snare
A PROPHECY SOLUTION

Regulatory Compliance: HIPAA

Healthcare Industry

Data Security Standard:
Health Insurance Portability and Accountability Act (HIPAA)

Copyright 2023 Prophecy International

How Snare Helps with HIPAA

In this white paper, we will discuss how Snare can help businesses comply with the Health Insurance Portability and Accountability Act (HIPAA).

In order to be compliant with HIPAA requirements, certain system logging practices need to be implemented in order to monitor the security and privacy of protected health information (PHI). Failure to provide an infrastructure designed to prevent and detect unauthorized activity can result in significant fines from the regulators in the event of a data breach. Although the security controls required to adequately protect PHI data are diverse and wide ranging, this paper will concentrate on logging and detection.

Implementing and maintaining appropriate HIPAA security controls can significantly reduce any potential liability associated with data breaches. HIPAA includes four penalty categories:

- **Category 1:** A violation that the organization was unaware of and could not have realistically avoided. A reasonable amount of care was taken to comply with HIPAA requirements.
- **Category 2:** A violation of HIPAA that the organization should have been aware of, but could not have avoided even with a reasonable amount of care.
- **Category 3:** A violation directly due to "willful neglect" of HIPAA rules, in cases where an attempt has been made to correct the violation.
- **Category 4:** A violation of HIPAA rules constituting willful neglect, where no attempt has been made to correct the violation within 30 days.

Penalty Category	**Minimum Penalty per Violation**	**Max Penalty per Violation**	**Maximum Penalty Per Year (cap)**	**Annual Penalty Limit (2022)**
1	Lack of Knowledge	$127	$63,973	$30,487
2	Reasonable Cause	$1,280	$63,973	$121,946
3	Willful Neglect	$12,794	$63,973	$304,865
4	Willful Neglect not Corrected within 30 days	$63,973	$1,919,173	$1,919,173

Reference https://www.hipaanswers.com/hipaa-violation-penalties/ - Figures will be adjusted for inflation

GDPR Penalties for the European Union (EU)

The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.
https://gdpr.eu/fines/

Australian PII laws and penalties are not as prescriptive as GDPR at the time of writing this white paper, but government reviews are assessing the opportunities to strengthen the protection of personal information. https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 will increase maximum penalties that can be applied under the *Privacy Act 1988* for serious or repeated privacy breaches from the current $2.22 million penalty to whichever is the greater of:

- $50 million;
- three times the value of any benefit obtained through the misuse of information; or
- 30 per cent of a company's adjusted turnover in the relevant period.

https://ministers.ag.gov.au/media-centre/parliament-approves-governments-privacy-penalty-bill-28-11-2022

HIPAA Logging and Compliance

In general terms, in order to comply with HIPAA, the following audit and logging related items should be addressed:

- **Identify the events that need to be logged.** Not all events are created equal, and not all events need to be logged. HIPAA requires that you log certain events, such as access to protected health information (PHI), but you may also want to log other events, such as system changes or security incidents.
- **Log the events in a secure manner.** The logs should be stored in a secure location and should be accessible only to authorized personnel.
- **Retain the logs for the required period of time.** HIPAA generally recommends that you retain logs for at least six years.
- **Review the logs on a regular basis.** You should review the logs on a regular basis to look for any suspicious activity.
- **Take action to address any security issues that are identified.** If you identify any security issues, you should take action to address them as soon as possible.

More specifically, Snare can assist in achieving HIPAA security goals in the following areas:

Audit Logs

Maintain comprehensive audit logs of all system activities, including access attempts, modifications, and deletions of PHI. These logs should capture details such as user identities, timestamps, and the specific actions performed.

- Snare Agents help facilitate this by collecting the system access attempts to PHI data by using a number of methods:
  - using system auditing policies to collect who logged into systems
  - using FIM and FAM - File Integrity Monitoring and File Access Monitoring to track who is accessing system files containing PHI data and what tools they are using, ie: MS Word, Notepad, Excel etc
  - where the information is in a database such as MS SQL then the Snare MS SQL agent can provide Database Activity Monitoring to track SQL queries such as select, insert, update and delete statements. Other databases such as Oracle can also be tracked from the relevant windows event logs or Unix audit log files which the Snare Agents can collect.
  - once the data has been collected and sent to Snare Central (and other SIEM technologies) a number of the out of the box reports for system and database activity can be applied. Snare also provides a number of customized reports for specific database to track user activity.

User Authentication and Authorization Logs

Track user authentication events, including: successful and failed login attempts, password changes, and user role or permission modifications. Authorization logs should record the grant or revocation of access privileges to systems and PHI.

- Snare Agents have out of the box policies that will collect most user authentication and authorization events from a system. All login, logoff, failed logins, password changes, user role changes, group and system permission changes are tracked by default on both Windows, Linux, MacOS and Solaris platforms. Database Activity can also be tracked for specific databases and system tables that contain sensitive data.
- Snare Central has many out of the box reports to help track and report on users activity for systems. Report templates are available for:
  - Administrative activity
  - File and Resource Activity
  - Login Activity
  - Process Monitoring
  - Windows Incident Detection
- There is also an event search where a customer can create their own advanced search to look for specific log activity for users, or systems.
- Snare Central can also raise real time alerts based on threshold settings for specific activities. These can be sent via email and SNMP traps.

System and Application Logs

Capture logs from various systems and applications, including operating systems, databases, firewalls, intrusion detection systems (IDS), and other security-related tools. These logs should include information about system events, errors, warnings, and security-related incidents.

- Snare Agents can collect text log files from logs generates by applications and services. The agent collects events in near real time and can send to Snare Central and other SIEM technologies.
- Snare Central can collect syslogs from almost any syslog device, including mainstream firewalls, routers, switches, wireless APs, Network IDS, IPS systems and other network appliances. Many other appliances and applications that send syslog data, can also integrate with the Snare Central server, including malware discovery and anti-virus tools. Snare Central has many out of the box reports for common devices, and more reports are being added on a regular basis.
- As mentioned above databases can be tracked using Database Activity Monitoring using our MS SQL agent, to track application and user activity. In general applications that have good role based access and logging controls dont need to be monitored directly but users that have direct ODBC access or administrative access can override technical controls and their login pose the most risk and should be monitored. Our Snare MSSQL agent can be finely tuned to just collect the logs from the specific users that need to be monitored and remove the noise from other system and user accounts.

Network Traffic Logs

Monitor and log network traffic to identify any suspicious or unauthorized activities, such as attempts to access PHI from unauthorized sources or large data transfers. Network logs should include source and destination IP addresses, port numbers, protocols, and packet information.

- By using the Snare Central Server customers can profile network traffic flow, and monitor specific events, by reviewing the firewall and other networking logs.
- The system also has a 2d/3d view of real time traffic flows that helps provide a visual of traffic flows and if this is expected or not. Other reports can help zoom in on specific application ports, protocols and if traffic is being allowed and denied based on the firewall rules in place.

Encryption and Decryption Logs

Maintain logs that document the encryption and decryption processes for PHI, including the algorithms, key management, and certificate information. These logs can help demonstrate compliance with encryption requirements.

- Snare Agents can collect system and application log content that detail the encryption and decryption process for PHI data.
- Snare Agents collect other tangential application logs that will help with ongoing compliance and review activities as part of the cyber hygiene processes.

Incident Response Logs

Document all security incidents and their corresponding response activities, such as investigating and mitigating breaches, containing incidents, and notifying affected parties. Incident response logs should include details of the incident, the actions taken, and the individuals involved.

- Using Snare Agents and Snare Central helps a customer with their Incident Response Activities by collecting the needed logs and forensics to support incident investigation. The actual ticketing process can be in the system of the customers choosing, but the ability to collect, store and then provide regular reporting coupled with the opportunity to perform ad hoc searches and forensic analysis facilitates the investigation and analysis of incidents.

Retention and Backup Logs

Log information about data retention and backup processes, including schedules, locations, and success/failure notifications. This helps ensure that PHI is properly protected and can be recovered in case of data loss or system failure.

- By focusing on optimising the storage of log data, Snare Central can store many years of events. Access to detailed forensic history can be critical in successfully tracing the extent and threat of any incident investigation. The Snare Agents make it easy to collect and send the information in near real time, and Snare Centrals' ability to collect virtually any syslog source makes it an ideal platform to keep the logs safe and away from the systems that generated the data. The logs collected by Snare Central can be backed up to other devices such as NAS, USB media as well as archive to ISO images for DVDs if required for any forensic investigation.

Log Monitoring and Analysis

Implement a log monitoring and analysis system to review logs regularly for any anomalies, security events, or policy violations. This can involve using security information and event management (SIEM) tools or dedicated log analysis solutions.

- Using Snare Agents to collect audit log data, combined with Snare Centrals' ability to collect syslog feeds from network appliances, all helps with the process of collecting, monitoring, and reviewing logs. Snare Central has over 650 out of the box reports to help facilitate log analysis and perform these log reviews interactively, or on a scheduled basis. The system provides the capability to dynamically clone, and modify, existing reports - in order to leverage existing expert configuration and analysis and deploy to related incidents.
- Real time notifications can be used to highlight high priority policy violations. Snare Central can multiplex event data to one or more third party SIEM, or SOC monitoring tools, to take advantage of individual product strengths, to support legacy applications, or to facilitate the forwarding of a limited view of high-priority events in situations where the third party tool is expensive to run.

Log Integrity and Protection

Implement measures to ensure the integrity and protection of logs, including access controls, encryption, backup, and regular testing. Unauthorized access, modification, or deletion of logs should be prevented.

- Snare Agents can include cryptographic checksums and event sequence numbers on a per-event basis to support authenticity, and non-repudiation.
- Snare Central also includes its own file integrity checks of event logs. A cryptographic checksum is used to highlight potential changes to operating system files, and stored event logs. Any errors or changes will be reported via the integrated Health Checker.
- Snare Central uses an append-only mechanism for log data. From a query engine perspective, files are designated as immutable, and file modifications or removals are not supported by the data storage engine. Snare Central has full role based access controls for the system

Log Retention Period

Determine an appropriate log retention period based on HIPAA requirements and organizational policies. Logs should be retained for a specified duration to support incident investigation, compliance audits, and legal requirements.

- Snare Central helps provide the centralized log storage for long term retention of log data. With 40-50:1 data compression Snare Central can store vast amounts of data in less space than most other vendors - ie: 1TB of Snare Central data can be 40-50 TB or raw data. While HIPAA does not specifically have a retention period defined its generally accepted to keep the data for 6 years or more for statutory requirements and legal needs. Some customers keep their data for 7 years or more depending on their record retention requirements. As Snare Central Server does not have any software or license limits associated with either data storage or per-second collection, it can make it easier for a customer to store whats needed rather than artificially limit collection, which may result in security blind spots in the network. The customer only needs to be concerned with how much disk and system capacity they will need to provide to keep the needed log data.

We have a number of other Snare-related reporting and compliance documents that can help with logging, compliance, and threat management strategies. White papers and reference material can be found here:

- https://www.snaresolutions.com/portfolio-item/complying-with-iso-27001/
- https://www.snaresolutions.com/portfolio-item/how-snare-makes-fim-easier/
- https://www.snaresolutions.com/portfolio-item/mitre-attack/
- https://www.snaresolutions.com/portfolio-item/nist-zero-trust/
- https://www.snaresolutions.com/portfolio-item/xdr-sysmon/
- https://www.snaresolutions.com/database-activity-monitoring/

Remember that HIPAA compliance extends beyond system logging, and additional security and privacy measures are necessary. It is recommended that legal and cybersecurity professionals be consulted to ensure comprehensive compliance with HIPAA regulations.

HIPAA does not specify a specific retention period for logs. However, it is generally recommended to retain logs for **a minimum of six years** as part of HIPAA compliance. This duration aligns with the typical statute of limitations for potential legal actions related to privacy and security breaches.

The retention period should consider various factors, including legal and regulatory requirements, organizational policies, industry best practices, and the specific needs of your organization. **Some organizations may choose to retain logs for longer periods to meet their internal needs, such as incident investigation, auditing, or forensic analysis.**

It is crucial to consult with legal professionals, compliance officers, or industry experts to determine the appropriate log retention period for your specific circumstances. Additionally, consider other applicable laws or regulations that may have specific requirements regarding log retention, as they may impact your decision.

When it comes to understanding the logging requirements for HIPAA compliance, it is essential to refer to the official sources, such as the HIPAA regulations and guidance provided by the U.S. Department of Health and Human Services (HHS). Here are some key references that can help you gain more detailed insights into HIPAA logging requirements:

1. HIPAA Security Rule: The Security Rule establishes the standards for protecting electronic PHI (ePHI) and provides guidance on implementing the necessary safeguards. Specifically, *164.308(a)(5)* addresses the need for implementing procedures to regularly review records of information system activity.
2. HIPAA Privacy Rule: The Privacy Rule addresses the use and disclosure of PHI and establishes the standards for individual privacy rights. Although it does not explicitly mention logging requirements, it emphasizes the need to protect and track the use of PHI.
3. HHS Guidance on HIPAA Security Rule: The HHS provides extensive guidance documents on various aspects of the HIPAA Security Rule. One such document is the "Security Series" available on the HHS website, which provides insights into implementing the security standards, including logging and audit controls.
4. HHS Guidance on Risk Analysis: Conducting a risk analysis is a crucial component of HIPAA compliance. The HHS provides guidance on performing risk assessments, which can help you identify the logging needs based on your organization's risk profile.
5. NIST Special Publication 800-66: This publication, titled "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," provides an overview of the HIPAA Security Rule requirements, including recommendations for implementing audit controls and reviewing logs.
6. NIST Special Publication 800-92: This publication, titled "Guide to Computer Security Log Management," offers guidance on establishing and managing log systems, including log collection, storage, analysis, and protection. It provides general best practices that can be applied to meet HIPAA logging requirements.

Remember to regularly check the HHS website for any updates, as HIPAA regulations and guidance may evolve over time. Additionally, consulting with legal and compliance experts can provide further clarification and guidance specific to your organization's needs

- HIPAA Security Rule:
    - URL: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
- HIPAA Privacy Rule:
    - URL: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- HHS Guidance on HIPAA Security Rule:
    - URL: https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- HHS Guidance on Risk Analysis:
    - URL: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
- NIST Special Publication 800-66:
    - URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
- NIST Special Publication 800-92:
    - URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Please note that URLs may change over time, so it's a good idea to verify the accuracy and accessibility of these resources through the respective websites of HHS and NIST (National Institute of Standards and Technology).

Authored By:

Steve Challans
Chief Information Security Officer (CISO)
Prophecy International

Snare Solutions https://www.snaresolutions.com