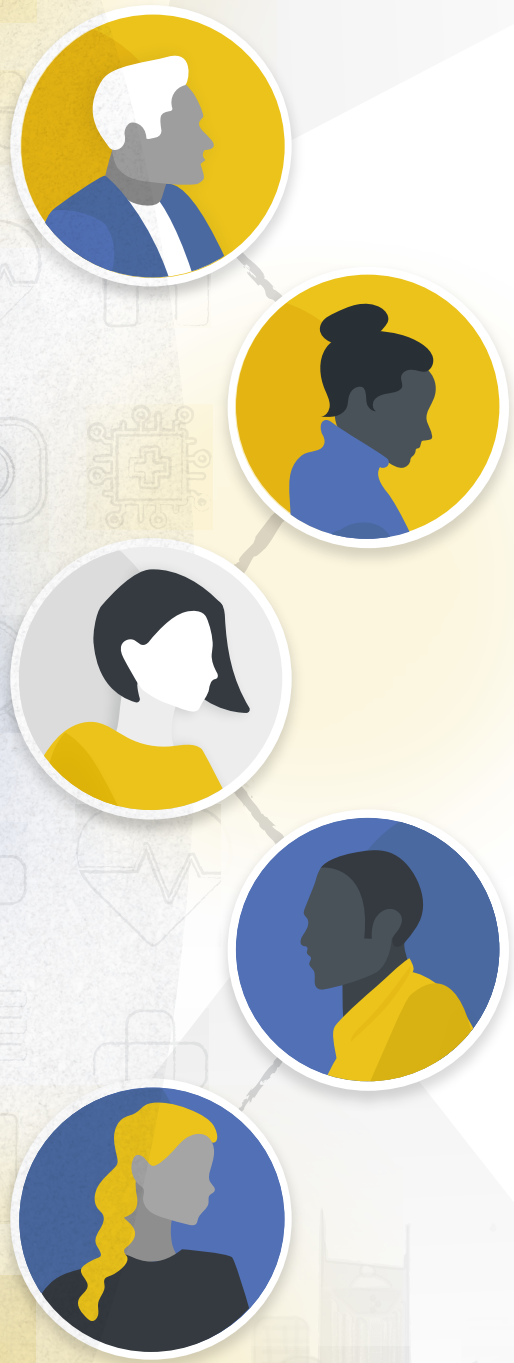
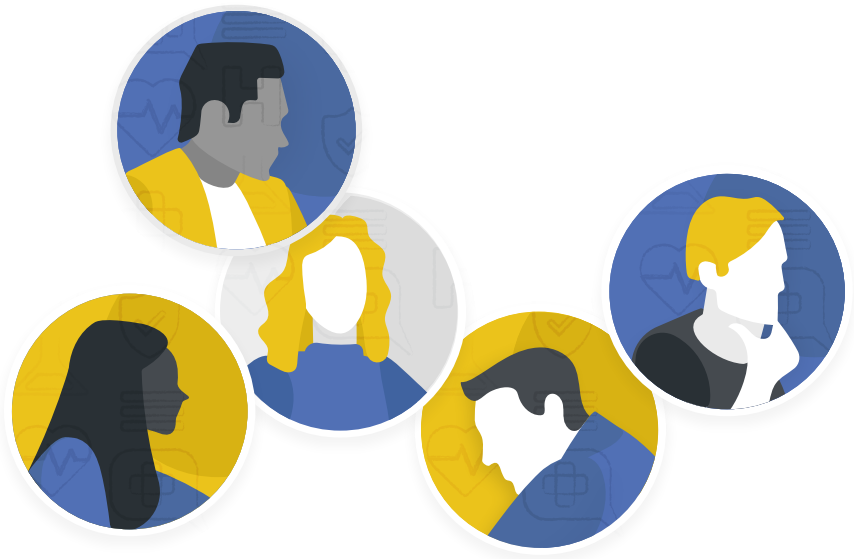


The IT Leader's Essential Guide to *HIPAA Compliance*

The 14 Key Questions You Need to Answer to Ensure Compliance

PROVISIONS GROUP



Understanding HIPAA

Understanding your HIPAA compliance obligations, as well as any vendors you're partnered with can be extremely confusing and overwhelming. Often, organizations or teams don't know where to start looking to fix gaps that are leaving data vulnerable and your organization to be out of HIPAA compliance.

In cases of a HIPAA violation, it's crucial to note that lack of awareness about HIPAA requirements cannot serve as a valid defense against government action and/or paying for fines and penalties.

Criminal HIPAA violations can result in fines of up to $1.5 million for organizations, as well as possible penalties such as jail time. Civil penalties can range from $100 to $50,000 per violation. This can lead to some serious damage to your finances as an organization.

In addition to the financial penalties, businesses may also face reputation damage and loss of trust from patients and employees, which can have lasting effects on the success and sustainability of the organization.

Directions

The purpose of this checklist is to help identify areas that need to be investigated and resolved **immediately** to be HIPAA compliant. After you download and/or print this list, read each question carefully and answer with the color-coded scores. The results of this checklist will fall into three categories:

Red Score "Not in Compliance"

If one or more of the questions has been answered in **red or "not in compliance"** then you are not in compliance. Unfortunately, it is an all or nothing when it comes to HIPAA, this means your organization is at risk for security breaches and/or getting penalized for not complying with HIPAA laws. We recommend making it a priority to resolve these issues to avoid threats and potential penalties.

Orange Score "Not sure/Need to check"

If one or more of the questions has been answered in **orange or "not sure/need to check"** then you may not be in compliance and need to make it a priority to determine if you are compliant. If you find that you are not, you need to make it a priority to resolve quickly.

Green Score "We are fully compliant"

If all the questions have been answered in **green or "fully compliant"** then you're set! Please continue to audit and monitor your organization with this checklist to stay compliant.

IT'S IMPORTANT TO NOTE THAT ANY ANSWER THAT IS NOT "FULLY IN COMPLIANCE", INCLUDING "NEED TO CHECK" IS CONSIDERED NOT COMPLIANT AND IS DEEMED TO BE AT RISK!

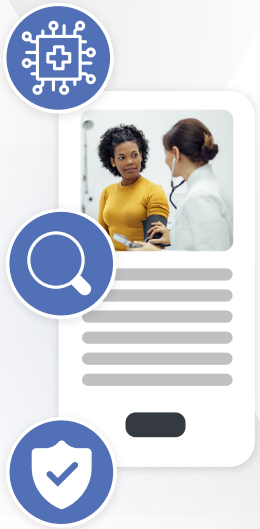
Question	Areas to Consider	Score
Do you have an IT compliance or risk strategy that accounts for both HIPAA related controls and any other international, federal, and state laws with which organizations must comply?	• Risk Management Plan • IT Security Management Plan • HIPAA Roadmap • HIPAA Aligned Compliance Tool (e.g., Drata, Vanta, Hyperforce)	
Do you have a data privacy and information security policy and program and does that program include a HIPAA aligned strategy for goals, milestones, roadmap, and capability maturity?	• IT Security Management Plan • IT Security Program Roadmap • IT Security Policy	
Do you have an information technology and technology service management policy and program and does that program include a HIPAA aligned strategy for goals, milestones, roadmap, and capability maturity?	• IT Service Management / Help Desk Tool (e.g., Freshservice, Zendesk) • Information Technology Management Plan • IT Program Roadmap	
Do you have a technology acceptable use and password policy that expresses the expectations and requirements of your users regarding their use of technology and authentication?	• Acceptable Use Policy • Password Policy that includes complexity, change, and MFA (multi-factor authorization) requirements	
Does your password policy and implemented controls make use of MFA and SSO whenever possible to ensure that users, apps, and data are securely accessed?	• Password Policy with MFA (multi-factor authorization) • Password Policy with SSO • Single Sign On system that supports MFA	
Do you have a monitoring, event, and incident management policy and plan with necessary technical controls so that you can detect and respond to issues with computers and technology?	• Incident Management Policy or Process • Security Incident Management Policy or Process • Availability Management Policy or Process	
Do you have a vulnerability and security incident management policy and plan with necessary technical controls so that any security issues, gaps, or risks are known?	• Vulnerability Management Policy or Process • Security Incident Management Policy or Process • IT Security Program Roadmap	
Do you have a backup, recovery, resilience, and capacity plan that will allow your infrastructure to respond to unplanned and planned events that would impact service availability, responsiveness, or scale?	• Backup Policy or Process • Capacity Management Policy or Process • Availability Management Policy or Process	

Question	Areas to Consider	Score
Do you have formal business continuity and disaster recovery plans and are those plans tested annually to ensure they would respond appropriately during a disaster scenario?	• Business Continuity Policy and Plan • DR (Disaster Recovery) Policy and Plan • Business Continuity or DR Policy Testing Results	✗ ? ✓
Do you know the data sources, targets, uses, and flows into and out of your environment for all systems with PHI or other sensitive data?	• Data Flow Diagrams • IT Systems and Database Inventories • Data Classification Policy	✗ ? ✓
Do you have data protection, classification, and handling policies in place and are they managed within a plan that is adequately resourced and sustainable?	• Data Classification Policy • Data Protection Policy • Data Handling and Data Loss Prevention Policy	✗ ? ✓
Do you have an account management policy and process that accounts for the onboarding, offboarding, and role change activities along with a system that ensures these activities are as automated as possible?	• User or Account Management Policy and Process • Employee Onboarding and Offboarding Process • Identity and Access Management System with Automated Provisioning and Deprovisioning	✗ ? ✓
Do you have an engineering function and solutions architecture that follows security best practices and accounts for cloud, devops, data, and security?	• SDLC (Software Development Lifecycle) Policy and Process • DevOps Policy and Process • Change Management Policy and Process	✗ ? ✓

Do you need more help with compliance?

We have over 20 years of experience in ensuring healthcare organizations and their vendors are fully in compliance with HIPAA laws and regulations. Not being fully compliant can lead to security breaches, legal actions, and/or hundreds of thousands of dollars in fines. Our team is here to help!

If this checklist shows that your organization is not in compliance or that you are complying and need assistance in continued auditing, use the QR code or link to reach out to us today for a **free HIPAA assessment** or to get help with any of your technology needs.



Schedule

Visit us at
ProvisionsGroup.com

PROVISIONS GROUP