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. The Security Rule under HIPAA requires covered entities and business associates to meet administrative, technical and physical safeguards to ensure the integrity, confidentiality, and availability 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.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. Use of Sophos products alone does not guarantee legal compliance. The information in this document does not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

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	Synchronized Security is a complete portfolio of world-class Sophos security products that work together, responding automatically to incidents and delivering enhanced security insights. Zero-touch incident response slashes exposure to threats while the integrated product portfolio minimizes security gaps. Enhanced insight into network traffic lets you identify and address hidden risks. Centralized management enables you to focus on priority alerts.
		Sophos Email Sophos Firewall	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 XDR 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 across all devices and platforms. Goes beyond the endpoint, pulling in rich network, email, cloud, and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Managed Detection and Response (MDR)	24/7 threat detection and response identifies and neutralizes advanced cyber attacks that technology alone cannot stop.
		Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

SOPHOS

Standard	Specification	Sophos product	How it helps
		Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/ Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
164.308(a)(1)(ii)(A) Risk Analysis	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Sophos Cloud Optix	Sophos Cloud Optix continuously analyzes public cloud resource configuration settings against HIPAA compliance standards. Identifying issues that could lead to a data breach, such as exposed cloud server ports and shared storage in public mode. Audit-ready reports then enable you to define which inventory items within your public cloud account are subject to certain compliance standards, reducing the hours associated with compliance audits. By automatically mapping security and compliance standards to your environments, Cloud Optix provides on-demand audit-ready reports that detail where organization pass or fail the requirements of each standard, with the option to include remediation steps within the reports themselves.
		Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk level and prioritize response.
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 XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Managed Detection and Response (MDR)	Threat-hunting experts monitor and correlate information system activity across the full IT security environment, identifying and investigating suspicious activities.
		Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
		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 ZTNA	Validates user identity, device health, and compliance before granting access to resources.

Standard	Specification	Sophos product	How it helps
		Synchronized Security feature in Sophos products	Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
		Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		Sophos Wireless	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
		Sophos Email	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
		Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device.
		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).
		Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
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 where it might be accessed.	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas.
		Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		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 ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Email	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.

Standard	Specification	Sophos product	How it helps
		Sophos Cloud Optix	Sophos Cloud Optix, Cloud Security Posture Management solution, connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		Sophos Switch	Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
		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 enables enforcement of device encryption and monitors compliance relative to encryption policy.
164.308(a)(3)(ii)(B) Workforce clearance procedure	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security Posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
		All Sophos Products	Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
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)(4)(ii)(A) Isolating healthcare clearinghouse functions	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Sophos Firewall	Sophos Firewall enables network segmentation by supporting different physical or virtual networks each with separate credentials required to provide access and protect data on these separate networks.
		Sophos ZTNA	Safeguards against attacks that rely on external entity's access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted users, irrespective of the location.
		Sophos Intercept X with XDR	Provides comprehensive defense in depth against threats that get in via external entities using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
164.308(a)(4)(ii)(C) Access Establishment and Modification	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	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).

Standard	Specification	Sophos product	How it helps
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 security 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	Educates and tests end users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics.
164.308(a)(5)(ii)(B) Protection from malicious software	Implement procedures for guarding against, detecting, and reporting malicious software.	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/ Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
		Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
		Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications. Server Lockdown allows only trusted whitelisted applications and associated files to run.
		Sophos Intercept X for Server	Prevents unauthorized applications from running with Server Protection, automatically scanning your system for known good applications, and whitelisting only those applications.
		Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
		Sophos Managed Detection and Response (MDR)	24/7 detection and neutralization of malicious software by human experts, leveraging AI, technologies and threat expertise.
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 XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Firewall	Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
		Sophos Cloud Optix	Cloud Optix enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.

Standard	Specification	Sophos product	How it helps
		Sophos Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
164.308(a)(5)(ii)(D) Password management	Procedures for creating, changing, and safeguarding passwords.	Sophos Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically.
		Sophos Firewall	Allows strong passphrase policy to be applied for admin accounts in terms of complexity, length, password reuse and use of a single dictionary word.
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	Synchronized Security is a complete portfolio of world-class Sophos security products that work together, responding automatically to incidents and delivering enhanced security insights. Zero-touch incident response slashes exposure to threats while the integrated product portfolio minimizes security gaps. Enhanced insight into network traffic lets you identify and address hidden risks. Centralized management enables you to focus on priority alerts.
		Sophos Managed Detection and Response (MDR)	Full incident response service included as standard, providing 24/7 coverage delivered by IR experts. Includes full root cause analysis and reporting.
		Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications. Server Lockdown allows only trusted whitelisted applications and associated files to run.
		Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also identifies and protects users and applications on the network. Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Lateral Movement Protection, a Synchronized Security feature, prevents the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
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	Synchronized Security is a complete portfolio of world-class Sophos security products that work together, responding automatically to incidents and delivering enhanced security insights. Zero-touch incident response slashes exposure to threats while the integrated product portfolio minimizes security gaps. Enhanced insight into network traffic lets you identify and address hidden risks. Centralized management enables you to focus on priority alerts.
		Sophos Email	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.

Standard	Specification	Sophos product	How it helps
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications. Server Lockdown allows only trusted whitelisted applications and associated files to run.
		Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also identifies and protects users and applications on the network. Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Lateral Movement Protection, a Synchronized Security feature, prevents the threat or hacker from spreading to other systems, stealing data, or communicating back to the host.
		Sophos Cloud Optix	Sophos's cloud security posture management solution, Sophos Cloud Optix, enables teams to proactively improve security posture, detecting insecure configurations and vulnerabilities. By automatically mapping security and compliance standards to your environments, Cloud Optix provides the visibility needed to monitor and maintain security posture 24/7.
		Sophos Managed Detection and Response (MDR)	24/7 detection of and response to security incidents across the IT environment, leveraging human expertise, AI, and advanced technologies.
		Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
164.308(a)(7)(ii)(B) Disaster-recovery plan	Establish and implement procedures to restore any loss of data.	Synchronized Security in Sophos products	Sophos products share real-time information via a unique Security Heartbeat™ ™ and then respond automatically to incidents in seconds. It isolates infected endpoints, blocking lateral movement; restricts Wi-Fi for non-compliant mobile devices and infected endpoints; scans endpoints on detection of compromised mailboxes; revokes encryption keys if a threat is detected.
		Sophos Intercept X Sophos Intercept X for Server	Includes rollback to original files after a ransomware or master boot record attack.
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.	All Sophos Products	Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. And includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right- sized IAM policies before they are exploited in cyberattacks.
		Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.

Standard	Specification	Sophos product	How it helps
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
164.312(a)(2)(i) Unique user identification	Assign a unique name and/or number for identifying and tracking user identity.	All Sophos Products	Sophos' user-identity based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
		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 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 Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		Sophos Email	Offers TLS encryption and support for SMTP/S along with full push-base, and optional pull-based portal encryption.
		Sophos Wireless	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 Firewall	Controls remote access authentication and user monitoring for remote access and logs all access attempts.
		Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud, and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		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 Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
		Sophos Intercept X 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.
164.312(c)(1) Integrity	Implement policies and procedures to protect ePHI from improper alteration or destruction.	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		Sophos Email	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.

Standard	Specification	Sophos product	How it helps
		Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		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 Intercept X Sophos Intercept X for Server	HIPS, Deep Learning, Anti-exploit, Anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
		Sophos Wireless	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 Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		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	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management
		Sophos Email	capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection safeguards your users and devices from malicious content and apps.
		Sophos Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.
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	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.

Standard	Specification	Sophos product	How it helps
		Sophos Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. A rich set of device management capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection safeguards your users and devices from malicious content and apps.
		Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
		Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.
164.312(e)(2)(ii) Encryption	Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Sophos Email	Offers TLS encryption and support for SMTP/S along with full push-base, and optional pull-based portal encryption.
		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 Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
		Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.

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

2022-11-23 CC (PC)

SOPHOS