2020

HIPAA COMPLIANCE CHECKLIST

Is your organization in compliance with the Health Insurance Portability and Accountability Act requirements? Use this checklist to find out.

RedTeam Security

THREAT PREVENTION EXPERTS

(612) 234-7848 | info@redteamsecure.com
www.redteamsecure.com

Table of Contents

About HIPAA

The term HIPAA refers to the 1996 Health Insurance Portability and Accountability Act, which outlines data privacy and security provisions meant to safeguard patients' medical information. The law has become even more relevant in the digital age, as more and more records become virtually accessible and cyber attackers set their targets on medical entities. Failure to comply with HIPAA regulations can result fines, criminal charges, civil action lawsuits or, in a worst-case scenario, a catastrophic data breach.

About This Checklist

This checklist was developed directly from HIPAA requirements outlined by the U.S. Department of Health and Human Services and supported by RedTeam's broad medical cybersecurity expertise.

Checklist items in bold print are covered by RedTeam's services, with additional information to help you take the next step in fulfilling that requirement.

For more information on HIPAA as well as who and what fall under its requirements, visit HHS.gov.

Part I: Administrative Safeguards

- ☐ Have you completed a risk analysis in accordance with NIST guidelines?
- ☐ Have you completed the risk management process per NIST guidelines?

NOTE: The NIST cybersecurity framework is a robust set of policies outlining cybersecurity best practices for private sector organizations in the U.S. It is considered the gold standard among cybersecurity professionals.

- ☐ Do you have formal sanctions against employees who fail to comply with security policies and procedures?
- ☐ Have you implemented procedures to regularly review records of information system activity? This may include audit logs, access reports, security incident tracking, et. al.
- ☐ Have you identified the security official who is responsible for developing and implementing the policies and procedures outlined here?
- ☐ Have you implemented policies and procedures to ensure that all members of the workforce have appropriate access to EPHI (electronic protected health information), and to prevent workforce members who do not have access from obtaining it?
- ☐ Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed?
- ☐ Have you implemented procedures to determine whether an employee's EPHI access is appropriate?
- ☐ Have you implemented procedures for terminating access to EPHI when an employee leaves your organization, or as otherwise necessary?

NOTE: Learn 6 essentials for raising your employees' cybersecurity awareness here.

- ☐ If you are a clearinghouse that is part of a larger organization, have you implemented policies and procedures to protect EPHI from the larger organization?
- ☐ Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process?
- ☐ Have you implemented policies and procedures to document, review, and modify a user's right of access to a workstation, transaction, program, or process?
- ☐ Do you have a security awareness and training program for all members of your workforce?
- ☐ Do you issue periodic information security reminders?
- ☐ Do you have policies and procedures for guarding against, detecting, and reporting malicious software?

- ☐ Do you have procedures for monitoring login attempts and reporting discrepancies?
- ☐ Do you have procedures for creating, changing, and safeguarding passwords?
- ☐ Do you have policies and procedures in place to address security incidents?
- ☐ Do you have procedures to identify and respond to suspected or known security incidents, mitigate them to the extent practicable, and document the incidents and their outcomes?
- ☐ Have you established policies and procedures for responding to an emergency or other occurrence? This might include fire, vandalism, system failure, or a natural disaster that damages systems that contain EPHI.
- ☐ Have you established written contracts with any subcontractors that create, receive, maintain, or transmit EPHI on your behalf that ensure compliance with these regulations?
- ☐ Have you established and implemented procedures to create and maintain retrievable exact copies of EPHI?
- ☐ Have you established procedures to restore any loss of EPHI data that is stored electronically?
- ☐ Have you established procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode?
- ☐ Have you implemented procedures for periodic testing and revision of contingency plans?
- ☐ Have you assessed the relative criticality of specific applications and data in support of other contingency plan components?
- ☐ Have you established a plan for periodic technical and non-technical evaluation of the security of EPHI?

NOTE: Third parties are one of your organization's biggest risk areas when it comes to HIPAA compliance. They're a growing source of data breaches; third parties were to blame for the breaches of Boston Medical Center and Medical Informatics Engineering, among others.

Part II: Physical Safeguards

- ☐ Have you implemented policies and procedures to limit physical access to your electronic information systems and the facilities in which they are housed?
- ☐ Have you established procedures that allow facility access in support of restoration of lost data during an emergency or disaster?
- ☐ Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft?
- ☐ Have you implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision?
- ☐ Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (i.e. hardware, walls, doors, and locks)?

NOTE: They are so simple, but so vulnerable: your doors. Learn the three biggest points of weakness for your doors and how to protect them here.

- ☐ Have you implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access EPHI?
- ☐ Have you implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users?
- ☐ Have you implemented policies and procedures that govern the movement of electronic media that contain EPHI inside and out of your facilities?
- ☐ Have you implemented policies and procedures to address the disposal of EPHI, and the hardware or electronic media on which it is stored?
- ☐ Have you implemented procedures for removing EPHI from electronic media before the media are available for reuse?
- ☐ Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement?
- ☐ Do you create a retrievable, exact copy of EPHI when needed before movement of equipment?

Part III: Technical Safeguards

- ☐ Have you implemented technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights?
- ☐ Have you assigned a unique name and/or number for identifying and tracking user identities?
- ☐ Have you established procedures for obtaining for obtaining necessary EPHI during an emergency?
- ☐ Have you implemented procedures that terminate an electronic session after a predetermined period of inactivity?
- ☐ Have you implemented a mechanism to encrypt and decrypt EPHI?
- ☐ Have you implemented audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI?
- ☐ Have you implemented policies and procedures to protect EPHI from being improperly altered or destroyed?
- ☐ Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner?
- ☐ Have you implemented authentication procedures to verify that a person or entity seeking access to EPHI is the one claimed?
- ☐ Have you implemented technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network?
- ☐ Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of?
- ☐ Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate?

NOTE: Consider using biometric authentication or, at the very least, two-factor authentication for users to access EPHI.

About RedTeam Security

RedTeam Security has been a premiere provider of offensive information security services since 2008. In today's marketplace, companies are overwhelmed by security threats from hackers originating from all over the world. Studies show that the number of attacks against companies are increasing and at the same time becoming more complex. As a result of these attacks, the number of data breaches have cost companies' tens of millions of dollars as well as grave reputational damage.

The information security experts RedTeam Security have years of experience helping organizations of all sizes identify and mitigate security vulnerabilities. Our team of highly trained analysts hold the following indsutry certifications;

- Certified Networking Associate (CCNA)
- Cisco Certified Networking Associate Security (CCNA Security)
- Cisco Certified Networking Associate Cyber Ops (CCNA Cyber Ops)
- Comptia Security+
- OSCP (Offensive Security Certified Professional)
- GWAPT (GIAC Web Application Penetration Tester)
- GIAC Security Essentials (GSEC)
- GIAC Certified Incident Handler (GCIH)
- GIAC Python Coder (GPYC)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Web Application Defender (GWEB)

At RedTeam Security we are committed to securing your organization. Whether you are ready to begin a project today or are looking for guidance on where to start, our team of security experts are here to help you navigate the complexities around information security. Schedule a free consultation with our team today, or answer a few questions to help us get started on a customized proposal for you immediately. We look forward to working with you.

Jon Anderson

President, RedTeam Security

Portfolio of Services

- Network Penetration Testing
- Web App Penetration Testing
- Physical Penetration Testing
- Cryptocurrency Penetration Testing
- Social Engineering
- Red Teaming
- Cyber Security Awareness Training
- Compliance (PCI, NERC, HIPAA, FDIC)

> **LEARN MORE**

Take the Next Step

Ready to improve your security posture with the help of RedTeam Security?

LOOKING FOR SOME GUIDANCE

Not sure where to start? Discuss your unique security needs and get your questions answered during a one-on-one consultation with one of our security professionals.

GO

READY FOR A PROPOSAL

Ready for us to prepare a proposal? Fill out our scoping questionnaire and give us a bit of background information on your project and we will send you a customized proposal.

GO

2020

Find. Fix. Fortify.

RedTeam Security

THREAT PREVENTION EXPERTS

(612) 234-7848 | info@redteamsecure.com
www.redteamsecure.com