HIPAA Endpoint Security Posture Checklist

A Practical Baseline Assessment for Health Care Organizations

visuaFUSION Systems Solutions | Leveling the IT Playing Field for Rural Health Care

For IT Managers / IT Staff:	For Hospital Administrators / Leadership:
Use this checklist to self-assess your current endpoint security posture against practical, well-established baselines. Check off items already in place and identify gaps.	Hand this checklist to your IT manager or IT staff and ask them to mark which items are already in place at your organization. Use the results to understand where you stand today.

This checklist covers endpoint security fundamentals that every health care organization handling electronic Protected Health Information (ePHI) should have in place. These are not aspirational goals. They are practical, well-understood security measures that have been standard practice in the industry for years.

Items are organized into three tiers to help you prioritize:

Tier 1: Baseline	Fundamental security controls that have existed since Windows Vista (2007). These are the absolute floor.
Tier 2: Standard	Widely adopted security measures that should be present in any modern health care IT environment.
Tier 3: Advanced	Mature security controls that significantly reduce risk. Organizations should be working toward these.

Organization Information

Organization Name: _____

Completed By: _____ Date: _____

Title / Role: _____

TIER 1: BASELINE SECURITY

Controls that have existed since Windows Vista was released in January 2007.

Windows Vista was released 19 years ago. If any of the items below are not in place at your organization, your endpoint security posture is at least 19 years behind the industry -- regardless of what other security tools or products you have deployed. None of the items in this tier require purchasing additional software. They are built into Windows and have been for nearly two decades.

☐ User Account Control (UAC) Enabled on All Endpoints

UAC must be enabled and set to a functional notification level on all workstations and servers. UAC is not just an "annoying popup." It is a core Windows security boundary that prevents processes from silently elevating to administrator privileges. Without UAC, credential theft tools (such as Mimikatz) can access protected memory and extract password hashes -- or in some configurations, actual plaintext passwords -- from a machine in minutes using freely available tools. This enables attackers to authenticate as any user who has logged into that machine without ever knowing their password. Extracting these credentials requires administrator-level access, which UAC is specifically designed to gate.

Supports: 45 CFR 164.312(a)(1) - Access Control; 45 CFR 164.308(a)(5)(ii)(B) - Protection from Malicious Software

If UAC is disabled, an attacker on your network can harvest credentials from every machine they touch.

☐ Windows Firewall Enabled with Specific Inbound Rules

The Windows Firewall must be enabled on all endpoints with a default-deny inbound posture. Only specific, documented exceptions should be allowed inbound (e.g., remote management tools used by IT). "Allow all inbound" rules defeat the entire purpose of the firewall. Without a host-based firewall, any service listening on a machine is directly reachable by any other device on the same network segment.

Supports: 45 CFR 164.312(e)(1) - Transmission Security; 45 CFR 164.306(a)(2) - Protect against reasonably anticipated threats

"Allow all inbound" rules are the same as having no firewall at all.

☐ End Users Do Not Have Local Administrator Rights

Standard end users must not have local administrator privileges on their workstations. Software that appears to require admin rights for normal operation can almost always be resolved through application shimming (adjusting file system permissions, registry permissions, UAC overrides, or service permissions) rather than granting full admin access. Users with admin rights can install unauthorized software, disable security tools, and create openings for malware that a standard user account would have blocked.

Supports: 45 CFR 164.312(a)(1) - Access Control; 45 CFR 164.308(a)(4) - Information Access Management

Application shimming resolves nearly every case where software "needs" admin rights to run.

☐ **All Systems Running Vendor-Supported Operating Systems with Regular Patching**

Every server and workstation must be running an operating system version that still receives regular security patches from the vendor. Systems running end-of-life operating systems must be, at minimum, isolated from the network (placed on a restricted VLAN or disconnected entirely) while a replacement or permanent mitigation plan is put in place. Unpatched systems are one of the top entry points for ransomware in health care, alongside phishing and compromised credentials.

Supports: 45 CFR 164.308(a)(5)(ii)(B) - Protection from Malicious Software; 45 CFR 164.310(d)(2)(iii) - Accountability

End-of-life systems must AT LEAST be isolated from the network immediately.

☐ **Every User Has Their Own Unique Login Credentials**

Every individual who accesses a workstation or email system must have their own uniquely assigned credentials. No shared logins. No shared "nurse" accounts. No generic department email addresses used by multiple staff. This is a Required implementation specification under HIPAA -- not addressable, not optional. Organizations often believe that because staff sign in to the EHR with their own credentials, they are covered. They are not. The EHR is not the only system containing PHI. Even sending IT a screenshot for support with a patient name or date of birth visible in the background makes that workstation and email account a system accessing ePHI -- subject to the same requirements. Unless your organization has the staff and hours to continuously audit and verify that absolutely no PHI ever touches shared workstations or shared email, the practical approach is to treat all workstations and email accounts to the same standard.

Required: 45 CFR 164.312(a)(2)(i) - Unique User Identification (Required); 45 CFR 164.312(b) - Audit Controls

Shared logins make audit trails meaningless. You cannot track who did what if three people share one account.

Tier 1 Score: _____ / 5 items in place

If any of these items are missing, address them before moving to Tier 2. These are your foundation -- everything else builds on top of them.

A NOTE ON CENTRAL MANAGEMENT: DOING IT vs. PROVING IT

Throughout this checklist, you will see "central management is preferred" on several items. Here is why that matters beyond just convenience:

It is one thing to DO something. It is another thing entirely to PROVE you did it.

Consider a stolen laptop containing PHI. If you encrypted that laptop but cannot produce a report proving it was encrypted at the time of theft, you will have a very hard time avoiding a reportable breach. The same applies to anti-virus, patching, screen lock policies, and every other control on this list.

Central management platforms (Active Directory Group Policy, Microsoft Configuration Manager, Intune, etc.) give you the reporting and audit trail to demonstrate that a control was in place at a specific point in time. Without that proof, regulators and auditors have no reason to take your word for it -- and neither will the Office for Civil Rights if they come knocking.

TIER 2: STANDARD SECURITY

Widely adopted measures that should be present in any modern health care IT environment.

☐ Full Disk Encryption on All Drives

Encryption must be implemented on all operating system drives, fixed data drives, and removable drives attached to systems that access or store ePHI. Windows BitLocker is the standard solution for Windows environments and is included in Windows Pro and Enterprise editions at no additional cost. Central management of encryption keys and recovery is strongly preferred (via Active Directory, MBAM, or Configuration Manager). Without disk encryption, a lost or stolen laptop is an automatic HIPAA breach with mandatory notification obligations.

Supports: 45 CFR 164.312(a)(2)(iv) - Encryption and Decryption; 45 CFR 164.310(d)(1) - Device and Media Controls

Central key management is strongly preferred. Without encryption, any lost device is a reportable breach. Without central reporting, you cannot PROVE a device was encrypted at the time it was lost.

☐ Anti-Virus / Anti-Malware Enabled with Daily Definition Updates

Anti-virus or anti-malware software must be enabled and actively running on all endpoints. Virus definitions and detection signatures must update at least once per day. Central management through a management console is strongly preferred so that IT staff can confirm protection status, receive alerts on detections, and identify endpoints that have fallen out of compliance. Windows Defender (built into Windows 10/11 and Server 2016+) is acceptable when properly configured and monitored.

Supports: 45 CFR 164.308(a)(5)(ii)(B) - Protection from Malicious Software; 45 CFR 164.306(a)(2) - Protect against reasonably anticipated threats

Central management lets you PROVE protection status and update compliance. "Installed" is not the same as "current."

☐ Screen Lock / Screensaver Enforced at 15 Minutes or Less

All workstations must automatically lock after no more than 15 minutes of inactivity. This should be enforced centrally via Group Policy or MDM rather than relying on individual users to configure their own settings. In health care environments where workstations are in shared or semi-public areas (nursing stations, front desks, exam rooms), this is critical to preventing unauthorized access to ePHI displayed on screen.

Supports: 45 CFR 164.312(a)(2)(iii) - Automatic Logoff; 45 CFR 164.310(b) - Workstation Use

Central enforcement lets you PROVE this policy is applied. Do not rely on users to configure this themselves.

☐ SSL, TLS 1.0, and TLS 1.1 Disabled

All deprecated encryption protocols (SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1) must be disabled on servers and workstations. These protocols contain known, exploitable vulnerabilities that score at the highest severity levels (CVSS 7.0-10.0) on vulnerability scanners. They are not theoretical risks -- they are well-understood attack paths that can allow an attacker to intercept or take over communications on a machine with these protocols enabled. Only TLS 1.2 and TLS 1.3 should remain enabled. This applies to web servers, email servers, remote access systems, and any other service that uses encrypted communications. Some legacy applications may require remediation or vendor engagement to support modern protocols.

Supports: 45 CFR 164.312(e)(1) - Transmission Security; 45 CFR 164.312(e)(2)(ii) - Encryption

TLS 1.0/1.1 vulnerabilities are rated high to critical severity. These are not low-risk findings.

☐ SMB v1 Disabled and SMB Signing Enforced

SMB version 1 must be fully disabled on all systems. SMBv1 is the protocol exploited by WannaCry, NotPetya, and numerous other ransomware attacks that have devastated health care organizations globally. In addition, SMB signing must be enforced to prevent man-in-the-middle and relay attacks against file shares and domain authentication. Note: SMB signing enforcement is the default starting in Windows 11 24H2 and Server 2025; all prior OS versions require explicit configuration.

Supports: 45 CFR 164.312(e)(1) - Transmission Security; 45 CFR 164.312(c)(1) - Integrity

SMBv1 was the attack vector for WannaCry ransomware which shut down hospitals worldwide.

☐ Monthly Phishing Simulation Testing

Phishing remains the #1 entry point for cyberattacks in health care, responsible for the initial compromise in roughly half of all ransomware incidents in the sector. Organizations should conduct simulated phishing tests at least monthly to identify high-risk users, reinforce training, and track improvement over time. Small health care organizations actually have an advantage here -- with smaller staff, face-to-face follow-up training with users who fail tests is feasible and far more effective than generic video modules. Central reporting is essential to identify repeat offenders and demonstrate a functioning security awareness program to auditors.

Supports: 45 CFR 164.308(a)(5)(i) - Security Awareness and Training; 45 CFR 164.308(a)(5)(ii)(A) - Security Reminders

Phishing is the #1 initial access vector in health care breaches. Test monthly, train the failures.

☐ Conditional Access Policies for Cloud Applications (M365 / Google Workspace)

Cloud-facing applications require Conditional Access policies that enforce the following: (1) Require authenticator-based or better MFA for all sign-ins originating from outside your organization's networks. (2) Require phishing-resistant MFA (FIDO2, certificate-based) for administrator accounts accessing admin portals, even from on-site. (3) Block sign-in traffic from countries outside the United States by default. Create a separate policy that designated users can be added to in advance of international travel, with a documented process for requesting and approving temporary travel access. These controls dramatically reduce the attack surface for credential-based compromises, which are among the top vectors for health care breaches alongside phishing.

Supports: 45 CFR 164.312(d) - Person or Entity Authentication; 45 CFR 164.312(a)(1) - Access Control

Admin accounts with standard MFA are still vulnerable to phishing. Phishing-resistant MFA closes that gap.

☐ MFA / Authentication Token Lifetime Set to 24 Hours Maximum

Authentication token lifetime controls how long a user stays signed in before being required to re-authenticate with MFA. This should be set to 24 hours maximum. Industry guidance recommends as short as 3 hours for high-security environments. Think of it this way: the token lifetime is the length of time an attacker has a valid ticket to operate as a person in your organization after a successful phishing attack -- before they would need to phish someone again. The shorter the lifetime, the smaller the window of opportunity. The default in many environments is 90 days, which gives an attacker three months of access from a single successful phish.

Supports: 45 CFR 164.312(a)(2)(iii) - Automatic Logoff; 45 CFR 164.312(d) - Person or Entity Authentication

Default token lifetimes of 90 days give attackers 3 months of access from a single successful phish.

Tier 2 Score: _____ / 8 items in place

These items represent the current standard of care for endpoint security in health care. Most can be implemented using tools already included with Windows, Active Directory, and your cloud platform (Microsoft 365 or Google Workspace).

TIER 3: ADVANCED SECURITY

Mature controls that significantly reduce risk. Organizations should be working toward these.

☐ **Application Whitelisting Implemented**

Application whitelisting (also called application control) restricts which software is allowed to execute on a system to a pre-approved list. Any executable, script, or installer not on the approved list is blocked from running. This is one of the single most effective controls against ransomware, malware, and unauthorized software. Windows includes built-in options: AppLocker (available in Enterprise editions) and Windows Defender Application Control (WDAC). Central management through Group Policy or Configuration Manager is strongly preferred.

Supports: 45 CFR 164.312(a)(1) - Access Control; 45 CFR 164.308(a)(5)(ii)(B) - Protection from Malicious Software

This is considered one of the single most effective defenses against ransomware and malware.

Tier 3 Score: _____ / 1 items in place

Application whitelisting is a significant undertaking that requires careful planning and testing, but the security benefit is substantial. If Tiers 1 and 2 are solid, this is the next highest-impact control to pursue.

QUESTIONS FOR YOUR CLINICAL SYSTEM VENDORS

Medication dispensing cabinets, lab analyzers, imaging systems, infusion pumps, and similar devices.

Medical device and clinical system vendors are frequently the weakest link in a health care organization's security posture. It is surprisingly common for these vendors to require configurations that directly contradict basic security practices -- including disabling Group Policy, requiring local administrator auto-logon, blocking security patches, and running unsupported operating systems. Many of these systems would not pass the Tier 1 (Windows Vista level) section of this checklist.

Ask your clinical system vendors these questions. The answers will tell you a lot:

1. Does your system support running in an Active Directory domain with Group Policy applied?

2. Does your system require local administrator privileges for normal operation or auto-logon?

3. Can your system receive centrally managed operating system patches and security updates?

4. Does your system support current encryption protocols (TLS 1.2 or higher)?

5. Does your system support unique user authentication (no shared/generic local accounts)?

6. Can endpoint protection (anti-virus/anti-malware) run on your system without exclusions that effectively disable it?

Or simply ask: "Can your system on our network be compliant with every item on this checklist?" If the answer is no, you now know exactly where that vendor's system falls short -- and that system needs to be isolated from the rest of your network until those shortcomings are resolved. A clinical system that requires your organization to weaken its security posture in order to function is a clinical system that needs to be on its own isolated network segment.

OVERALL ASSESSMENT SUMMARY

Tier	Items in Place	Total Items	Gaps
Tier 1: Baseline	_____	5	_____
Tier 2: Standard	_____	8	_____
Tier 3: Advanced	_____	1	_____
Total	_____	**14**	_____

Notes / Priority Actions:

_____

_____

_____

_____

_____

_____

HIPAA Compliance Disclaimer

This checklist is provided for educational and self-assessment purposes only and does not constitute legal advice. Each health care organization is ultimately responsible for its own HIPAA compliance program, including documented risk assessments and implementation of required safeguards. The recommendations in this checklist are designed to support your compliance strategy, not replace it. The items listed represent widely recognized security best practices and reference applicable sections of 45 CFR Part 164, but meeting these items alone does not guarantee full HIPAA compliance.

Questions? Contact visuaFUSION Systems Solutions at (308) 708-7490 or visit https://visuaFUSION.com