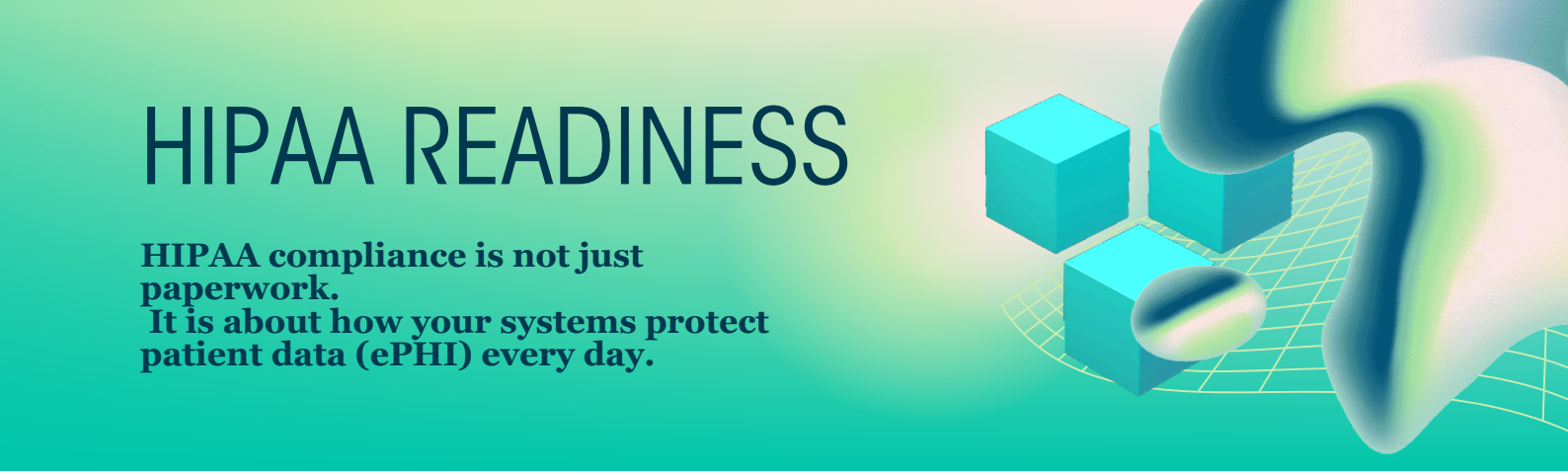

HIPAA IT Readiness Checklist for Small Businesses (2026 Edition)

Use this checklist to evaluate whether your IT environment is ready to support HIPAA requirements.

HIPAA IT Readiness Checklist

1. Identify Where ePHI Exists

□ You know which systems store or process patient data
□ Email, file storage, backups, and devices are included
□ Data flow between systems is understood

Why this matters:
You cannot protect what you cannot locate.

2. Access Control Is Enforced

□ Each user has a unique login
□ Access is based on job role (least privilege)
□ Shared accounts are not used
□ Access is removed when employees leave

Why this matters:
HIPAA requires controlled access to ePHI.

3. Multi-Factor Authentication (MFA) Is Enabled

□ MFA is required for email and cloud systems
□ MFA is used for remote access

□ Admin accounts have stronger protection

Why this matters:
MFA is one of the most effective ways to prevent unauthorized access.

4. Devices Are Secured and Managed

□ All work devices require login protection
□ Devices are encrypted
□ Antivirus or endpoint protection is active
□ Devices are kept up to date

Why this matters:
Lost or compromised devices are a major source of breaches.

5. Data Is Encrypted (At Rest and In Transit)

□ Data is encrypted on devices and servers
□ Secure connections (HTTPS, VPN, etc.) are used
□ Email containing sensitive data is handled securely

Why this matters:
Encryption reduces exposure if systems are compromised.

6. Audit Logs and Monitoring Are in Place

□ Access to sensitive systems is logged
□ Logs are reviewed periodically
□ Suspicious activity is investigated

Why this matters:
HIPAA requires the ability to track and review access.

7. Backup and Recovery Are Verified

□ Backups are performed regularly
□ Backup data is protected and isolated
□ Restore testing has been completed
□ Recovery timelines are understood

Why this matters:
Data availability is part of HIPAA—not just confidentiality.

8. Incident Response Plan Exists

□ A response plan is documented
□ Roles and contacts are defined
□ Breach response steps are understood
□ The plan is reviewed periodically

Why this matters:
HIPAA requires timely response to security incidents.

9. Business Associate Agreements (BAAs) Are in Place

□ Vendors handling ePHI have signed BAAs
□ Cloud providers, IT providers, and software vendors are included
□ Vendor responsibilities are clearly defined

Why this matters:
Vendors are part of your compliance responsibility.

10. Workforce Security and Training

□ Employees receive HIPAA/security training
□ New hires are trained early
□ Phishing awareness is included
□ Employees know how to report incidents

Why this matters:
Human error is a leading cause of HIPAA violations.

11. Remote Access Is Secured

□ Remote access requires MFA
□ Access is limited to approved users
□ Devices used remotely are secured

Why this matters:
Remote work expands exposure to ePHI.

12. Data Retention and Disposal Is Controlled

□ Retention timelines are defined
□ Old data is securely deleted
□ Devices are wiped before reuse or disposal

Why this matters:
Improper data handling increases breach risk.

13. Risk Assessment Is Performed Regularly

□ IT risks are reviewed periodically
□ Vulnerabilities are identified and addressed
□ Changes in systems are evaluated

Why this matters:
HIPAA requires ongoing risk assessment—not a one-time effort.

What HIPAA Readiness Looks Like

You know where patient data is stored
Access is controlled and monitored
Devices and systems are secured
Vendors are accounted for
You can respond quickly to incidents

Quick Rule of Thumb

HIPAA compliance is not a document.
It is how your systems behave every day.

SofTouchSystems.com
No-Surprise IT — Predictable. Proactive. Proven.