SOLUTION BRIEF

HIPAA Compliance Reports

Simplify HIPAA Compliance With Arctic Wolf SOC-as-a-Service

Arctic Wolf SOC-as-a-Service

- Continuous vulnerability assessment, and managed threat detection and response
- Dedicated security experts on your IT team
- 24x7 monitoring with unlimited log sources

Benefits

- Simplifies HIPAA compliance with customized reporting
- Monitors access to electronic patient health information (ePHI) data on-premises and in the cloud
- Provides real-time alerts of unauthorized access to systems, processes, and devices that could expose ePHI data

Today, medical professionals access electronic patient health information (ePHI) from anywhere via laptop, tablets, or smartphones. Physicians and healthcare insurers monitor biometric data through wearable devices worn by patients in remote sites. As all this happens, hackers spare no effort in stealing ePHI data for financial gain.

The U.S. Department of Health and Human Services (www.hhs.gov) created the Health Insurance Portability and Accountability Act (HIPAA) in 1996 to protect the confidentiality and integrity of ePHI data. The Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009, imposed mandatory audits and fines for non-compliance.

Security is a crucial part of Administrative Simplification rules under Title II of HIPAA, which aim to protect the confidentiality, integrity, and availability of electronic protected health information. The Department states, "[It] is important to recognize that security is not a one time project, but rather an ongoing, dynamic process." HIPAA therefore requires security-related processes, many of which are often better implemented with technology services. HIPAA regulations do not mandate particular security technologies. Instead, they specify a set of principles for guiding technology choices – principles that are foundational to the Arctic Wolf security operations center (SOC)-as-a-service.

Arctic Wolf's SOC-as-a-service enables all organizations, such as nursing homes and hospitals, to meet HIPAA compliance requirements through Arctic Wolf™ Managed Risk, and Arctic Wolf™ Managed Detection and Response solutions. Arctic Wolf simplifies compliance reporting by customizing it to meet your business needs with the help of our dedicated Concierge Security™ Team of engineers.

Arctic Wolf Meets HIPAA Compliance Rules

The Arctic Wolf Managed Detection and Response and Managed Risk solutions provide real-time threat monitoring and response, vulnerability management, and policy compliance to meet the key security technology auditing requirements detailed in the Department's "Health Insurance Reform: Security Standards," Final Rule 45 CFR Part 164.308. Arctic Wolf fulfills key Administrative Safeguards for evaluation, security management, security incident procedures, training, and security assurance requirements of business associate contracts.

> Arctic Wolf removes a big security burden for our organization. Locating, training, and retaining security personnel would be a major challenge for us, so Arctic Wolf's Concierge Security Team is invaluable in helping us improve our security posture and meet HIPAA compliance obligations.
>
> — Rhett Jackson, Executive Director of Facilities and Information Systems, Madison Memorial Hospital

MADISON MEMORIAL HOSPITAL

HIPAA Compliance Requirements

Electronic patient health information (ePHI) and electronic medical records can be stored in a variety repositories, such as file servers, databases, access logs, and other types of unstructured and structured data repositories. Safeguarding access and transmission of ePHI data in a manner compliant with HIPAA requires diligent administration and close cooperation between the IT teams and the many business units that need access to the data.

Finding the right balance between the tasks that your IT organization can support and the checks automated through Arctic Wolf's SOC-as-a-service enables you to streamline HIPAA compliance and reduce costs.

The primary requirements of HIPAA are:

Section	Requirement
Sec. 164.308(a)(1)	Security Management Process
Sec. 164.308(a)(3)	Workforce Security
Sec. 164.308(a)(4)	Information Access Management
Sec. 164.308(a)(5)	Log-in Monitoring and Password Management
Sec. 164.308(a)(6)	Security Incident Procedures
Sec. 164.308(a)(7)	Disaster Recovery Plan
Sec. 164.310(c)	Workstation Security
Sec. 164.312(a)(1)	Access Control
Sec. 164.312(b)	Audit Control
Sec. 164.316(b)	Standard Documentation Requirements

For more information on HIPAA, go to the US Department of Health and Human Services website.

Arctic Wolf Compliance Solution for HIPAA

Arctic Wolf 's SOC-as-a-service monitors all activity in on-premises IT infrastructure and in cloud applications using physical/virtual sensors and scanners. Arctic Wolf's SOC-as-a-service continuously monitors network flows, ingests log records from unlimited number of log sources, and uses human-augmented machine learning to accurately detect and respond to advanced attacks and uncover potential vulnerabilities.

An Arctic Wolf Concierge Security Team (CST) is dedicated to each customer account. Your CST augments your IT-staff with security expertise, hunts down advanced zero-day attacks and vulnerabilities, identifies HIPAA violations, and provides customized compliance reports to meet your HIPAA requirements. The table on the next two pages shows how the Arctic Wolf SOC-as-a-service enables you to address each of the eight HIPAA requirements.

Arctic Wolf Compliance Solution for HIPAA

Requirement	Arctic Wolf Solution
Sec. 164.308(a)(1): Security Management Process	
Implement policies and procedures to prevent, detect, contain, and correct security violations.	**Arctic Wolf monitors end user and administrative access and configuration changes to all systems that create, receive, maintain, and transmit ePHI data, which enables development/enhancement of the required policies and procedures. Arctic Wolf Managed Risk continuously scans your internal and external networks and devices for vulnerabilities, enabling you to take proactive intervention on identified risks.**
Sec. 164.308(a)(3): Workforce Security	
Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI and prevent people who do not have access to ePHI.	**Arctic Wolf monitors activities of active and in-active user accounts, escalates de-provisioning of in-active accounts through manual/automated means, which enables development/ enhancement of the required policies and procedures.**
Sec. 164.308(a)(4): Information Access Management	
Implement policies and procedures for authorizing access to ePHI data that are consistent with the applicable requirements.	**Arctic Wolf audits changes in Active Directory (AD), Group Policies, Exchange, and file servers, and flags unauthorized actions, which enables development/ enhancement of the required policies and procedures.**
Sec. 164.308(a)(5): Log-In Monitoring and Password Management	
Procedures for monitoring log-in attempts, reporting discrepancies, and monitoring password changes.	**Arctic Wolf monitors failed/successful logins/logoffs and all password changes to prevent excessive help desk calls.**
Sec. 164.308(a)(6): Security Incident Procedures	
Implement policies and procedures to address security incidents.	**Arctic Wolf investigates all attack vectors (e.g. phishing, ransomware, etc.), and generates security incidents to initiate response actions, which enables development/enhancement of the required policies and procedures.**
Sec. 164.308(a)(7): Disaster Recovery Plan	
Establish policies and procedures for responding to an emergency or other occurrence.	**Arctic Wolf audits anomalous login activity, and changes, including before/ after values for immediate data recovery. This promotes quick rollback of unauthorized and accidental changes to Active Directory and other systems.**

Arctic Wolf Compliance Solution for HIPAA (Continued) >

Arctic Wolf Compliance Solution for HIPAA (Continued)

Sec. 164.310(c): Workstation Security	
Implement physical safeguards for all workstations that access ePHI data to restrict access to authorized users.	**Arctic Wolf scans endpoints for unpatched vulnerabilities, and collects log information from endpoint security solutions when unauthorized access or advanced malware is detected. The Arctic Wolf™ Agent is deployed on Windows and Mac workstations to provide additional safeguards to physical devices.**
Sec. 164.312(a)(1): Access Control	
Implement technical policies and procedures for electronic information systems that maintain ePHI data to allow access only to those persons or software programs authorized to have it.	**Arctic Wolf collects relevant data from access control systems and Active Directory, monitoring endpoint activity, and file access. It escalates unauthorized access via security incidents to the Concierge Security Team.**
Sec. 164.312(b): Audit Control	
Implement hardware, software, and/or procedural mechanisms that record and examine activity in endpoints that contain ePHI data.	**The Arctic Wolf Concierge Security Team monitors and reports user logins/logouts in Active Directory, all user activity on endpoints, and continuously monitors network traffic to detect anomalous activity.**
Sec. 164.316(b): Standard Documentation Requirements	
Maintain policies and procedures implemented to comply with documentation requirements.	**Arctic Wolf provides reports for account creations and deletions, data retention policies, admin lockouts, configuration changes, and about who, what, where, and when these changes were made.**

About Arctic Wolf

Arctic Wolf Networks delivers the industry-leading security operations center (SOC)-as-a-service that redefines the economics of cybersecurity. The Arctic Wolf Managed Detection and Response and Managed Risk services are anchored by the Arctic Wolf Concierge Security Team who provide custom threat hunting, alerting, and reporting. Arctic Wolf's purpose-built, cloud-based SOC-as-a-service offers 24×7 monitoring, risk management, threat detection, and response. For more information about Arctic Wolf, visit arcticwolf.com.

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com