Secure Endpoint Configuration

Workstation Requirement	Technical Control	Operational Procedures (Local IT Responsibility)	Administrative Procedures (Cybersecurity and unit leadership responsibility)	Policy Reference
System Configuration	Qualys Cloud Agent installed and configured on the device to be a member of the HIPAA Secure endpoint compliance management group.	Remediate all identified gaps until control compliance is met. Develop reports and dashboard(s) demonstrating that all endpoint configuration remains compliant. Develop notification method for critical compliance gaps and remediate immediately. Review reports and dashboard on a monthly basis and remediate all gaps. Email to grc-cybersecurity@cio.wisc.edu when asset no longer accesses restricted data.	Cybersecurity Governance, Risk and Compliance (GRC) monitors and notifies units on Urgent and Critical compliance gaps and escalates to appropriate leadership., Review timeframe to be determined.	UW Madison HIPAA 8.13 System Configuration
System patching & vulnerability management	Qualys Cloud Agent installed and configured to be a member of the HIPAA Secure endpoint compliance management group.	Remediate all identified vulnerabilities according to campus vulnerability remediation timeline. Develop vulnerability reports that are reviewed at minimum, on a monthly basis. Develop notification and remediation procedures to respond and remediate urgent and critical and zero day vulnerabilities (either from established Qualys reports or from CSOC notifications). Review report deltas and remediate remaining identified vulnerabilities.	Cybersecurity Governance, Risk and Compliance (GRC) monitors and notifies units on zero day vulnerabilities and monitors the vulnerability deltas to ensure assets in the HIPAA Secure endpoint compliance management group are being patched. Review timeframe to be determined.	UW Madison HIPAA 8.13 System Configuration; UW Madison HIPAA 8.3 HIPAA Security Auditing; UW Madison IT Electronic Devices Policy; UW Madison IT Vulnerability Scanning Policy
Anti-Virus/Anti-malware	Deploy Cisco's Advance Malware Protection (AMP) to all assets or assets that are used for the handling of ePHI.	Install AMP and enable automatic updates. Enable notification alerts on identified threats. Review AMP reports on a weekly basis.	Cybersecurity Operations Center (CSOC) will review reports looking for anomalies and out-of-compliance assets. Review timeframe to be determined.	UW HIPAA 8.13 System Configuration; UW Madison IT Electronic Devices Policy
Host-based Firewall	Utilize a host-based firewall on all assets used for ePHI.	Deploy a host-based firewall and manage the firewall compliance of assets from a centralized control point. Ensure end-users cannot turn the host based firewall off. Develop notification methods to alert Local IT if the firewall is turned off and to re-enable in a reasonable amount of time.	Local HIPAA Security Coordinator will monitor host based firewall controls as a critical compliance control for all assets in the Secure Endpoint Compliance Policy. Review timeframe to be determined.	UW Madison HIPAA 8.13 System Configuration; UW Madison IT Network Firewall Policy
Administrator access	Remove end User permissions so they are not local admins	Develop access and account provisioning procedures to ensure that administrator access is a separate account, not accessible by the end user and employs MFA.	Local HIPAA Security Coordinator will monitor, administrator access controls as a critical compliance control for all assets in the Secure Endpoint Compliance Policy. Review timeframe to be determined.	UW Madison HIPAA 8.13 System Configuration

Secure Endpoint Configuration

Workstation Requirement	Technical Control	Operational Procedures (Local IT Responsibility)	Administrative Procedures (Cybersecurity and unit leadership responsibility)	Policy Reference
Data at Rest	Data storage locations, if not stored in Box, are encrypted. Laptops and Desktop should use drive encryption.	Develop procedures to ensure asset hard drives used to store restricted data are encrypted. Develop encryption key management procedures. Review Qualys Secure Endpoint Policy compliance reports monitor that encryption is active.	Local HIPAA Security Coordinator will monitor disk drive encryption controls as a critical compliance control for all assets in the Secure Endpoint Compliance Policy. Review timeframe to be determined.	UW Madison HIPAA 8.10 Remote Access; UW Madison HIPAA 8.13 System Configuration; UW Madison IT Storage and Encryption Policy
Data in Transit	Data-in-transit must occur over an encrypted protocol. Deploy WiscVPN to all assets in the HIPAA Secure asset group	Develop procedures to install WiscVPN. Develop end user training on how and when to use WiscVPN to access restricted data via wireless networks and off campus networks.	Local HIPAA Security Coordinator will monitor to ensure WiscVPN is installed and updated as a critical compliance control for all assets in the Secure Endpoint Compliance Policy. Review timeframe to be determined.	UW Madison HIPAA 8.10 Remote Access; UW Madison HIPAA 8.13 System Configuration; UW Madison IT Storage and Encryption Policy
Data Storage on portable media	Use of Portable devices should not be used to store restricted data. If the business use case requires the use portable devices, these devices should have equal or better encryption to laptops and desktops	Develop procedures to request encrypted portable devices as storage locations. Develop procedures to track, sanitize and depose of portable devices. Monitor use of portable devices.	Cybersecurity Governance, Risk and Compliance (GRC) will verify that procedures are in place to manage portable devices as storage locations. Review timeframe to be determined.	UW Madison HIPAA 8.10 Remote Access; UW Madison HIPAA 8.13 System Configuration; UW Madison IT Storage and Encryption Policy

Secure Endpoint Configuration

Workstation Requirement	Technical Control	Operational Procedures (Local IT Responsibility)	Administrative Procedures (Cybersecurity and unit leadership responsibility)	Policy Reference
Data in use	Restricted Data may only be accessed via an approved workstation that has met the requirements.	Develop training procedures that ensures the project folder owner understands and agrees to policy/procedure.	Technical contact or HIPAA Security Coordinator continues to monitor and ensure compliance is being met per the agreed upon approval guidelines. Review timeframe to be determined.	UW Madison HIPAA 8.2 HIPAA Security Oversight; UW Madison HIPAA 8.10 Remote Access; UW Madison HIPAA 8.13 System Configuration; UW Madison IT Restricted Data Security Management Policy; UW System Acceptable Use of Information Technology Resources
Maintenance & Testing of security posture	Monthly reporting of compliance stature for each device accessing Box.	Generate reports and publish for review. (Hipaa coordinator or Local IT Security contact)	Local HIPAA Security Coordinator will review reports for out-of-compliance assets and update/patch assets to ensure they are staying in compliance. Review timeframe to be determined.	UW Madison HIPAA 8.2 HIPAA Security Oversight; UW Madison HIPAA 8.3 HIPAA Security Auditing