



# HIPAA



## HIPAA Risk Assessments A CTI Security Advisory Service

Compliance can be complicated. At CTI, our compliance team consists of multiple veteran Certified HIPAA Privacy Security Experts with years of experience. We have the knowledge to guide you through annual HIPAA risk assessments and ensure your continued compliance to these HHS standards — before you face heavy fines or losses.

Our privacy and security experts aren't simply compliance box checkers. They bring years of IT experience to every engagement with the goal of ensuring your compliance through reasonable, achievable controls. We'll offer our findings and recommendations to help you prioritize any remediation -- and we'll assist with remediation if needed.

### Why do you need a HIPAA Risk Assessment?

Since the HIPAA Privacy Rule was established in 2003, all healthcare organizations that handle protected health information (PHI) are required by law to complete a HIPAA Risk Assessment. Relatively few healthcare organizations, however, successfully complete this mandatory annual assessment. The Office of Civil Rights (OCR) is no longer taking its time to enforce these regulations and is actively pursuing organizations in violation of HIPAA regulations, charging them with severe penalties and fines.

### SERVICE OVERVIEW

A risk assessment allows organizations to identify and evaluate network environments, address gaps in security and protection, and raise any red flags where security and noncompliance might be an issue.

The HHS Security Standards Guide defines nine components of a risk analysis that healthcare-related organizations use that electronic protected health information (ePHI) must include in their documentation:

**Scope of the Analysis.** Identify any potential vulnerabilities to the availability, privacy, and integrity of your ePHI data. This means all electronic software, hardware, and media your organization uses to create, transmit, receive, or store ePHI.

**Data Collection.** Locate where data is being stored, received, transmitted, and maintained.

**Identify and Document Potential Threats and Vulnerabilities.** Document any perceived threats to sensitive data, and any vulnerabilities that may lead to compromised ePHI.

**Assess Current Security Measures.** Identify ways your organization protects sensitive data.

**Determine the Potential Impact of Threat Occurrence.** Evaluate the maximum damage of each potential threat.

**Determine the Level of Risk.** HHS suggests taking an average of the likelihood of threat occurrence and the potential impact of threat occurrence.

**Finalize Documentation.** Basically, put your analysis into words. HHS does not specify a particular format.

**Periodic Review and Updates to the Risk Assessment.** Perform another risk analysis any time your organization implements new technology or operation standards.

**Determine the Likelihood of Threat Occurrence.** Assess the likelihood of ePHI breaches and threat occurrence.

## HOW CAN CTI HELP?

CTI can provide your organization with comprehensive evaluations of your current environment and recommend a remediation strategy based on our observations. In short, we can help fix issues that would otherwise make your organization noncompliant. CTI's Advisory Services include building policy, process, procedures, testing guidelines, and incident response, all around protection of your critical healthcare data.

CTI can also perform all security testing, vulnerability and penetration testing, social engineering, application testing, security configurations reviews, and any other forms of testing pertinent to healthcare services.

- To ensure that technical controls mandated by procedures and policies are implemented properly, an organization must undergo a technical evaluation that includes vulnerability and penetration testing. A vulnerability test evaluates weaknesses or "openings" in an organization's security systems. A penetration test simulates an actual attack on an organization's network.
- Application testing is very similar to both of these processes, with the operative difference being that your web-based applications are tested for weaknesses and response measures.
- Social engineering fraud is a process by which individuals are manipulated into divulging protected information or granting access to protected information. Social engineering measures often include coercion, deception, or trespassing into off-limits areas. CTI can ensure that your physical security teams and policies are in place to defend against theft.

These tests must be performed by a certified, independent expert, such as CTI. Most security experts recommend quarterly vulnerability tests and annual penetration tests. CTI can use vulnerability and penetration testing to show just how susceptible your organization is to an attack, and also provide remediation strategies to prevent attacks in the future.

CTI is authorized to issue an Attestation of Completion, certifying that your organization has thoroughly and successfully completed your testing processes.

## PROVISION LOG MONITORING, ANALYSIS & ALERT MANAGEMENT

Enterprises can generate millions of log alerts every day, making the recognition and analysis of meaningful alerts in real-time a complicated, resource-consuming challenge.

Today, security teams are already struggling to stay focused simply on managing resource bandwidth. Our ProVizion management platform can put you in control.

### ProVizion Features

- 24/7 real-time monitoring, alerting, and analysis by certified security analysts
- Asset classification and reporting
- Flexible and customizable reporting
- Pre-built security and compliance reports

## ABOUT CTI

CTI solves business problems by providing services spanning business advisory, technology, and advanced analytics. We help companies envision, design, implement and manage complex data-centric business solutions. Our approach is to understand your business strategy before evaluating how data can strengthen your goals. We focus on producing meaningful insights from your data asset. We expose those insights, embedding them into your business processes while guiding user adoption for a more data-driven culture.

## CONTACT US

CTI is located in Burlington, Mass., serving customers in New England, Metro New York, Metro Atlanta, and beyond.

Corporate Office:

78 Blanchard Road  
Suite 304  
Burlington, MA 01803  
Tel: 781-273-4100  
800-932-4249  
Fax: 781-273-7351