SOPHOS

HIPAA Security Standards Compliance Reference Card

The Health Insurance Portability and Accountability Act (HIPAA) provides for the protection of individually identifiable health information that is transmitted or maintained in any form or medium. HIPAA looks to healthcare providers and their business associates to meet administrative, technical and physical safeguards to ensure the integrity and confidentiality of electronic protected health information (ePHI). This document describes how Sophos products can be effective tools to help address some of these administrative and technical safeguards as part of a customer's efforts to comply with HIPAA. All Sophos Central products, Sophos Cloud Optix, SophosLabs, SophosLabs Intellix, Sophos tech support, and Sophos Managed Threat Response carry a 2020 SOC2 Type 1 and HIPAA Type 1 attestation.

Standard	Specification	Sophos product	How it helps
164.308 Administrative Safeguards			
164.308(a)(1)(i) Security Management Process	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls, stopping advanced attacks. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Email on Central Sophos Email Appliance Sophos XG Firewall Sophos SG UTM	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Intercept X Sophos Intercept X Advanced with EDR Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease. Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be. Includes rollback to original files after a ransomware or master boot record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.

Standard	Specification	Sophos product	How it helps
		Sophos XG Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
164.308(a)(1)(ii)(D) Information System Activity Review	Implement procedures to regularly review records of information system activity, such as audit logs, access logs, access reports, and security incident tracking reports.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Intercept X Advanced with EDR	Detect, investigate, and respond to suspicious endpoint activity.
		Sophos XG Firewall	Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
		Sophos SafeGuard Enterprise	Provides detailed logging of all access attempts.
		Sophos Mobile	Creates detailed log events of all malicious activity on mobile devices, helping to identify suspicious activity that may try to access sensitive data.
164.308(a)(3)(i) Workforce security	Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	Sophos XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
		Sophos Central on Email Sophos XG Firewall Sophos SG UTM	Prevents messages containing sensitive data from leaving the organizations with data loss prevention rules providing policy driven encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to help protect email content from unauthorized access.
164.308(a)(3)(ii)(A) Authorization and/or supervision	Ensures the authorization and/or supervision of workforce members who work with ePHI or in locations	Sophos XG Firewall Sophos SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos SafeGuard Enterprise	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).

HIPAA Security Standards Compliance Reference Card

Standard	Specification	Sophos product	How it helps
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
164.308(a)(3)(ii)(C) Termination procedures	Ensure that access to ePHI is terminated as soon as possible when a workforce member's employment ends.	Sophos Central	Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
164.308(a)(5)(i) Security Awareness Training	Implement a security awareness and training program for all members of the workforce (including management). Component of the security awareness and training program should include aecurity reminders, protection from malicious software, log-in monitoring, and password management.	Sophos Training and Certifications	Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
		Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organizations end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to data loss prevention, password protection, and more..
164.308(a)(5)(ii)(B) Protection from malicious software	Implement procedures for guarding against, detecting, and reporting malicious software.	Sophos XG Firewall	Visibility and control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications / software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints. View a full list of controlled software/applications.
		Sophos Mobile	Monitor mobile devices for jailbreaking and side-loading of applications. Deny access to email, network, and other resources if device is not in compliance with policy.
		Sophos Intercept X Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.
164.308(a)(5)(ii)(C) Log-in monitoring	Implement procedures for monitoring log-in attempts and reporting discrepancies.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall	Controls remote access authentication and user monitoring for remote access and logs all access attempts.
		Sophos SafeGuard Enterprise	Provides detailed logging of all access attempts.
		Sophos Mobile	Creates detailed log events of all malicious activity on mobile devices, helping to identify suspicious activity that may try to access sensitive data.

Standard	Specification	Sophos product	How it helps
164.308(a)(6)(i) Security incident procedures	Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls, stopping advanced attacks. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Email on Central Sophos XG Firewall Sophos SG UTM	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Intercept X Sophos Intercept X Advanced with EDR Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease. Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be. Includes rollback to original files after a ransomware or master boot record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
		Sophos XG Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
164.308(a)(6)(ii) Response and reporting	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; document security incident and their outcomes.	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls, stopping advanced attacks. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Email on Central Sophos XG Firewall Sophos SG UTM	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
		Sophos Intercept X Sophos Intercept X Advanced with EDR Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease. Get a root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be. Includes rollback to original files after a ransomware or master boot record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.

Standard	Specification	Sophos product	How it helps
		Sophos XG Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
164.308(a)(7)(ii)(B) Disaster-recovery plan	Establish and implement procedures to restore any loss of data.	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls. The Security Heartbeat also shares this information with Sophos Encryption, which revokes the encryption keys on the affected machine until the problem is fixed to prevent any data theft. After the systems have been automatically returned to their initial, clean state, the XG Firewall restores network access to the device, the encryption keys are returned, and your network is botnet-free.
		Sophos Intercept X Sophos Intercept X for Server	Includes rollback to original files after a ransomware or master boot record attack. Sophos Clean provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
164.312 Technical Safeguards			
164.312(a)(1) Access control	Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.	Sophos XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos SafeGuard Enterprise	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location. Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.
		Sophos Enterprise Console and Sophos Central	Configurable role-based administration provides granular control of administrator privileges.
		Sophos Central	Keeps access lists and user privileges information up to date. Procedures are in place to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).

HIPAA Security Standards Compliance Reference Card

Standard	Specification	Sophos product	How it helps
164.312(a)(2)(i) Unique user identification	Assign a unique name and/or number for identifying and tracking user identity.	Sophos XG Firewall Sophos SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		Synchronized Security feature of Sophos Email and Sophos Phish Threat	Sophos Email 'At Risk Users' report highlights exactly which users are clicking email links re-written by time-of-click URL protection. Identifying users who have either been warned or blocked from visiting a website due to its risk profile. It's then simply one-click from the report to enroll users in Phish Threat simulations and security awareness training – increasing their threat awareness and reducing risk.
164.312(a)(2)(iv) Encryption and decryption	Implement procedures that specify a mechanism to encrypt and decrypt ePHI.	Sophos SafeGuard Encryption Sophos Central Device Encryption	Encrypts data on Macs, Windows, and mobile devices. Device Encryption provides centrally-managed, full disk encryption using Windows BitLocker and Mac FileVault. Sophos application-based (synchronized) encryption is automatic and always on, i.e. content is encrypted as soon as it is created and it stays encrypted even when shared or uploaded to a cloud-based file-sharing system or removable devices. Role-based management is available to separate authorization levels and your encryption policies, keys, and self-service key recovery can be centrally managed.
		Sophos Email on Central Sophos XG Firewall Sophos SG UTM	Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.
		Sophos Mobile	Sophos Secure Workspace secures work documents with AES-256 encryption, allowing a secure way to manage, distribute, and edit business documents and view web content on mobile devices. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps.
		Sophos Wireless Sophos XG Firewall Sophos SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
164.312(b) Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall	Controls remote access authentication and user monitoring for remote access and logs all access attempts.
		Sophos SafeGuard Enterprise	Provides detailed logging of all access attempts.
		Sophos Mobile	Creates detailed log events of all malicious activity on mobile devices, helping to identify suspicious activity that may try to access sensitive data.
		Sophos Endpoint Protection Sophos Intercept X for Server	Creates detailed log events for all malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process PHI and PII.

HIPAA Security Standards Compliance Reference Card

Standard	Specification	Sophos product	How it helps
164.312(c)(1) Integrity	Implement policies and procedures to protect ePHI from improper alteration or destruction.	Sophos SafeGuard Enterprise	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
		Sophos Email Appliance Sophos XG Firewall Sophos SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos XG Firewall Sophos SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos Mobile	Provides enterprise mobility and security management capabilities for traditional and mobile endpoints, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app secures sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.
		Sophos Wireless Sophos XG Firewall Sophos SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
164.312(d) Person or entity authentication	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Sophos XG Firewall Sophos SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos SafeGuard Enterprise	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
		Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.

HIPAA Security Standards Compliance Reference Card

Standard	Specification	Sophos product	How it helps
164.312(e)(1) Transmission security	Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	Sophos Email on Central Sophos XG Firewall Sophos SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
		Sophos SafeGuard Enterprise	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
		Sophos XG Firewall Sophos SG UTM	Allows for policy-based encryption for VPN tunnels, protecting data in transit
164.312(e)(2)(ii) Encryption	Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Sophos Email on Central	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		Sophos Mobile	Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
		Sophos SafeGuard Encryption	Encrypts data on Macs, Windows, and mobile devices. Manages BitLocker and FileVault full disk encryption as well as always-on file encryption stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted remains encrypted as files move across the network.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2020-07-02 CC (PC)

SOPHOS