TECH365

*Trusted Support Year-Round*

# HIPAA COMPLIANCE GUIDE

## COMPLIANCE WITHOUT THE COMPLICATION


(317) 762-8362

WECARE@TECH365.SUPPORT

HTTPS://TECH365.SUPPORT

# TABLE OF CONTENTS



TECH365

# A PRACTICAL GUIDE TO HIPAA COMPLIANCE

## Overview

Tech365 supports healthcare organizations and business associates with secure, HIPAA-aligned technology solutions. This guide outlines the core requirements of HIPAA and explains how practical security controls help protect sensitive health information.

## What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law designed to protect sensitive patient health information. HIPAA is intended to:

- Protect patients' medical records and personal health information (PHI)
- Ensure the confidentiality, integrity, and availability of healthcare data
- Standardize electronic health transactions
- Allow individuals to maintain health insurance coverage during job changes

## Understanding HIPAA Compliance

HIPAA establishes national standards for safeguarding medical records and other personal health information. The regulation continues to evolve as technology and security risks change. There are three primary rules that define HIPAA compliance:

### The Privacy Rule

Defines how protected health information may be used and disclosed.

### The Security Rule

Requires administrative, physical, and technical safeguards to protect electronic protected health information (ePHI).

### The Breach Notification Rule:

Requires organizations to notify affected individuals and federal authorities in the event of a breach involving unsecured PHI.

This guide explains these requirements and highlights how proper technology controls support compliance.

# THE PRIVACY RULE

## Primary Objectives

- Protect the privacy of protected health information (PHI)
- Define how PHI may be used and disclosed
- Ensure patients have the right to access and control their health information

## What is Protected Health Information (PHI)?

Protected Health Information (PHI) includes any individually identifiable health information transmitted or maintained in electronic, paper, or oral form such as:

- Name, address, birth date, and social security number
- Medical records, diagnoses, treatment plans
- Billing information, insurance data
- Lab results, imaging, prescriptions

## Key Requirements of the Privacy Rule

| CATEGORY | DESCRIPTION |
|---|---|
| Use & Disclosure | PHI may only be used or disclosed for treatment, payment, or operations unless patient authorization is obtained. |
| Minimum Necessary Rule | Only the minimum amount of PHI necessary should be accessed or disclosed to accomplish the intended purpose. |
| Patient Rights | Patients have the right to access, review, and request amendments to their health records. |
| Administrative Requirements | Covered Entities and Business Associates must designate a privacy officer, implement policies, and train staff. |
| Safeguards | Reasonable safeguards must be in place to protect PHI from intentional or unintentional disclosure. |

# HOW SECURE TECH SUPPORTS THE PRIVACY RULE

## Access Control Systems

- Make sure employees only see the patient information they actually need
- Add secure sign-in protections so unauthorized users cannot access sensitive data
- Review and adjust permissions as roles change

## Data Protection

- Encrypt patient information so it cannot be read if systems are compromised
- Protect email and remote access so data stays secure outside the office
- Use secure communication tools when sharing sensitive information

## Activity Monitoring

- Track who accesses patient data and when
- Monitor for unusual activity and investigate when something looks off
- Maintain records that support compliance reviews

## Secure File Storage & Sharing

- Use compliant cloud platforms designed to protect health information
- Control who can access shared files
- Keep detailed logs of file access and activity

## Device Protection

- Install security software on all devices accessing patient data
- Manage smartphones, tablets, and laptops that connect to your systems
- Enable remote wipe if a device is lost or stolen

## Backup & Disaster Recovery

- Maintain encrypted backups stored securely offsite
- Regularly test backups to confirm data can be restored
- Plan for system recovery during outages or cyber incidents

## Email Security

- Protect email with encryption and filtering
- Reduce the risk of phishing and malicious attachments
- Maintain message records for compliance support

## Training and Access Logs

- Provide structured HIPAA training for staff
- Set clear policies for handling patient information
- Monitor user activity to reduce misuse or accidental exposure

# TECH365'S ROLE IN PRIVACY RULE COMPLIANCE

| | |
|---|---|
| **HIPAA Risk Assessments** | • Evaluate your systems to identify security gaps and areas of risk<br>• Review how patient information is accessed, stored, and protected<br>• Provide a clear remediation plan to reduce exposure |
| **Access Control Implementation** | • Limit access to patient information based on job responsibilities<br>• Monitor who accesses data and when<br>• Automatically log users out to reduce unauthorized access |
| **Data Encryption & Transmission Protections** | • Encrypt sensitive information stored in your systems<br>• Protect email and remote connections used to access patient data<br>• Secure how data is shared between locations and partners |
| **Secure Backup & Disaster Recovery** | • Maintain encrypted backups stored securely offsite<br>• Store copies in separate locations to reduce risk<br>• Test recovery processes to confirm data can be restored |
| **Access Policies** | • Establish clear rules for who can access patient information<br>• Document employee responsibilities and expectations<br>• Require signed acknowledgments of data handling policies |
| **Business Associate Agreement Management** | • Ensure required agreements are in place with partners handling patient data<br>• Maintain organized records of all agreements<br>• Review agreements regularly to confirm ongoing compliance |
| **Technical Safeguards Setup** | • Protect devices and systems with appropriate security controls<br>• Manage smartphones and laptops that access patient information<br>• Monitor systems for suspicious activity |
| **Incident Response & Breach Notification Readiness** | • Develop a clear response plan for security incidents<br>• Track and document potential breaches<br>• Support required notifications if an incident occurs |
| **Documentation & Audit Readiness** | • Maintain organized records of policies and security controls<br>• Document risk assessments and corrective actions<br>• Prepare supporting documentation for potential audits |

# THE SECURITY RULE

## Primary Objectives

- Protect the confidentiality, integrity, and availability of electronic health information
- Safeguard systems against expected threats and vulnerabilities
- Prevent unauthorized access, use, or disclosure of patient data
- Ensure staff follow established security practices

## What is ePHI?

Electronic Protected Health Information refers to patient health information that is created, stored, transmitted, or received electronically.

This includes information stored in:

- Electronic medical record systems
- Billing and insurance platforms
- Diagnostic imaging and lab systems
- Email messages containing patient information
- Cloud platforms, mobile devices, and portable storage

## Key Requirements of the Security Rule

| CATEGORY | DESCRIPTION |
|---|---|
| Administrative Safeguards | • Conduct regular risk assessments and address vulnerabilities<br>• Assign clear responsibility for overseeing security efforts<br>• Provide staff training on protecting patient information<br>• Maintain backup, recovery, and contingency plans |
| Physical Safeguards | • Control access to facilities and areas where systems are located<br>• Secure workstations and devices that store or access patient data<br>• Establish policies for proper disposal or reuse of equipment<br>• Limit physical access to authorized personnel only |
| Technical Safeguards | • Assign unique user accounts to control system access<br>• Monitor and log system activity involving patient data<br>• Protect data from unauthorized changes or deletion<br>• Encrypt sensitive information during storage and transmission |

# SECURITY RULE COMPLIANCE SUPPORT

## ADMINISTRATIVE SAFEGUARDS

**Security Risk Assessments:**

Regular system evaluations to identify vulnerabilities and prioritize fixes.

**Policy Management:**

Clear documentation and policy updates to support ongoing compliance.

**Security Awareness Training:**

Ongoing training to help staff recognize threats and protect patient information.

**Access Control Oversight:**

Centralized management of user access to limit exposure of sensitive data.

## PHYSICAL SAFEGUARDS

**Video Surveillance Systems:**

Monitor access to server rooms and other sensitive areas.

**Keycard and Biometric Access Systems:**

Restrict entry to secure areas and equipment.

**Asset Management Software:**

Track devices that store or access patient information.

**Device Management Controls:**

Enforce encryption, remote wipe, and usage policies on mobile devices.

## TECHNICAL SAFEGUARDS

**Data Encryption:**

Protect patient information with encryption in storage and transit.

**Access Controls:**

Limit system access using secure logins and multi-factor authentication.

**Activity Monitoring:**

Track system activity and alert administrators to suspicious behavior.

**Secure Backups:**

Maintain encrypted backups with reliable restoration capabilities.

# TECH365'S ROLE IN SECURITY RULE COMPLIANCE

The Security Rule focuses on protecting electronic patient information through administrative, physical, and technical safeguards. Our role is to implement and manage the security controls that keep your organization aligned and protected.

| | |
|---|---|
| **Risk Analysis & Assessment** | • Conduct structured security risk assessments<br>• Identify vulnerabilities across systems and workflows<br>• Provide clear recommendations to reduce risk |
| **Infrastructure Security** | • Secure networks and segment sensitive environments<br>• Configure firewalls and protective system controls<br>• Isolate critical systems that store patient information |
| **Endpoint & Access Security** | • Protect laptops, desktops, and mobile devices<br>• Enforce secure login requirements<br>• Manage user access and remove permissions when roles change |
| **Data Protection** | • Maintain encrypted backups of critical systems<br>• Protect data stored in cloud and on-premise environments<br>• Monitor file access for unusual activity |
| **Incident Response Strategy** | • Develop clear plans for handling security incidents<br>• Prepare response procedures for potential data breaches<br>• Monitor systems to detect and investigate threats |
| **Ongoing Monitoring & Support** | • Continuously monitor system health and security alerts<br>• Apply updates and patches to reduce vulnerabilities<br>• Provide ongoing oversight of security controls |
| **Training & Documentation** | • Deliver structured compliance training for staff<br>• Maintain documentation of policies and security activities<br>• Prepare records to support audits and assessments |

## What This Means For Your Business

- ✓ Reduced risk of costly data breaches
- ✓ Stronger protection for patient data
- ✓ Clear documentation for audits
- ✓ Defined response processes
- ✓ Greater control over data access
- ✓ Ongoing compliance oversight

# THE BREACH NOTIFICATION RULE

## Primary Objectives

- Ensure transparency when patient data is compromised
- Protect individuals from fraud and misuse of their information
- Promote timely response and corrective action after incidents

## Key Requirements of the Breach Notification Rule

### Definition of a Breach

A breach is the unauthorized access, use, or disclosure of unsecured patient health information.

### Risk Assessment Requirement

When a potential breach occurs, the organization must evaluate:

- The type of information involved
- Who accessed the information and whether it was viewed or acquired
- The potential risk of harm and steps taken to reduce that risk

## Breach Notification Requirements

| PARTY TO NOTIFY | WHEN | HOW |
|---|---|---|
| Affected Individuals | Within 60 calendar days | Written notice by mail or email |
| HHS (Office for Civil Rights) | <500 individuals: Annually<br>≥500 individuals: Within 60 days | Via HHS Breach Portal |
| Media (if ≥500 affected in one region) | Within 60 days | Press release to prominent outlets |

Notifications must include:

- A description of what happened
- The type of information involved
- Steps individuals can take to protect themselves
- Actions being taken to investigate and prevent future incidents
- Contact information for follow-up questions

# HOW TECHNOLOGY SUPPORTS COMPLIANCE

## PREVENTION & DETECTION

- Encrypt patient information so it remains protected if systems are compromised
- Monitor systems for unusual access or suspicious activity
- Control user access to limit exposure of sensitive data

## INVESTIGATION & DOCUMENTATION

- Maintain audit logs to track access and system changes
- Evaluate incidents to determine potential risk and required response
- Document findings and corrective actions for compliance records

## NOTIFICATION & COMMUNICATION

- Deliver compliant breach notifications when required
- Inform affected individuals through secure communication channels
- Maintain backup and recovery systems to support continuity after incidents

## Tech365's Role in Breach Notification Compliance

| | |
|---|---|
| Breach Detection & Monitoring | • Monitor systems for unusual activity or unauthorized access<br>• Track access attempts and security events<br>• Provide continuous oversight of endpoint activity |
| Incident Response Planning | • Develop and maintain documented response plans<br>• Test response procedures through internal exercises<br>• Train staff on how to respond to potential breaches |
| Access Control & Authentication | • Develop and maintain documented response plans<br>• Test response procedures through internal exercises<br>• Train staff on how to respond to potential breaches |
| Data Protection & Encryption | • Encrypt sensitive data during transmission<br>• Protect information stored on devices and in the cloud<br>• Ensure encryption is properly configured and maintained |
| Secure Backup & Recovery | • Maintain encrypted backups of critical systems<br>• Test backups regularly to confirm restoration capability<br>• Support business continuity after security incidents |
| Documentation & Reporting Support | • Maintain breach logs and risk documentation<br>• Support required reporting to regulatory authorities<br>• Assist with preparing documentation for affected individuals |

# HOW TECHNOLOGY SUPPORTS COMPLIANCE

## PREVENTION & DETECTION

- Encrypt patient information so it remains protected if systems are compromised
- Monitor systems for unusual access or suspicious activity
- Control user access to limit exposure of sensitive data

## INVESTIGATION & DOCUMENTATION

- Maintain audit logs to track access and system changes
- Evaluate incidents to determine potential risk and required response
- Document findings and corrective actions for compliance records

## NOTIFICATION & COMMUNICATION

- Deliver compliant breach notifications when required
- Inform affected individuals through secure communication channels
- Maintain backup and recovery systems to support continuity after incidents

## Tech365's Role in Breach Notification Compliance

| | |
|---|---|
| Breach Detection & Monitoring | • Monitor systems for unusual activity or unauthorized access<br>• Track access attempts and security events<br>• Provide continuous oversight of endpoint activity |
| Incident Response Planning | • Develop and maintain documented response plans<br>• Test response procedures through internal exercises<br>• Train staff on how to respond to potential breaches |
| Access Control & Authentication | • Develop and maintain documented response plans<br>• Test response procedures through internal exercises<br>• Train staff on how to respond to potential breaches |
| Data Protection & Encryption | • Encrypt sensitive data during transmission<br>• Protect information stored on devices and in the cloud<br>• Ensure encryption is properly configured and maintained |
| Secure Backup & Recovery | • Maintain encrypted backups of critical systems<br>• Test backups regularly to confirm restoration capability<br>• Support business continuity after security incidents |
| Documentation & Reporting Support | • Maintain breach logs and risk documentation<br>• Support required reporting to regulatory authorities<br>• Assist with preparing documentation for affected individuals |

# WHY HIPAA COMPLIANCE MATTERS

HIPAA compliance protects your operations, reputation, and patient trust. Without structured safeguards and oversight, the risk of disruption, scrutiny, and financial strain increases.

## The Business Impact of Getting IT Wrong

A single breach can lead to:

- Operational downtime
- Required public notifications
- Long-term reputation damage
- Increased regulatory scrutiny
- Loss of patient or partner trust
- Legal exposure and financial strain

## Compliance Is Ongoing, Not One-Time

Security threats evolve. Technology changes. Staff roles shift. Systems expand. Compliance must evolve alongside them.

That means:

- Regular risk evaluations
- Continuous monitoring
- Tested response plans
- Documented processes
- Clear accountability

Organizations that treat it as a structured discipline operate with greater confidence and fewer surprises.

## Bringing It All Together

Effective HIPAA compliance requires prevention, monitoring, response, documentation, and recovery working together. It requires leadership. It requires structure. And it requires accountability.

When compliance is actively managed, your organization is not just meeting regulatory requirements. You are protecting your operations, your reputation, and the people who trust you with their information.

# PREPARED FOR THE UNEXPECTED

At Tech365, we don't just provide IT support and compliance solutions. We make a promise to safeguard your business, your people, and your data. One way we do that is by maintaining strong, comprehensive insurance coverage. We have taken extra steps to ensure that everyone involved, from your team to ours, has coverage in place when things do not go as planned. Because when your technology partner is protected, so are you.

**OUR INSURANCE COVERAGE INCLUDES:**

- **$1 Million Commercial Auto**
  If our technicians are en route to your office and an accident occurs, this coverage ensures that any damages or liabilities are properly handled. It protects our staff, your property, and the public. This keeps disruptions and liabilities away from your business.

- **$1 Million Employers Liability**
  This protects our team members while they are on the job. In the rare event of a work-related injury, our coverage prevents complications or liability from reaching your business. It reflects our commitment to safety and accountability in every interaction.

- **$2 Million General Liability**
  Accidents can happen, even in the most controlled environments. This policy covers things like property damage or accidental injuries that may occur during service calls or installations. It protects both our company and yours from potential financial impact.

- **$3 Million Cybersecurity Policy**
  Your data security is critical. In the unlikely event of a cyber breach involving our systems or service delivery, this policy provides financial protection and response resources. It is an added layer of defense that ensures you are not left vulnerable by association.

- **$5 Million Umbrella Coverage**
  This extended coverage adds an additional layer of protection beyond the limits of our other policies. It provides peace of mind for larger, unexpected events and ensures that even rare, high-impact situations are covered without placing your business at risk.

We are fully insured because we take your trust seriously. From safeguarding your systems to backing our work with real protection, Tech365 is here to provide confidence every step of the way. When you choose us, you are choosing a partner who plans ahead not just for success, but for safety and stability.

TECH365

# SERVER ROOM LOG

| DATE | NAME AND POSITION | PURPOSE |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

TECH365