Introduction to HIPAA Compliance for Small Businesses

Never have a false sense of security.™
Streamline Your HIPAA Compliance

SecurityMetrics Guided
HIPAA Overview

HIPAA compliance is often a difficult and time-consuming task for office managers and practitioners. SecurityMetrics has simplified your responsibilities with the HIPAA dashboard, letting you track your risk analysis, risk management plan, staff training, and policies/procedures, all in one portal.

Guided HIPAA Compliance is broken down into three steps:

1. **Breach Protection Consulting.** This step serves to increase your overall data security posture, throughout your organization so you can prevent a potential breach.

2. **Guided Risk Analysis.** Get a deeper understanding of your organization’s vulnerabilities and how to solve them.

3. **Prioritized Risk Management Plan.** Implement a seamless, prioritized plan, so every member of your staff can be aware of their specific responsibilities.

A SecurityMetrics HIPAA Support Advisor analyzes the top risks to your organization’s data, which include:

- Password management
- Firewalls
- Malware
- Remote access
- Wireless security
- Web browsing
- Email
- Theft
- Social engineering

Addressing vulnerabilities found during the top risks review can significantly increase your organization’s data security.

Monthly Resources

SecurityMetrics provides a monthly newsletter, podcast, and blog that covers HIPAA compliance and management tips, educational materials, and recent healthcare news. These resources help you stay updated to avoid pitfalls that lead to a compromise.

HIPAA Compliance Risk Analysis

Health and Human Services (HHS) has levied fines for the lack of a formal and thorough risk analysis. SecurityMetrics provides an analysis of your current compliance level, a map of all systems that interact with PHI, and vulnerability and risk identification. SecurityMetrics Guided Risk Analysis includes our award-winning support to ensure your risk analysis is accurate and complete.

System Vulnerability Identification

All systems used to create, receive, maintain, and transmit PHI have inherent risks. As data security experts, SecurityMetrics identifies risks and vulnerabilities based on your systems in use. After creating a PHI map of your systems that interact with PHI, we produce a list of associated risks, threats, and vulnerabilities.

External Network Vulnerability Scans

Data thieves access protected health information (PHI) through unprotected networks. Our vulnerability scans help you achieve external network security by searching for even the most recent vulnerabilities. Our finely tuned scan engines expose weaknesses in your network. Our support team helps you remediate discovered vulnerabilities to protect your patient data.
Prioritized Risk Management

After performing the risk analysis, SecurityMetrics provides a prioritized risk management plan. This plan is based on the results of your organization's systems, controls, risks, and vulnerabilities. The risk management plan is prioritized from high to low risk to address the most threatening risks first.

"I appreciated the expert help from SecurityMetrics as our office worked through understanding HIPAA regulations. The staff was knowledgeable and very helpful. The validation process went off without a hitch!"

– Kathy Marks, Office of Dr. Mike Bloom

Guided Risk Management Plan Implementation

Understanding the technical action items in the risk management plan can be difficult. SecurityMetrics HIPAA experts guide you and your IT resources through implementation to check that your organization is secure and on the journey to compliance.

Policies and Procedures

HIPAA policies and procedures aren’t just paperwork—they are the blueprint for your organization’s daily compliance efforts. SecurityMetrics provides customizable Privacy Rule (28), Security Rule (20), and Breach Notification policies and related procedures.

SecurityMetrics’ policies and procedures templates save you time, energy, and money so you can focus on managing your organization. An assigned support specialist assists you in tailoring policies and procedures so they accurately reflect the uniqueness of your organization.

Additional Security and Compliance Tools

SecurityMetrics has additional tools to help you secure PHI and help you on your journey to HIPAA compliance. We offer data security and HIPAA training, penetration testing, onsite compliance assessments, and HIPAA consulting to meet your organization’s unique needs.
Guided HIPAA Compliance Packages

**Pro**
$4,999 USD/year

- **Compliance Management**
  - Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training)

- **Services**
  - Breach Protection Checklist
  - $100,000 service warranty (after attesting to Breach Protection Checklist)
  - Risk Analysis
  - Risk Management Plan

- **Policies and Training**
  - HIPAA Policies & Procedures (including Breach Notification Policy & Business Associate Agreement Template)
  - Dedicated HIPAA Coach to guide you through Risk Analysis & Risk Management Plan
  - Monthly Vulnerability Scans (5 IP addresses)
  - HIPAA Training (25 Seats)
  - Up to 4 hours with a HIPAA Specialist for deeper discovery and a start to remediation of high risk areas

**Plus**
$2,499 USD/year

- **Compliance Management**
  - Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training)

- **Services**
  - Breach Protection Checklist
  - $100,000 service warranty (after attesting to Breach Protection Checklist)
  - Risk Analysis
  - Risk Management Plan

- **Policies and Training**
  - HIPAA Policies & Procedures (including Breach Notification Policy & Business Associate Agreement Template)
  - Dedicated HIPAA Coach to guide you through Risk Analysis & Risk Management Plan
  - Monthly Vulnerability Scans (3 IP addresses)
  - HIPAA Training (6 Seats)

**Basic**
$999 USD/year

- **Compliance Management**
  - Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training)

- **Services**
  - Breach Protection Checklist
  - $100,000 service warranty (after attesting to Breach Protection Checklist)
  - Risk Analysis
  - Risk Management Plan

- **Policies and Training**
  - HIPAA Policies & Procedures (including Breach Notification Policy & Business Associate Agreement Template)
  - Monthly Vulnerability Scans (1 IP address)
HIPAA Compliance FAQs

What is the purpose of HIPAA?
The use of electronic health records has the potential to reduce costs and improve care, but has caused an increased focus on data security and introduced new vulnerabilities to healthcare organizations. The Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect patient information. HIPAA includes rules on privacy, security, and breach notification with regard to protecting consumer healthcare information.

Who enforces HIPAA?
HIPAA is regulated and enforced by the Health and Human Services (HHS) Office for Civil Rights (OCR). Recent changes to HIPAA legislation have provided additional guidance and authority for the OCR to enforce HIPAA compliance through audits and financial penalties. The State Attorney General has been given authority to also levy fines related to HIPAA violations and compromises.

How much can I be fined?
The penalties outlined below are assessed per day and per violation. After a breach, the HHS is not the only one with authority to mandate fines. We are also seeing class action lawsuits, State Attorney Generals, and the FTC collecting money based on HIPAA violations.

For example, you may be liable for several of the following fines, losses, and costs:

- HHS settlements: Up to $1.5 million/violation/year
- State attorney generals: $150,000 – $7 million
- Business associate changes: $5,000+
- Lawyer fees: $5,000+
- Technology repairs: $2,000+
- Class action lawsuits: $1,000/record
- Breach notification costs: $1,000+
- Ongoing credit monitoring for affected patients: $10-$30/record
- ID theft monitoring: $10-$30/record

Total Possible Cost $180,000-$8.3 Million+
Why is there increased enforcement?
Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more records have been reported to the HHS. These breached records have negatively impacted covered entities and business associates, resulting in over $41 million in resolution agreements and fines.

Which trainings am I required to do?
HIPAA requires regular employee training on both the Privacy, Security, and Breach Notification Rules. Other trainings you may consider include data security, responsible use of social media, and Payment Card Industry Data Security Standard (PCI DSS).

To find out more recommended training options, visit https://www.securitymetrics.com/workforce-training.

Am I required to have an onsite assessment?
Onsite assessments conducted by a third party are not required to achieve HIPAA compliance, but in many cases, they are recommended.

Depending on the complexity of your IT infrastructure, the number of locations you have, and the way you work with PHI, you may want to consider an onsite assessment. For the majority of small covered entities, an offsite HIPAA compliance assessment is sufficient to demonstrate compliance with the law.

How do I become HIPAA compliant?
Most offices have made some progress towards HIPAA compliance. However, with recent changes and an increased focus on technical security, many offices are falling short. Both Privacy and Security Rules require covered entities and business associates to:

- Conduct an acceptable risk analysis
- Prepare an actionable risk management plan
- Make regular and demonstrable progress on the plan

To find out more of what’s required for PCI compliance, visit https://www.securitymetrics.com/lp/hipaa/hipaa-guide.

How do I calculate my organization’s risk of a breach?
Penetration testing, or ethical hacking, is the most accurate way to know your data is safe. A penetration test analyst examines your business environment and manually checks your network to find weaknesses the way a hacker would, through live testing. SecurityMetrics Penetration Test Analysts are experts at helping protect sensitive data.
About Us

We secure peace of mind for organizations that handle sensitive data. We hold our tools, training, and support to a higher, more thorough standard of performance and service. Never have a false sense of security.™

We are a PCI certified Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Certified Forensic Investigator (PFI), and Managed Security provider with over 20 years of data security experience. From local shops to some of the world’s largest brands, we help all businesses achieve data security through managed services and compliance mandates (PCI, HIPAA, HITRUST, GDPR). We have tested over 1 million systems for data security and compliance.