SOPHOS

Understand HIPAA ePHI:

Secure it with evolved cybersecurity solutions from Sophos

HIPAA stands for the Health Insurance Portability and Accountability Act. It was passed by Congress in 1996 to build an efficient and more streamlined healthcare system in the U.S. HIPAA offers federal protection for personal health information, including health information in medical records, conversations regarding medical treatment, as well as electronic billing and other processes related to the patient's health. The HIPAA Security Rule places safeguards to ensure the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI), while the HIPAA Privacy Rule places limits on the use and disclosures of PHI.

Failure to comply with HIPAA regulations invites hefty fines and can be debilitating for the financial and reputational health of a business. And it can all start with a single stolen smartphone, laptop, or USB device leading to HIPAA violation. In 2018, Fresenius Medical Care North America (FMCNA) had five breaches adding up to millions in settlement costs[1]. The organization failed to heed HIPAA's risk analysis and risk management rules. In 2019, Touchstone Medical Imaging, a Tennessee Diagnostic Medical Imaging Services Company, paid $3 million to settle a breach exposing over 300,000 patients' protected health information[2]. The list goes on and on.

Who does HIPAA apply to?

"HIPAA covered entities" include all those who create, receive, store, or transmit PHI on a regular basis, like all health plans, healthcare clearinghouses, and healthcare providers.

The regulation also applies to "business associates," third-party service providers like storage and transmission services, claims processing services, data analysts, or billing and benefit management services, that provide services for or on behalf of covered entities, requiring them to have access to PHI.

A Ponemon Institute research states that data breaches cost the healthcare sector an average of $6.5 million, which is over 60 percent more than all other sectors. Those industries spend about $3.9 million, on average.[3]

Is all PHI sacred and applicable under HIPAA?

Protected health information (PHI) is the information about patients or health plan members. Health information maintained in educational or employment records by an employer, even if the employer is a HIPAA-covered entity, doesn't constitute PHI. Any information is treated as PHI and falls under the HIPAA Privacy Rule's scope only if it can identify an individual. There are 18 identifiers or types of "protected information," including names, phone numbers, email addresses, social security numbers, geographical addresses, driver's license numbers, medical diagnoses, prescribed medications, and medical record numbers, among others. If these details are removed from the information, it is considered de-identified PHI and it is no longer subjected to the privacy rules under HIPAA.

HIPAA PHI Identifiers		
Patient name	Dates (birth, treatment, death)	Physical addresses
Fax numbers	Social security numbers	Certificate/license numbers
Phone numbers	Full face photos/other pictures	URLs/web addresses
Email addresses	Health plan beneficiary information	Internet Protocol (IP) addresses
Medical records	Device identifiers and serials	Biometric (finger, voice, etc.) info
Account numbers	Vehicle identification informations	Other uniquely identifying info

PHI is sellable

PHI can be sold by healthcare organizations for marketing activities or for research, but only with few disclaimers. Prior to disclosure of any health information that is not permitted by the HIPAA Privacy Rule, a written authorization must be obtained from the patient permitting the company or the business associate to use the data. And this health information must be de-identified, in other words, it must be stripped off all information that allow a patient to be identified.

Why is PHI so exciting on the dark web?

Health information doesn't come with an expiration date. The longevity of this information, and precious details that accompany the PHI like the social security numbers and other government-issued documents like the driver's license, can enable fraudsters to wrongly file tax returns or even create false identities. Stolen medical records can be misused to acquire prescription drugs or receive medical care. In the United States, where more than 90% of the population has some form of health insurance, it's no surprise that more than 300 million records have been stolen since 2015. This has affected about one in every 10 healthcare consumers[5].

Value of an electronic medical record can be worth $1,000 to hackers.[4]

Is HIPAA only about healthcare organizations?

HIPAA does not protect all health information. Nor does it apply to every person who may see or use health information. In the same breath, HIPAA does not apply to employers simply because they collect health information of their employees. HIPAA does apply to these employers when they obtain this information from third-party associates who are usually covered entities under HIPAA.

As an employer, if you pay for a portion of the cost for your employees' medical care, you are considered a health plan and HIPAA's Privacy rule and compliance apply to you. Under the Privacy rule, you must protect the sensitive healthcare information at all times. The rule of "minimum necessary" now starts applying to you, which implies that protected health information may be disclosed in cases where the law requires such disclosures, but only to the extent that such disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law. Besides other requirements mandated by HIPAA to a covered employer, the employer must also ensure that the employee/employees handling PHI within the organization receive proper training about HIPAA and are made aware of phishing threats.

HIPAA violations are a very costly affair

A HIPAA violation occurs when the integrity of protected health information is compromised. Unencrypted health records, hacking and ransomware, loss or theft of devices containing PHI, and lack of employee training on how to deal with sensitive health information are some of the many reasons that lead up to HIPAA violations. Both innocent or willful violation of HIPAA rules can result in heavy fines and mandatory structural reorganization.

- A violation attributable to ignorance can attract a fine of $100 – $50,000.
- A violation which occurred despite reasonable vigilance can attract a fine of $1,000 – $50,000.
- A violation due to willful neglect which is corrected within thirty days will attract a fine of between $10,000 and $50,000.
- A violation due to willful neglect which is not corrected within thirty days will attract the maximum fine of $50,000[6].

Penalties can easily reach the maximum fine of $1,500,000 per year, per violation category. Violations can also carry criminal charges that may result in jail time.

Most frequent HIPAA violations

Here are the top HIPAA violations that any employer must be aware of to prevent them from happening in their organizations:

Improper HIPAA Safeguards: There has been no shortage of stories involving millions of dollars in fines as a result of a HIPAA security breach owing to a lost laptop or USB containing unencrypted data. Alternately, this could be the result of the accidental disclosure of medical data of some 150 employees enrolled in a company's wellness program that was sent out to a wrong email address. Ransomware, of late, has emerged as the most potent threat to healthcare data. The young CEO of A1care revealed how his company was almost forced out of business because of a ransomware attack that threatened to expose personal data of its clients if the ransom was not paid[7]. Disappointingly, CSO Online estimates that healthcare-related malware attacks like ransomware will likely quadruple by 2020[8]. The HIPAA Security Rule imposes physical, administrative, and technical safeguards on an organization to defend against HIPAA-related security breaches with innocent or malicious intent and prevent HIPAA violations.

Use and Disclosure: As per the HIPAA Privacy Rule, a covered entity may not use or disclose PHI unless the Privacy Rule permits or requires in specified situations, or the covered entity is authorized in writing by the individual who is the subject of the information. Improper distribution of PHI to an incorrect party results in a Use and Disclosure violation and constitutes a HIPAA settlement and related fine. A clear case of impermissible Uses and Disclosures happened when a staff member of a medical practice discussed HIV testing procedures with a patient in the waiting room, thereby disclosing PHI to several other individuals[9]. Also, computer screens displaying patient information were easily visible to patients. In another case, the New York Presbyterian Hospital paid up $2.2 million to OCR as settlement amount for HIPAA violation when it allowed a TV show to film patients without obtaining prior permission from the patients[10].

The Minimum Necessary Rule: A component of the HIPAA Privacy Rule, the Minimum Necessary Rule, states that employees of covered entities may only access, use, transmit, or otherwise handle the minimum amount of PHI necessary to complete a given task. If a large portion of a patient's medical record is exposed to a data breach because the Minimum Necessary Rule was not followed, this can lead to a violation of the HIPAA Privacy Rule and resultant HIPAA fines. As an example, a patient intake form should not include questions about the patient's salary or financial status unless required for treatment. The information is unnecessary and could damage the patient's privacy. Alternatively, doctors cannot share patient details with doctors who are not participating in the treatment of that patient even when they work for the same hospital.

Access Controls: Access Control is the first Technical Safeguard Standard of the HIPAA Security Rules. It limits the number of staff members at an organization who have access to PHI. Access to PHI should be limited based on the roles and responsibilities of the employee in question. A classic example of the failure to comply with this requirement is the Anthem HIPAA breach in 2015. Anthem, America's second-largest health insurer, suffered a colossal data breach when cybercriminals gained access to its systems and records of 78.8 million plan members. Anthem agreed to pay OCR $16 million and another $115 million to settle a class action lawsuit filed on behalf of 19.1 million customers whose sensitive information was stolen. Anthem also agreed to implement additional security controls to ensure sensitive information is better protected in the future, including the use of encryption for data at rest and enhancements to its data security procedures[11].

Many of the HIPAA data breaches on the HHS Wall of Shame are a direct result of the provider giving full access to unencrypted data to a vendor or employee, relying on them to secure it properly, and then being liable when that didn't happen[12].

Ransomware and HIPAA

Healthcare data is a goldmine for cybercriminals that comes with a very impressive selling price. A ransomware attack on healthcare data unlocks its worth almost instantaneously. Losing access to real-time patient data even for a short time can be life-threatening and the cybercriminals understand this well. If there's one industry likely to be held hostage with hijacked PHI, it's healthcare.

Ransomware attacks accounted for over 70% of all malware incidents in the healthcare sector as per the 2019 Verizon Breach Investigations Report[13].

With ransomware becoming a serious menace for the healthcare industry, the Department of Health and Human Services has released new guidance[14] on ransomware attacks that states: *Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination. A breach under the HIPAA Rules is defined as, "…the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."*

When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.

Stop ransomware with Sophos cybersecurity

The always-evolving threat protection capabilities by Sophos keep organizations secure against ransomware and other critical advanced threats. Sophos Intercept X with XDR gives you advanced protection technologies that disrupt the whole attack chain. Deep learning predictively prevents attacks, while CryptoGuard rolls back the unauthorized encryption of files in seconds. Available for endpoints, mobile devices, and servers, it stops both local and remote file encryption, returning data to its original state. Sophos XG Firewall is packed with protection technologies to keep ransomware off your network. Plus, the elegant, intuitive interface makes it easy to lock down your remote desktop protocol, protecting against targeted ransomware.

Intercept X and Sophos Firewall are great on their own, but even better together with Synchronized Security. If anything triggers a detection in either product, Sophos Firewall and Intercept X work together to automatically isolate the affected devices – preventing the threat from spreading further.

The Sophos Managed Threat Response (MTR) service reinforces the fight against advanced attacks with a dedicated, round-the-clock team of threat hunters and response experts who constantly scan for and act on suspicious activity.

Phishing emails are the most common way that ransomware and other targeted attacks enter your organization. Sophos Phish Threat provides phishing simulation emails and online tutorials to train users on how to spot and stop phishing emails.

Sophos protects ePHI and helps you stay HIPAA compliant

Sophos' unique IT security capabilities offer award-winning protection for organizations to best ensure coordinated and uninterrupted protection across servers, endpoints, and firewalls and stop advanced attacks; preserve, protect, and provide secure access to the electronic health records; and achieve compliance with the very stringent HIPAA regulations.

Because of easy data mobility and convenient tools and communication apps, sensitive information – including the ePHI – has today moved to employees' personal devices. Sophos facilitates training and awareness among your user groups dealing with sensitive ePHI about phishing and socially engineered attacks.

Theft or accidental loss of mobile devices

Countless laptops are misplaced, stolen, or lost, and many of them contain sensitive data like the PHI. As a part of compliance, organizations need to provide proof that the missing device was encrypted. Full-disk encryption is the first line of defense in such scenarios. Sophos Encryption automatically encrypts content as it is created, and the content stays encrypted even when it's shared or uploaded to a cloud-based, file-sharing system. Sophos Synchronized Security continuously validates the user, application, and device integrity. If your data ever ends up in the wrong hands, Sophos Encryption renders the information unusable. The files remain encrypted and unreadable.

Sophos Encryption seamlessly integrates with Intercept X for Mobile to keep your files secure across Windows, Android, and iOS platforms.It lets you centrally manage Windows BitLocker and macOS FileVault native device encryption. It offers a three-click policy setup, no-key management servers to install, and compliance and reporting features. Over-the-air deployment means it only takes a couple of clicks to push out the new encryption policy and secure data on your remote laptops.

Workforce mobility

Sophos Mobile enables you to enforce security policies in scenarios where employees are viewing sensitive information in their home networks. The strong authentication and access control technologies Sophos provides enable organizations like yours to allow access of ePHI to only those persons who have been granted the access rights.

Data security in public cloud

Sophos solutions keep your cloud-based workloads in AWS, Azure, and GCP public cloud environments secure. Sophos Cloud Optix continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.

Take a look at how Sophos comprehensively supports your HIPAA compliance efforts:

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 Threat Response	A team of threat hunters and response experts provide 24/7 monitoring, detection, and response capabilities delivered as a fully-managed service. They proactively hunt for and validate potential threats and incidents—and stop them before they can cause harm.
		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	Cloud Optix ensures security teams are able to focus on and fix their most critical public cloud security vulnerabilities before they are identified and exploited in cyberattacks. By identifying and risk-profiling security, compliance, and cloud spend risks, Cloud Optix ensures teams respond faster, providing contextual alerts that group affected resources with detailed remediation steps.
		Sophos 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 Sandboxing inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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.
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 Threat Response	Proactively hunt threats 24x7 and neutralize even the most sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
		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.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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 Zero Trust Network Access	Validates user identity, device health, and compliance before granting access to resources.
		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.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos RED (remote ethernet device) extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		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 Zero Trust Network Access	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.
		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)(B) Workforce clearance procedure	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate	Sophos Zero Trust Network Access	Validates user identity, device health, and compliance before granting access to resources.
		Sophos Central Device Encryption	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 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.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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.
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).
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.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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 Threat Response	Incorporates vulnerability intelligence to provide customers with proactive security posture improvements.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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 Intercept X Advanced with XDR	Detect, investigate, and respond to suspicious endpoint activity.
		Sophos Firewall	Controls remote access authentication and user monitoring for remote access, and logs 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)(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.

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	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 Threat Response	Proactively hunt threats 24x7 and neutralize even the most sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
		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	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 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.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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.
		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 Threat Response	Proactively hunt threats 24x7 and neutralize even the most sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
		Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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.
		Zero Trust Network Access	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		Sophos Central Device Encryption	Authenticates users for access to specific files/folders with the use of user- or group-specific keys.
		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.

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.	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 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.

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 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.
		Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos RED (remote ethernet device) extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos Zero Trust Network Access	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 Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.

STANDARD	SPECIFICATION	SOPHOS PRODUCT	HOW IT HELPS
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 Zero Trust Network Access	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 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 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 Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.

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	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. 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 Zero Trust Network Access	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.

1. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/fmcna/index.html
2. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/tmi/index.html
3. https://healthitsecurity.com/news/data-breaches-cost-healthcare-6.5m-or-429-per-patient-record
4. https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#2c9bf8a950cf
5. https://www.healthcarefinancenews.com/news/healthcare-data-breaches-will-cost-industry-4-billion-years-end-and-2020-poised-be-worse
6. https://www.hipaajournal.com/hipaa-violation-cases/
7. https://www.itprotoday.com/data-security-and-encryption/ransomware-attack-victim-once-bitten-twice-shy
8. https://www.csoonline.com/article/3237674/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html
9. https://www.hhs.gov/civil-rights/for-providers/compliance-enforcement/examples/aids/cases/index.html
10. https://www.hipaajournal.com/new-york-hospital-fined-2-2-million-for-unauthorized-filming-of-patients-3402/
11. https://www.hipaajournal.com/16-million-anthem-hipaa-breach-settlement-takes-ocr-hipaa-penalties-past-100-million-mark/
12. https://virgilsecurity.com/hipaa-data-breaches/
13. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
14. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

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

22-03-07 HIPPA WP (MP)

SOPHOS