CompliancePoint®

HIPAA Readiness Checklist

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that resulted in the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. HIPAA standards are broken down into:

HIPAA Privacy Rule
Addresses the use and disclosure of all protected health information

HIPAA Security Rule
Protects all electronic protected health information (ePHI) – individually identifiable health information a Covered Entity creates, receives, maintains, or transmits in electronic form

HIPAA Breach Notification Rule
Requires Covered Entities and their Business Associates to provide notification following a breach of unsecured protected health information

HIPAA's goal is to provide health data integrity, confidentiality, and availability. The rules implementing the HIPAA regulations are developed and enforced by the US Department of Health and Human Services (HHS) and provide guidance on:

Use and disclosure

Access to PHI

Storage of PHI

Transmission of PHI

Breach Notification

HIPAA applies to both Covered Entities and Business Associates. Covered Entities are those organizations who are involved in the treatment and payment of healthcare services. Additionally, Covered Entities are also organizations involved in healthcare operations. Covered Entities include providers such as doctors and hospitals, health plans and health care clearinghouses. Business Associates are persons or entities that perform activities on behalf of a Covered Entity that involve the use or disclosure of protected health information.

Why is it Important?

HIPAA is important because it helps to enable trust between consumers and the providers involved in handling their health information. The consequences of a breach of this information can damage your brand and customer reputation, resulting in a material impact to your organization's sales and value. HIPAA compliance is a competitive differentiator because consumers are more likely to do business with a company that respects their privacy, and the business can avoid large fines and public scrutiny over data handling practices.

$100–$50k

fines per violation for non-compliance, with a potential of up to $1.5M

An enterprise-wide security risk assessment is required by the HIPAA Security Rule and failure to perform one was cited as a contributing factor in 19 enforcement actions in 2020 alone, amounting to over $13.5 Million in financial penalties*. Mitigating risk in HIPAA involves the organization understanding the regulations and ensuring it has implemented the appropriate manual and technical controls. By building and having processes around the requirements and a solid governance layer, an organization can reduce the likelihood of consumer complaints and the likelihood of a data breach, reducing the risk of HIPAA investigation or enforcement.

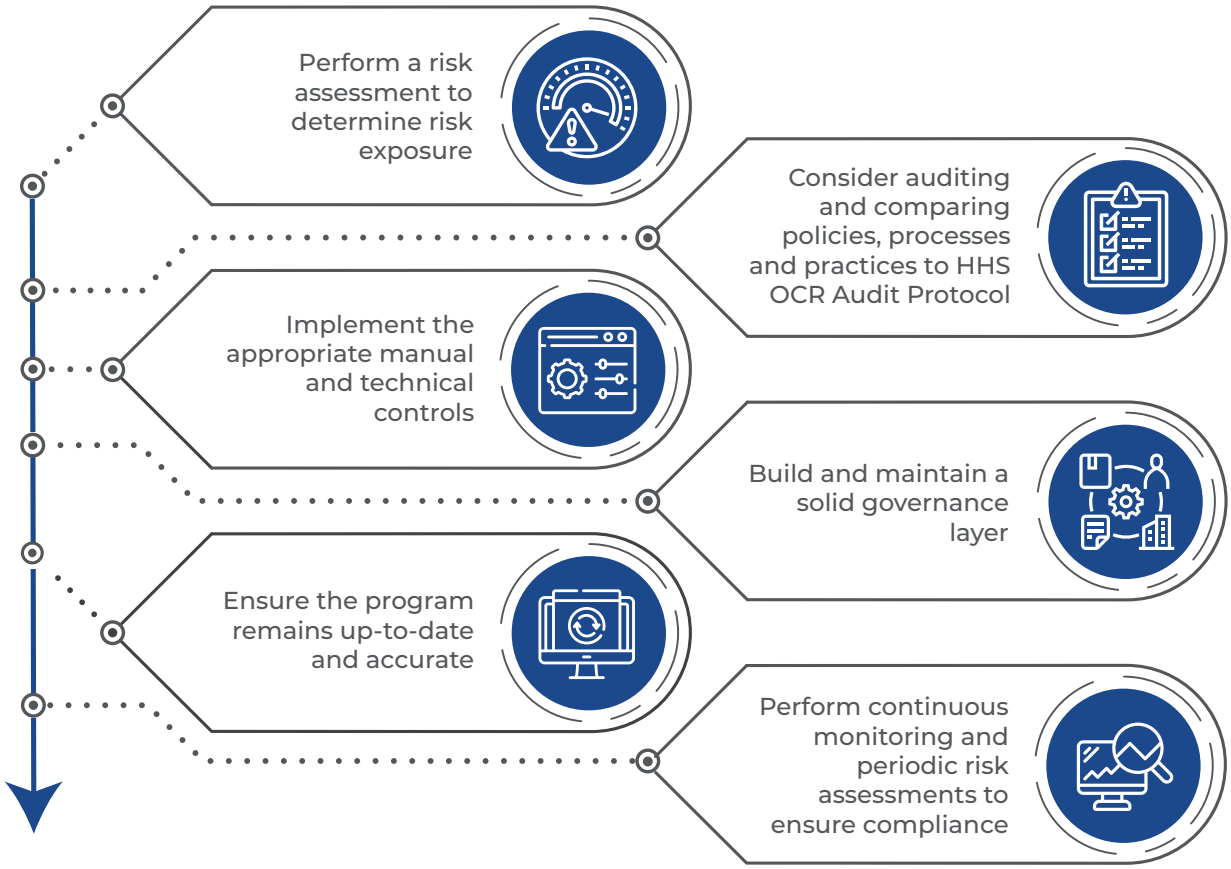
What Does it Mean to Be Compliant?

HIPAA requires Covered Entities and Business Associates to implement policies and procedures to meet the standards of the Privacy, Security, and Breach Notification Rules.

HIPAA Privacy Rule	
COVERED ENTITIES	• Provide accurate Notice of Privacy Practices outlining how you use PHI • Provide access to PHI by individuals • Allow for review and amendment of PHI • Provide accountings of disclosures of PHI • Maintain and disclose PHI in accordance with the regulation and your Notice of Privacy Practices
BUSINESS ASSOCIATES	• Provide access to PHI as required to the Covered Entity or individual • Do not inappropriately use or disclose PHI • Provide accounting for disclosures to the Covered Entity
HIPAA Security Rule	
TECHNICAL SAFEGUARDS	• Access Control • Audit Controls • Integrity Controls • Transmission Security
PHYSICAL SAFEGUARDS	• Physical Access Controls • Workstation Security • End User Device and Portable Media Controls
ADMINISTRATIVE SAFEGUARDS	• Security Management • Risk Management • Security Awareness and Training • Security Incident Process • Contingency Plan • Contractual Agreements

*https://www.hipaajournal.com/2020-hipaa-violation-cases-and-penalties/

What Does the Compliance Process Look Like?



Organizations should begin their HIPAA compliance journey with a risk assessment to determine their risk exposure and how their current controls measure up for compliance. Following the risk assessment, organizations will have a roadmap to work from. Further, the risk assessment will help establish priorities and assist in determining the level of input and workload for the cross-functional teams often needed to solve for HIPAA.

After the risk assessment, the organization should consider performing an audit comparing their current policies, processes and practices to the Department of Health and Human Services Office of Civil Rights Audit Protocol (Audit Protocol | HHS.gov). This will allow the organization to provide evidence of compliance with the guidance issued by the Department of Health and Human Services to regulators and customers.

Following the implementation of the HIPAA requirements, it is important to ensure the program remains up-to-date and accurate. This includes operationalizing tasks to ensure they are repeatable and flexible, and monitoring for changes in the HIPAA guidance which may require the program to be updated to comply. An organization's ecosystem is always changing, especially when it comes to vendors and the personal information collected. These changes will need to be accounted for in the program and updated on a regular basis. Further, HIPAA requires organizations to do continuous monitoring and periodic risk assessments to ensure compliance with the requirements.

HIPAA Readiness Checklist

The checklist below can be used to determine your organization's HIPAA compliance posture.

Governance Requirements	YES	NO
Do you have an Assigned Security Official responsible for overseeing your organization's information security framework?		
Have you formally documented your Information Security Policies and Procedures?		
Do your employees and contractors agree to an Acceptable Use Policy?		
Do you have contracts outlining expected security with any organizations you share protected health information with (Business Associate Agreements)?		
Do have an Incident Response Plan to respond to security issues? Has it been tested?		
Do you have a formal Employee Sanction Policy?		
Do you have a documented Contingency/Disaster Recovery Plan? Has it been tested?		
If you are a covered entity, do you have an Assigned Privacy Official?		
If you are a covered entity, do you have a formal Notice of Privacy Practices that is provided to your patients/customers?		
If you are a covered entity, have you formally documented your Privacy Policies and Procedures?		

Operational Requirements	YES	NO
Are all employees provided with HIPAA Training upon hiring and annually thereafter?		
Do you provide periodic security reminders?		
Are formal background checks performed prior to onboarding employees or contractors?		
Do you have physical access controls restricting access to areas with confidential information?		
Do you perform an annual Enterprise Security Risk Assessment?		
Do you have formal monitoring of information system activity? (audit logging, access monitoring)		
Are processes in place to delete logical and physical access in a timely manner for terminated employees, contractors and vendors?		
Do you have a formal media sanitization process for devices and media that are no longer in use or being reassigned?		
Do you have formal controls for the use and disclosure of PHI?		
Do you have a formal process to address requests for access and/or modification of PHI maintained by your organization?		

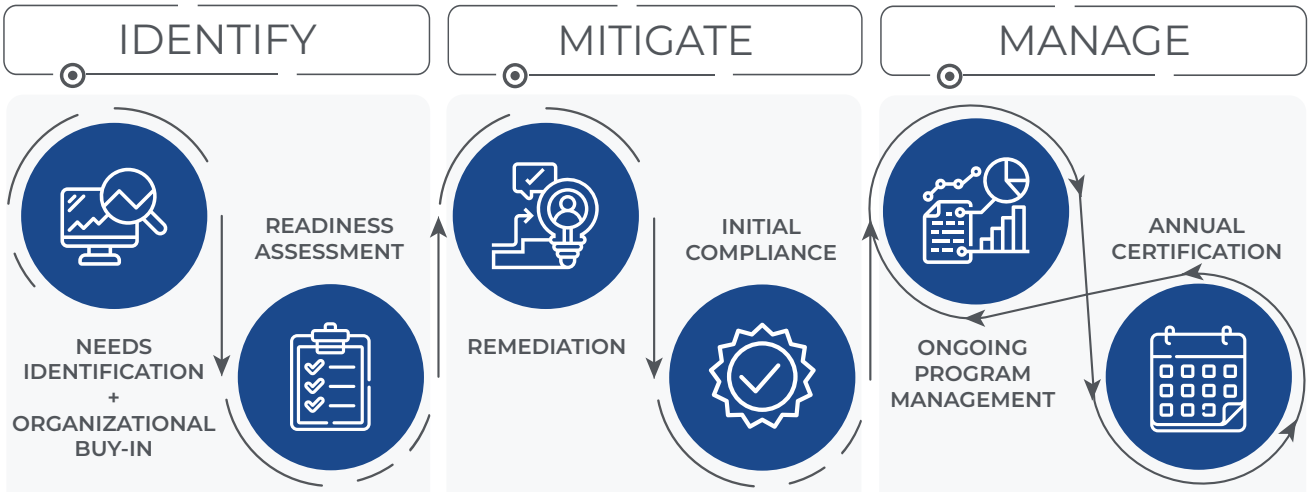
Technical Requirements	YES	NO
Have logical access controls which allow you to limit access to PHI to the minimum required access level been implemented?		
Do you have a formally documented ePHI data flow?		
Has up-to-date Anti-Virus protection been installed on all devices?		
Are all end user devices equipped with automatic log-off when unused for a predetermined time?		
Is all ePHI always encrypted?		
Do you monitor transmission of ePHI so transmissions are not intercepted or altered?		
Do you have active intrusion detection monitoring? Are alerts responded to in a timely manner?		

Got questions about your business?
Click here to speak with an expert!

NEED HELP?

How CompliancePoint Can Help

CompliancePoint provides a full suite of services that help organizations manage and respond effectively to compliance requirements. Using our IDENTIFY, MITIGATE + MANAGE approach, we help organizations proactively identify their gaps, build out frameworks to meet compliance requirements and help manage long term programs to maintain this posture.



HEALTHCARE SERVICES

IDENTIFY	MITIGATE	MANAGE
• Data Inventory & Mapping • Readiness/Gap Assessments • Risk Assessments • Vulnerability Scanning & Penetration Testing	• Policy and Procedure Development • Privacy and Security Training • Remediation Consulting	• Compliance and Security Program Management • Compliance Program Monitoring • Breach Reporting Assistance • Annual certification of HIPAA program • HITRUST Management Program

About CompliancePoint

CompliancePoint is a leading provider of risk management services focused on information security, data privacy, and compliance. Organizations face many risks associated with engaging their marketplace including how they process information internally and with whom they share information downstream. Our mission is to help our clients interact responsibly with their customers and the marketplace.

The difference is simple – data privacy, security and compliance have been at the core of our service offering for almost two decades. We provide our clients with a broad view of industry best practices and benchmarking that allows our customers to make informed business decisions, helping to minimize impact to business operations and maximize return on investment.

- Business-centric approach
- Full lifecycle support
- Company-specific recommendations
- Over 2,500 companies assessed
- True practitioners with hands-on experience
- Net Promoter Score (NPS) of 92 – our customers love us!

For more information about HIPAA or other healthcare regulations and how they apply to your specific organization, contact us at **connect@compliancepoint.com**