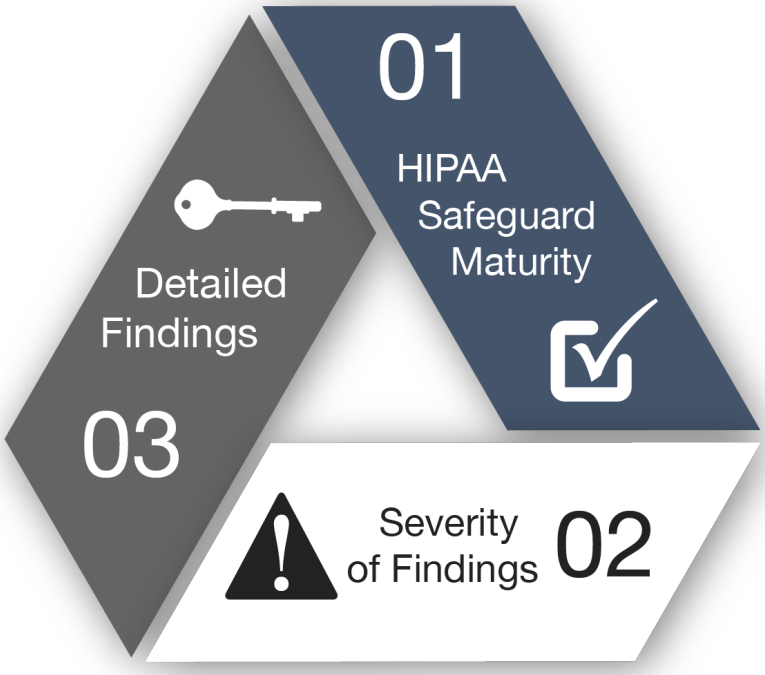


The HIPAA Risk Advisor Dynamic Risk Score is very similar to the grade system you may have had in high school or college. The range goes from 0-100% for each of the HIPAA Security Rule Safeguards; Administrative, Physical, and Technical. Each of the 48 Safeguards' controls/ questions are weighted based on their criticality in reducing risk. Responses are averaged across the entirety of the assessment for a total overall Dynamic Risk Score. We recommend that your practice strive to maintain at least a score of 75%, and we'll help you get there.

> "The HIPAA Security Analysis Report gives us the best of both worlds. It provides a prioritized to-do list for our staff and IT provider, and helps us satisfy the HIPAA Security Rule requirement for a security risk analysis."
>
> - Practice Administrator, small family practice

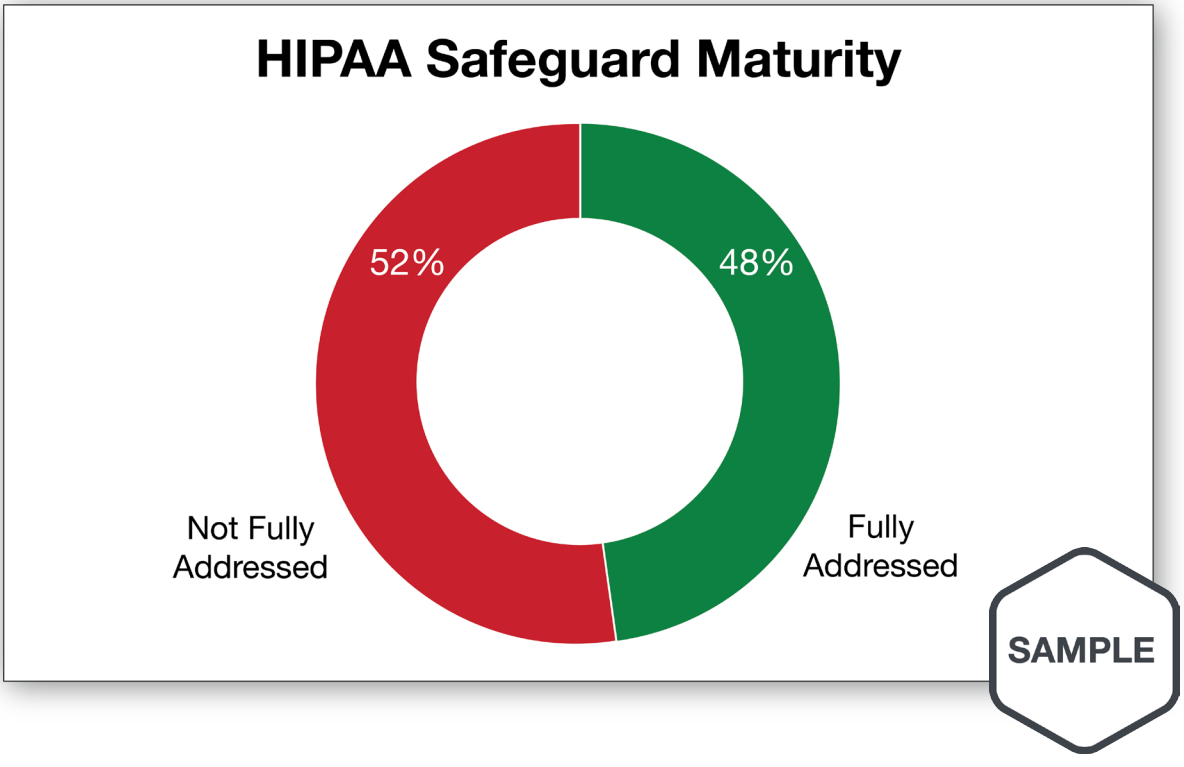
Common Sense, Pragmatic Risk Analysis

Our Security Analysis Report is divided into three major analytical sections:



01 HIPAA Safeguard Maturity

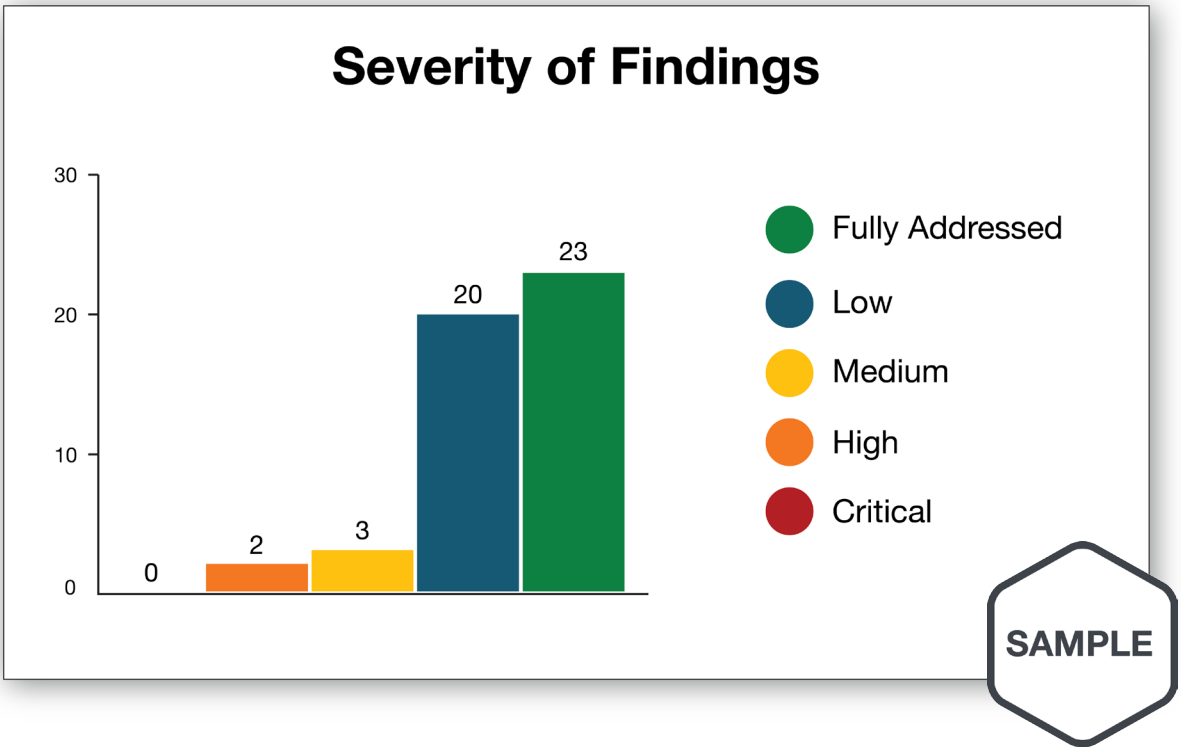
We evaluate how each of the HIPAA Administrative, Physical, and Technical Safeguards have been implemented. Each of the 48 controls associated with the Safeguards are either Fully Addressed or Not Fully Addressed.



02 Severity of Findings

We define “Severity” as an estimation of the negative consequences to the organization. The Severity ranking of a control is determined by analyzing a combination of the following variables:

- The impact and likelihood of a vulnerability being exploited
- Whether the control item is considered a primary Administrative, Physical, or Technical Safeguard control
- How existing processes align with industry accepted standards.



Possible severity rankings are:

Critical	Applies to primary control deficiencies that result in an extremely high likelihood of compromise and result in a negative impact to the underlying target environment.
High	Applies to primary control deficiencies that result in a high likelihood of compromise and / or have a significant negative impact the underlying target environment.
Medium	Applies to secondary control deficiencies that result in a potential to compromise and / or have a negative impact on the underlying target environment.
Low	Control is unlikely to or does not compromise and / or have a negative impact on the underlying target environment.

03 Detailed Findings and Recommendations

Our HIPAA Security Analysis Report includes a comprehensive and detailed list of findings regarding the implementation of Administrative, Physical, and Technical Safeguards. Here are just a few examples of the 48 specific HIPAA controls we'll examine and include in our report.

164.308 - Administrative Safeguards

Administrative Safeguards are administrative actions, policies, and procedures to manage the security measures put in place to protect electronic protected health information (ePHI). These Safeguards also help manage the conduct of the covered entity's or business associate's workforce as it relates to the protection of ePHI.

Information System Activity Review	Severity
	Medium
HIPAA Reference	164.308(a)(1)(ii)(D) – Required
Requirement	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Findings	The HIPAA Information System Activity Review Policy does not provide sufficient detail for administrators to adequately log activities to recreate events in the event of an incident. Nor does the policy provide specific guidance on how often and which mechanisms are used for the review of logs. Although a syslog server is used to consolidate some system logs it is not used as an aggregate of all logs (server, application, database, and network devices). Reviews of the various logs are performed manually by different teams and in inconsistent intervals, which could result in an inadvertent incomplete review.
Controls in Place	A high-level documented HIPAA Information System Activity Review Policy Manual reviews of the application, system and database logs.
Recommendations	Ensure all HIPAA system component logs are centralized to allow for the long term storage of security logs in a single location and the production of aggregated security reports. Develop a security reporting process to generate a full portfolio of high-value security reports and alerts for critical system components through the use of automated tools. Establish a consistent security report review interval and more thoroughly define review timelines based upon specific report types. Common intervals are daily or weekly for security reports and more frequently for security alerts.

164.310 - Physical Safeguards

Physical Safeguards are physical measures, policies, and procedures that help protect the covered entity's or business associate's information systems. These controls also help protect the assets, both facilities and equipment, from both natural and manmade threats.

Contingency Operations	Severity
	Low
HIPAA Reference	164.310(a)(2)(i) – Addressable
Requirement	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
Findings	We reviewed the essential components needed for a contingency operational plan. While a few checklist drafts exist, the practice needs to formally establish and implement physical security controls for contingency planning purposes.
Controls in Place	A high-level HIPAA Application and Data Criticality Analysis Policy A comprehensive Business Continuity Plan
Recommendations	Develop, document, and implement an emergency physical access process. The process should define the emergency locations, how physical security is to be implemented at all backup locations, personnel with access, and all personnel roles / responsibilities.

164.312 - Technical Safeguards

Technical Safeguards consist of the technology, policies, and procedures used to protect and control electronic access to the covered entity's or business associate's ePHI and affiliated systems.

Automatic Logoff	Severity
	Low
HIPAA Reference	164.312(a)(2)(iii) – Addressable
Requirement	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
Findings	The policies have the duration for inactivity inconsistently documented.
Controls in Place	See 3.1.5.5 (Password Management)
Recommendations	Define and document the approved screensaver and automatic logoff requirements for each type of system component. Implement a session timeout or screensaver requirement for all system components.

SAMPLE

Summary

A HIPAA Risk Advisor subscription provides more than just a detailed risk analysis report. We offer subscribers access to an online portal with sample security policies, FAQs, HIPAA security employee training materials, and more. Additionally, each subscriber is assigned a dedicated HIPAA Security Consultant for consultative reviews and interviews before publishing the final HIPAA Security Analysis Report.

To find out more, visit www.hipaariskadvisor.com and get started today.