BABSTECH LLC

CYBERSECURITY & COMPLIANCE ADVISORY

20-Point Cybersecurity & HIPAA Readiness Checklist

A practical self-assessment for small businesses and healthcare practices

Use this checklist to quickly identify common security gaps in your practice.

This 20-point checklist helps small businesses and healthcare practices spot everyday security weaknesses involving employee access, passwords, MFA, devices, remote work, backups, vendors, policies, and incident response. Answer each item honestly, add up your score, and use the results to decide what to address first.

1. Answer all 20 questions using YES, PARTIALLY, NO, or NOT SURE.
2. Score: YES = 2 points, PARTIALLY = 1 point, NO = 0 points, NOT SURE = 0 points.
3. Add your total (maximum 40) and read the readiness guidance on the last page.

ACCOUNT & ACCESS SECURITY

1. Multi-Factor Authentication

Is MFA enabled on systems containing sensitive or patient information?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

2. Unique User Accounts

Does every employee have an individual account rather than shared credentials?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

3. Access Reviews

Are employee permissions periodically reviewed?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

4. Employee Offboarding

Is access immediately removed when an employee leaves?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

PASSWORD SECURITY

5. Password Policy

Are strong password requirements established and enforced?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

6. Password Manager

Does the organization use or encourage an approved password manager?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

DEVICE SECURITY

7. Device Protection

Are computers and mobile devices protected with passwords/PINs and automatic screen locking?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

8. Encryption

Are devices containing sensitive information appropriately encrypted?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

9. Updates & Patching

Are operating systems, applications, browsers, and devices regularly updated?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

10. Endpoint Protection

Do business devices have appropriate anti-malware/security protection?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

EMAIL & PHISHING

11. Email Security

Are employees trained to recognize phishing and suspicious messages?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

12. Email MFA

Is MFA enabled for business email accounts?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

DATA PROTECTION

13. Backups

Is critical business information backed up regularly?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

14. Backup Recovery

Has the organization verified that important data can actually be restored from backups?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

REMOTE WORK

15. Remote Access

Are employees given secure procedures for accessing business systems remotely?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

16. Public Wi-Fi

Are employees instructed on how to safely handle sensitive information when away from the office?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

HIPAA & VENDOR RISK

17. Vendor Management

Does the practice know which third-party vendors handle or access protected health information?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

18. Business Associate Agreements

Are appropriate BAAs maintained with vendors that handle PHI when required?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

POLICIES & INCIDENT RESPONSE

19. Security Policies

Does the organization maintain documented cybersecurity and information-security policies appropriate to its operations?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

20. Incident Response

Does the organization have a documented process explaining what employees should do if they suspect a breach, lost device, phishing attack, or other security incident?

☐ YES ☐ PARTIALLY ☐ NO ☐ NOT SURE

Score Your Readiness

Add 2 points for every YES, 1 point for every PARTIALLY, and 0 points for every NO or NOT SURE. Maximum score = 40.

YOUR TOTAL SCORE _____ **/ 40**

34 – 40	**STRONG FOUNDATION** Your organization appears to have many fundamental cybersecurity safeguards in place. Continue reviewing, testing, documenting, and improving your security program.
24 – 33	**IMPROVEMENT NEEDED** Several important safeguards may require attention. Prioritize identified gaps and develop a remediation plan.
0 – 23	**HIGH-PRIORITY GAPS** Your responses indicate that important cybersecurity safeguards may be missing or uncertain. Consider conducting a structured cybersecurity risk assessment.

This score is an informal readiness indicator only. It is not a determination of HIPAA compliance.

Not Sure What Your Score Means?

BabsTech can help you understand your security gaps and determine what to address first.

Book Your Free 20-Minute Cybersecurity Consultation →

BabsTech LLC
Cybersecurity & Compliance Advisory
babstech.org