Your Roadmap to 2025 HIPAA Compliance with Gigamon

A Guide to Compliance

Executive Overview

The United States Department of Health and Human Services (HHS) reports that healthcare cybersecurity challenges are escalating, with breaches costing $10.1M on average and 92 percent of organizations experiencing an attack annually. According to the Federal Register 45 CFR Parts 160 and 164 RIN 0945-AA22, between 2018 and 2023, the industry has faced:

- **100 percent** increase in unsecured protected health information (PHI) being breached
- **950 percent** increase in individuals affected
- **260 percent** increase in cyberattacks
- **264 percent** increase in ransomware
- **125 percent** increase in cyber-attacks from 2015 to 2019 with a **128 percent** increase from 2022 to 2023 highlighting the speed in escalation

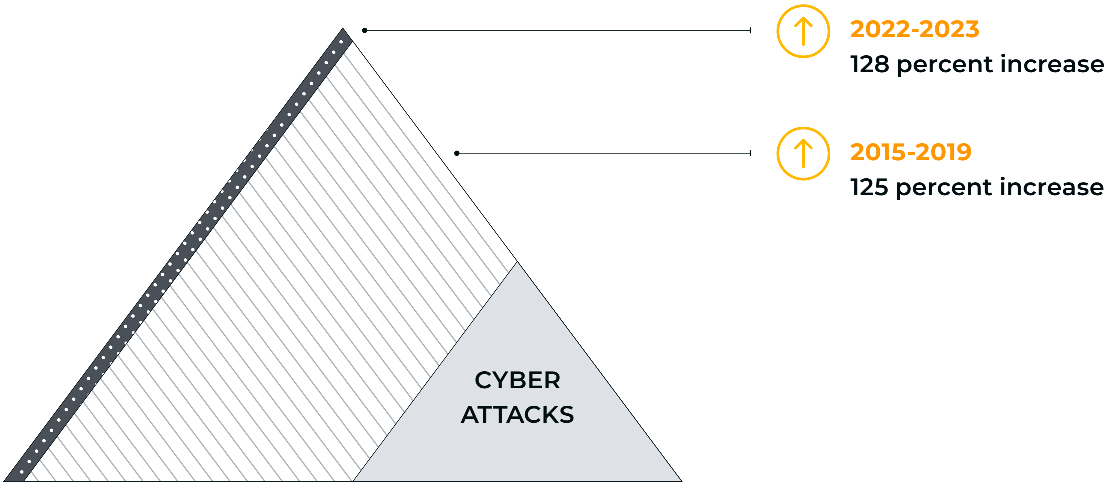
HHS is seeking to mitigate exposure to breaches with a major update to the Health Insurance Portability and Accountability Act (HIPAA). The department found that regulated entities investments in cybersecurity resources often fall short and leave them exposed to cyberthreats. Evidence suggests that senior management often lacks adequate awareness of cybersecurity, including both threats and methods for securing their entities from threats. Why would they? They are in the healthcare business, not the cybersecurity business.

Patient care and outcomes are measurably reduced during such events. Studies have found that cyberattacks can have a substantial effect on access to healthcare and potentially mortality. Nearly three-quarters of organizations that responded to the HHS survey experienced negative effects on everything from patient care to longer hospital stays to increased complications.

This document is a guide on how to help you achieve and maintain HIPAA compliance with an asset that exists in every organization—the network. Taking advantage of network visibility and network-derived intelligence and telemetry will expedite achieving specific HIPAA goals and lower the associated costs.

New 2025 HIPAA regulations expand the requirements in several key areas, including more robust identity management, asset inventory, and ensuring optimal performance of medical equipment on the network.

This paper outlines which aspects of the updated HIPAA requirements Gigamon can help with and how it can assist with the new reporting aspects of compliance.



This chart is a quick at-a-glance HIPAA expansion along with which controls Gigamon network-derived telemetry can assist:

Sections	Standard	Implementation specifications	HIPAA expansion	Gigamon can help
164.308(a)(1)	Technology Asset Inventory	Inventory	●	●
		Network Map	●	●
		Maintenance	●	●
164.308(a)(2)	Risk Analysis	Assessment		●
		Maintenance	●	●
164.308(a)(3)	Evaluation	Performance		●
		Response	●	●
164.308(a)(4)	Patch Management	Policies and Procedures	●	
		Maintenance	●	
		Application	●	
		Exceptions	●	
		Alternative Measures	●	
		Compensating Controls	●	●
164.308(a)(5)	Risk Management	Planning		
		Maintenance	●	
		Priorities	●	
		Implementation	●	
164.308(a)(6)	Sanction Policy	Policies and Procedures		
		Modifications	●	
		Application	●	
164.308(a)(7)	Information System Activity Review	Policies and Procedures		
		Scope	●	●
		Record Review	●	
		Record Retention	●	●
		Response	●	
		Maintenance	●	

Sections	Standard	Implementation specifications	HIPAA expansion	Gigamon can help
164.308(a)(8)	Assigned Security Responsibility	Inventory		
164.308(a)(9)	Workforce Security	Authorization and/or Supervision		
		Work Force Clearance Procedure		
		Modification and Termination Procedures		
		Notifications	●	
		Maintenance	●	
164.308(a)(10)	Information Access Management	Isolating Healthcare Clearinghouse functions		●
		Access Authorization		
		Authentication Management		
		Access Determination	●	
		Network Segmentation	●	●
		Maintenance	●	●
164.308(a)(11)	Security Awareness Training	Training		
		Timing		
		Ongoing Education		
		Documentation		
163.308(a)(12)	Security Incident Procedures	Planning and Testing		
		Response	●	●
163.308(a)(13)	Contingency Planning	Critically Analysis		
		Data backups		
		Information System Backups		
		Disaster Recovery Plan		
		Emergency Mode Operation Plan		
		Testing and Revision Procedures	●	
164.308(a)(14)	Compliance Audit		●	
164.308(b)(1)	Business Associate Contracts and Other Arrangements	Written contract or other arrangement		
		Written verification	●	

Sections	Standard	Implementation specifications	HIPAA expansion	Gigamon can help
164.308(b)(2)	Omitted in Source Docs			
164.308(b)(3)	Delegation of Business Associate		●	
164.310(a)	Facility Access Controls Information Access Management	Contigency Operation		
		Facility Security Plan		
		Access Management and Validation Procedures		
		Physical maintenance Records		●
		Maintenance	●	
164.310(b)	Workstation Use	Policies and Procedures		●
		Maintenance	●	
164.310(c)	Workstation Security			●
164.310(d)	Technology Asset Controls	Disposal		
		Media Sanitization		
		Maintenance		
164.312(a)	Access Control	Unique Identification		●
		Administration and Increased Access Privileges		
		Emergency Access Procedure		
		Log-in Attempts		
		Network Segmentation	●	●
		Data Controls	●	
		Maintenance	●	
134.312(b)	Encryption Enforcement and Verification	Implementation Specifications	●	●
		Exceptions	●	●
		Alternative Measures	●	●
		Compensating Controls	●	●
		Maintenance	●	●

Sections	Standard	Implementation specifications	HIPAA expansion	Gigamon can help
164.312(c)	Configuration Management	Anti-malware Protection	●	
		Software Removal	●	
		Configuration	●	
		Network Ports	●	
		Maintenance	●	●
164.312(d)	Audit trail and System Log Controls	Monitor and Identify	●	●
		Record	●	●
		Retain	●	●
		Scope	●	●
		Maintenance	●	●
164.312(e)	Integrity			●
164.312(f)	Authentication	Information Access Management Policies		
		Multi-factor Authentication	●	
		Exceptions	●	
		Alternative Measures	●	
		Compensating Controls	●	
		Maintenance	●	
164.312(g)	Transmission Security			
164.312(h)	Vulnerabiltiy Management	Vulnerability Scanning	●	
		Monitoring	●	
		Penetration Testing	●	●
		Patch and Update Installation	●	
164.312(i)	Data Backup and Recovery	Data Backup	●	
		Monitor and Indentity	●	
		Record	●	
		Testing	●	
164.312(j)	Information Systems Backup and Recovery		●	

Architectural Overview

The value Gigamon delivers lies in two key capabilities: a) full access to all network communications, including lateral (East-West) traffic, and b) the efficient extraction and delivery of packet-level metadata to your existing tools. The Gigamon Deep Observability Pipeline goes beyond current security and observability approaches that rely exclusively on metrics, events, logs, and traces (MELT) data to extend the value of your cloud, security, and observability tools with real-time network-derived telemetry.

For a better appreciation of the unique visibility offered here, it is important to understand where Gigamon is positioned in the network. Deploying Gigamon network taps, integral to the Gigamon Deep Observability Pipeline, is the first step in the process of gaining consistent deep observability across your hybrid cloud environment. The taps observe network traffic from Layers 2–7. Gigamon is not part of the Layer 3 communication pathway and does not participate in Layer 3 traffic. These appliances observe traffic in various locations across the network while extracting security- and performance-related intelligence through deep packet inspection. Although Gigamon does not look for threats, it can provide a rich set of metadata from external network observation of applications and protocols in use to detect threats that may have previously been unseen. External means the behavior is observed from outside the application, process, or workload and is not derived from internal applications, processes, or workload logs.

In virtual environments, this visibility is extended to virtual machines and containers. Traffic is observed, and in some cases, such as containers, traffic is duplicated so it can be observed independent of the state of the workload. This works in both public and private clouds.

A particular area of risk in healthcare is the medical Internet of Things (IoT). According to researchers at Brown University, medical devices are preferred targets in healthcare. Since all IoT devices communicate on the network, observing their behavior though network telemetry is a practical way to monitor them. Their communications should be fairly static, and any behavior outside of that should be investigated.

Because of this broad footprint, the logs and metadata generated can span distinct administrative boundaries within an organization. For example, a network conversation that starts on-prem and then goes to the public cloud would in many instances be seen as two conversations: a log entry on-prem and a log entry in the public cloud. Gigamon would log the entry once and append its inspection-derived metadata to the conversation—details like the specific certificate, cipher, and encryption level; how long it took; and what the URL was if any.

This is different from other kinds of observability tools:

- Routers and switches can create network logs, but they participate in the traffic, and their logs are not application aware. Logging of such information is best effort on appliances and in public clouds.
- Next-generation firewalls (NGFWs) can provide rich logging with application visibility. Typically, they participate in Layer 3 communications, so they do not have the workload-to-workload visibility Gigamon offers. An NGFW is also expensive in terms of engineering hours, and it would have to touch every broadcast domain to have the same reach as Gigamon.
- Endpoint detection and response (EDR) is another rich source of logging. This could be considered the inverse of Gigamon visibility. Logs and traces are created from within the workload, affording a top-down view, while Gigamon offers a bottom-up view from outside the workload. The two solutions complement one another.

This is not a comprehensive list of visibility solutions but serves to highlight the unique nature of where Gigamon is positioned. You can't protect or monitor what you can't see.

Mapping the HIPAA Requirements

This is a high-level overview of how Gigamon can help meet the new HIPAA requirements. A more extensive explanation can be found in the practitioner's guide. The first challenge with the new HIPAA update is that section numbers are changing. In the older framework, Section 164.308(a)(1) was Securing Management Process, which has:

- Risk analysis
- Risk management
- Sanction policy
- Information system activity review

Each of those categories now has its own expanded section with a new section number. For example, risk management was previously part of 308(a)(1); it now has its own dedicated section, 164.308(a)(5). Section 164.308(a)(1) is now "technology asset inventory."

The sections that follow will use the new HIPAA format. Here we'll explore these sections and standards in more depth. We will give excerpts from the new guidelines along with a description of how Gigamon aids in meeting those requirements. Descriptions may be shortened, for example, to remove legal references; for the exact text, consult the official publication. We'll only cover areas in which Gigamon can help.

Practitioner's Guide

- ● Orange indicates Gigamon value proposition
- ● Yellow indicates HIPAA expansion

Section 164.308(a)(1): Technology asset inventory

● INVENTORY

Description of Inventory
Develop a written inventory of the covered entity's or business associate's technology assets that contains the identification, version, person accountable, and location of each technology asset.

How Gigamon Helps
The Gigamon Deep Observability Pipeline can aid in inventory creation and verification by observing both known and unknown physical and virtual devices that communicate on the network. This includes IoT and other devices that can be a challenge to observe. This information will supplement existing sources.

● NETWORK MAP

Description of Network map
Develop a network map that illustrates the movement of electronic protected health information throughout the covered entity's or business associate's electronic information systems, including but not limited to how electronic protected health information enters and exits such information systems, and is accessed from outside of such information systems.

How Gigamon Helps
Gigamon offers a bottom-up view of network traffic in motion. This can be used to identify and track how and where protected health information travels through the network. This deep observability can extend beyond administrative boundaries—for example, from on prem to the public cloud or to a third party. A secondary function is that Gigamon can mirror or duplicate selected traffic to chosen tools for further analysis and tracking. This can be used to initially map data flows and perform a discovery. Additionally, continuous telemetry monitoring can observe changes and verify existing guardrails are in place.

● MAINTENANCE

Description of Maintenance

Review and update the written inventory of technology assets required and the network map

(1) On an ongoing basis, but at least once every 12 months

(2) When there is a change in the covered entity's or business associate's environment or operations that may affect electronic protected health information, including but not limited to:

Adoption of new technology

- assets
- upgrading
- updating
- patching of technology assets

Newly recognized threats to electronic protected health information:

- confidentiality
- integrity
- or availability

Changes in the environment based on:

- a sale
- transfer
- merger
- or consolidation of all or part of the covered entity or business associate with another person

A security incident that affects the protected health information:

- confidentiality
- integrity
- availability of electronic PHI

Relevant changes in federal, state, tribal, or territorial law

How Gigamon Helps

The Gigamon Deep Observability Pipeline can aid ongoing maintenance and reporting in many ways. The first is by continuously observing devices and applications, both known and unknown. During dynamic situations such as mergers, acquisition, or interfacing with covered entities, known and unknown systems can be observed. A new addition is the requirement of availability. This is a broad requirement to ensure any device with Protected Health Information (PHI) can perform well. This also includes systems that may not have PHI but can be patient affecting such as electronic door locks and HVAC systems. Gigamon can assist in meeting the requirement by observing the behavior on the devices with PHI. This observation is external, and telemetry can be created regardless of the internal state of the device. For example, if there is a performance problem, network-derived telemetry can quickly help determine where the problem is (is it the network or not?). During security events, Gigamon is an additional source of immutable network telemetry. Threat actors routinely turn off or erase logs or leave systems in states with inaccurate logs. The 12-month report can be made easier by running a report on all observed devices from the existing data lake or SIEM during that period, easing the operational burden.

Section 164.308(a)(2) Risk analysis

● ASSESSMENT

Description of Assessment

Conduct an accurate and comprehensive written assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted by the covered entity or business associate.

How Gigamon Helps

The Gigamon Deep Observability Pipeline will lay the foundation of risk assessment by helping you accurately understand devices and dataflow in the network. Traffic and network segmentation can also be observed to help facilitate risk analysis.

● MAINTENANCE

Description of Maintenance

Review, verify, and update the written assessment on an ongoing basis, but at least once every 12 months and, in accordance with paragraph (a)(1)(ii)(C)(2) of this section, in response to a change in the covered entity's or business associate's environment or operations.

How Gigamon Helps

Administrations will always be undergoing some kind of change as part of ongoing operations. Gaining deep observability into ongoing network and device telemetry can help speed any risk report by observing existing guardrails and detecting any security or configuration drift. In dynamic environments with partners and hybrid environments prone to a lot of change, this high maturity telemetry can enrich reporting.

164.308(a)(3) Evaluation

- ● PERFORMANCE

Description of Performance

Perform a written technical and nontechnical evaluation to determine whether a change in the covered entity's or business associate's environment or operations may affect the confidentiality, integrity, or availability of electronic protected health information.

Perform a written technical and nontechnical evaluation within a reasonable period of time before making a change in the covered entity's or business associate's environment or operations as described in paragraph (a)(1)(ii)(C)(2) of this section.

How Gigamon Helps

Network telemetry performance information of all data in motion on the network allows technical evaluations to determine changes in covered entities or business associate's environment or operations affecting confidentiality, integrity, or availability of PHI. Additionally, changes in behavior and communication patterns can indicate changes in a partner network's integrity. Confidentiality can be ensured by making sure proper encryption is in place for data in motion. Periodic reports can be run from this telemetry to help ease operational burden of the reporting requirement.

- ● RESPONSE

Description of Response

Respond to the written technical and nontechnical evaluation in accordance with the covered entity's or business associate's risk management plan required by paragraph (a)(5)(ii)(A) of this section.

How Gigamon Helps

Network-derived telemetry efficiently delivered to existing tools can speed up reporting and ability to deliver written technical responses and reports.

Section 164.308(a)(4) Patch management

- ● Policies and procedures
- ● Maintenance
- ● Application
- ● Exceptions
- ● Alternative measures
- ● COMPENSATING CONTROLS

Description of Compensating controls

A covered entity or business associate must implement reasonable and appropriate security measures to address the identified risk in a timely manner until a patch, update, or upgrade that does not adversely affect the confidentiality, integrity, or availability of electronic protected health information becomes available.

How Gigamon Helps

Through network-derived telemetry, Gigamon can help verify confidentiality, integrity, and availability of devices.

- Confidentiality: Assuring the network is running with the proper encryption and no unexpected behavior or communications take place
- Integrity: Integrity of data in motion is verified by having appropriate encryption in use
- Availability can be verified by making sure the system can communicate and respond in an appropriate manner on the network

Section 164.308(a)(5) Risk management

- ● Planning
- ● Maintenance
- ● Priorities
- ● Implementation

Section 164.308(a)(6) Sanction policy

- ● Policies and procedures
- ● Modifications
- ● Application

164.308(a)(7) Information system activity review

- Policies and procedures
- SCOPE

Description of scope
Records of activity in the covered entity's or business associate's relevant electronic information systems by persons and/or technology assets include but are not limited to audit trails, event logs, firewall logs, system logs, data backup logs, access reports, antimalware logs, and security incident tracking reports.

How Gigamon Helps
Gigamon Deep Observability Pipeline falls within the scope of record of activities within the network and electronic information system. These logs and telemetry can be used in locations or generated for devices that do not have logging capability themselves or used to supplement/verify existing logging

- Record review
- RECORD RETENTION

Description of Record Retention
Retain records of activity in the covered entity's or business associate's relevant electronic information systems by persons and technology assets for a period of time that is reasonable and appropriate for the type of report or log.

How Gigamon Helps
The Gigamon Deep Observability Pipeline will lay the foundation of visibility and telemetry by observing the behavior of devices and workloads. Logging can be created in parallel or offloaded onto Gigamon, which is especially useful in hybrid cloud environments.

- Response
- Maintenance

164.308(a)(8) Assigned security responsibility

164.308(a)(9) Workforce security

- Authorization and/or supervision
- Work force clearance procedure
- Modification and termination procedures
- Notification
- Maintenance

164.308(a)(10) Information access management

- ISOLATING HEALTH CARE CLEARING HOUSE FUNCTIONS

Description of 164.308(a)(10) Isolating health care clearinghouse functions
Establish and implement written policies and procedures for authorizing access to electronic protected health information and relevant electronic information systems to Isolate health care clearinghouse functions. If a health care clearinghouse is part of a larger organization, the clearinghouse must establish and implement written policies and procedures that protect the electronic protected health information and relevant electronic information systems of the clearinghouse from unauthorized access by the larger organization.

How Gigamon Helps
Gigamon telemetry can help in discovering communication with healthcare clearing houses, especially with other organizations. Once guardrails are in place, network-derived telemetry can be used to monitor network level access and observe any unauthorized or unknown connections from the network layer.

- Access authorization
- Authentication management
- Access determination
- NETWORK SEGMENTATION

Description of Network segmentation
Establish and implement written policies and procedures that ensure that a covered entity's or business associate's relevant electronic information systems are segmented to limit access to electronic protected health information to authorized workstations.

How Gigamon Helps
Network segmentation is a challenge without a detailed understanding of system communication before and after segmentation; there is a high risk of blocking the wrong kind of traffic and potentially disrupting vital communications. The Gigamon Deep Observability Pipeline can observe network traffic and telemetry to known and unknown computers, both physical and virtual, on the network to verify or provide observed communications so you can design and implement network segmentation.

- MAINTENANCE

Description of 164.308(a)(10) Maintenance
Review and test the written policies and procedures at least once every 12 months, and modify as reasonable and appropriate.

How Gigamon Helps
By running reports based on observed network telemetry, you can at least partially verify policies and procedures.

164.308(a)(11) Security awareness training

- Training
- Timing
- Ongoing education
- Documentation

163.308(a)(12) Security incident procedures

- Planning and testing
- RESPONSE

Description of 163.308(a)(12) Response

1. Identify and respond to suspected or known security incidents.
2. Mitigate, to the extent practicable, harmful effects of security incidents that are suspected or known to the covered entity or business associate.
3. Identify and remediate, to the extent practicable, the root cause(s) of security incidents that are suspected or known to the covered entity or business associate.
4. Eradicate the security incidents that are suspected or known to the covered entity or business associate.
5. For suspected and known security incidents, develop and maintain documentation of investigations, analyses, mitigation, and remediation.

How Gigamon Helps
The Gigamon Deep Observability Pipeline is integral to any detection and response plan. It’s a source of immutable network telemetry based on the observations of network traffic in motion, no matter the internal state of affected devices. If logging was turned off or erased this telemetry will still be created. This telemetry is critical in tracking lateral movement and verifying the cessation of the incident. This could be workloads or infrastructure such as printers, badge readers, routers, and firewalls. Advance threat actors have been observed establishing persistence mechanisms with compromised devices including routers and firewalls, without this level of telemetry and visibility that can be difficult to detect. This broad lateral telemetry is also application aware and can observe common connection and evasion techniques, greatly aiding in response, investigation, and analysis.

163.308(a)(13) Contingency planning

- Criticality analysis
- Data backups
- Information system backups
- Disaster recovery plan
- Emergency mode operation plan
- Testing and revision procedures

164.308(a)(14) Compliance Audit

164.308(b)(1) Business associate contracts and other arrangements

- Written contract or other arrangement
- Written verification

164.308(b)(2) – Omitted in source docs

164.308(b)(3) Delegation of business associate

164.310(a) Facility access controls

- Contingency operations
- Facility security plan
- Access management and validation procedures
- PHYSICAL MAINTENANCE RECORDS

Description of 164.310(a) Physical Maintenance records
Establish and implement written policies and procedures to document repairs and modifications to the physical components of a facility that are related to security, including but not limited to hardware, walls, doors, locks, and security cameras.

How Gigamon Helps
Many devices, such as badge readers, door locks, time clocks, and cameras, are now on the network. Their digital security, as well as physical security, must now be maintained. The underlying infrastructure is automated, and communication with these devices is difficult to see. With Gigamon network-derived telemetry, you can observe these devices for unusual

behavior, errors, or unexpected communications and conditions.

- ● Maintenance

164.310(b) Workstation use

- ● POLICIES AND PROCEDURES

Description of 164.310(b) Policies and procedures
Establish and implement written policies and procedures that govern the use of workstations that access electronic protected health information or the covered entity's or business associate's relevant electronic information systems. The written policies and procedures must specify all of the following with respect to a workstation that accesses electronic protected health information or the covered entity's or business associate's relevant electronic information systems:

- The functions for which a workstation may be used.
- The manner in which a workstation may be used to perform those functions.
- The physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information, including the removal of such workstations from a facility and the movement of such workstations within and outside of a facility.

How Gigamon Helps
Healthcare is a dynamic operating environment where equipment can move around a facility. Having locks and secure cases for physical protection is important. Being able to track that equipment is easier via network telemetry. By seeing where the equipment is on the physical and logical network, you can often track its location to a general geographic area or tell if the device has left the on-prem network. You can also observe unusual communication or unauthorized applications, indicating a possible drift in security guardrails.

- ● Maintenance

164.310(c) Workstation security

Description of 164.310(c) Workstation Security
Implement and modify physical safeguards for all workstations that access electronic protected health information or relevant electronic information systems and restrict access to authorized users. Establish and implement written policies and procedures that govern the receipt and removal of technology assets that maintain electronic protected health information into and out of a facility, and the movement of these assets within the facility.

How Gigamon Helps:
Healthcare is a dynamic operating environment where equipment can move around a facility. Having locks and secure cases for physical protection is important. Being able to track that equipment is easier via network telemetry. By seeing where the equipment is on the physical and logical network, you can often track its location to a general geographic area or tell if the device has left the on-prem network. You can also observe unusual communication or unauthorized applications, indicating a possible drift in security guardrails.

164.310(d) Technology asset controls

- ● Disposal
- ● Media sanitization
- ● Maintenance

164.312(a) Access control

- ● UNIQUE IDENTIFICATION

Description of 164.312(a) Unique identification
Assign a unique name, number, and/or other identifier for tracking each user and technology asset in the covered entity or business associate's relevant electronic information systems.

How Gigamon Helps
Digital assets often have a series of technical identifiers such as MAC address that allows them to be fingerprinted via network observation. This way, device movement can be tracked across a campus.

- ● Administrative and increased access privileges
- ● Emergency access procedure
- ● Log-in attempts
- ● NETWORK SEGMENTATION

Description of 164.312(a) Network segmentation
Deploy technical controls to ensure that the covered entity's or business associate's relevant electronic information systems are segmented in a reasonable and appropriate manner.

How Gigamon Helps

Gigamon provides crucial network telemetry to help design and implement network segmentation to minimize high friction configurations. Additionally, once segmentation is in place, Gigamon telemetry can help verify the effectiveness and spot any kind of security or configuration drift.

- Data controls
- Maintenance

134.312(b) Encryption and decryption

- IMPLEMENTATION SPECIFICATIONS

Description of 134.312(b) Implementation specifications

Deploy technical controls to encrypt and decrypt electronic protected health information using encryption that meets prevailing cryptographic standards. Encrypt all electronic protected health information at rest and in transit, except to the extent that an exception applies.

How Gigamon Helps

All network traffic should be encrypted. Gigamon network-derived telemetry provides complete visibility into both encrypted and non-encrypted traffic. Unencrypted traffic, weak ciphers, expired certificates, weak protocols especially from IoT can be difficult to monitor and detect via class means. The Gigamon Deep Observability Pipeline can layer of control verification in such environments. Gigamon also has broad classic decrypt features that can decrypt sensitive traffic, mask PHI and send that traffic to other inspection tools.

- EXCEPTIONS

Description of 134.312(b) Exceptions

The covered entity or business associate documents that an exception applies and that all other applicable conditions are met.

How Gigamon Helps

Systems that cannot encrypt traffic or cannot use modern encryption, will need to be segmented on the network. Gigamon telemetry can help identify those systems and then verify guardrails that have been put in place work. Additionally, these systems often have unique identifying characteristics in their communication patterns or in deprecated encryption, allowing visibility into their use and location which aids in reporting compliance.

- ALTERNATIVE MEASURES

Description of 134.312(b) Alternative measures

Where an exception applies, a covered entity or business associate must document in real time the existence of an applicable exception and implement reasonable and appropriate compensating controls.

How Gigamon Helps

Systems not using encryption can be observed in real time aiding this documentation.

- COMPENSATING CONTROLS

Description of 134.312(b) Compensating controls

For exception the covered entity or business associate must secure such electronic protected health information by implementing reasonable and appropriate compensating controls reviewed and approved by the covered entity's or business associate's designated Security Official.

The covered entity or business associate shall be presumed to have implemented reasonable and appropriate compensating controls where the covered entity or business associate has deployed the security measures prescribed and as instructed by the authorized label for the device, including any updates or patches recommended or required by the manufacturer of the device.

Entities or business associate that have implemented compensating controls the implementation and effectiveness of compensating controls must be reviewed, documented, and signed by the designated Security Official at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, to continue securing electronic protected health information and relevant electronic information systems.

- MAINTENANCE

Description of 134.312(b) Maintenance

Review and test the effectiveness of the technical controls required at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

How Gigamon Helps

Systems that cannot encrypt traffic or cannot use modern encryption will need to be segmented on the network. Gigamon can help identify those systems and then verify guardrails that have been put in place work. Additionally in merger and acquisition or change scenario it can be quickly observed if guardrails are in place or need to be altered along with needed reporting.

164.312(c) Configuration management

- Anti-malware protection
- Software removal
- Configuration
- Network ports
- MAINTENANCE

Description of 164.312(c) Maintenance

Review and test the effectiveness of the technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

How Gigamon Helps

Gigamon network telemetry can identify known and unknown applications in use, including shadow IT. This can be used to detect unwanted, unknown, or unapproved software in use on electronic information systems.

164.312(d) Audit trail and system log controls

- MONITOR AND IDENTIFY

Description of 164.312(d) monitor and identify: Deploy technology assets and/or technical controls that record and identify activity in the covered entity's or business associate's relevant electronic information systems.

(2) Implementation specifications—(i) Monitor and identify. The covered entity or business associate must deploy technology assets and/or technical controls that monitor in real-time all activity in its relevant electronic information systems, identify indications of unauthorized persons or unauthorized activity as determined by the covered entity's or business associate's risk analysis, and alert workforce members of such indications in accordance with the policies and procedures.

How Gigamon Helps

Gigamon network-derived telemetry can observe a business associate's behavior on the network. This can include known and unknown applications and which devices/IoT are interacted with. Gigamon offers a bottom-up view of network traffic in motion. This can be used to identify and track how and where a business associate travels through the network. This deep observability can extend beyond administrative boundaries—for example, from on prem to the public cloud or to a third party. A secondary function is that Gigamon can mirror or duplicate selected traffic to chosen tools for further analysis and tracking. This can be used to initially map data flows and perform a discovery.

- RECORD

Description of 164.312(d) Record

The covered entity or business associate must deploy technology assets and/or technical controls that record in real-time all activity in its relevant electronic information systems.

How Gigamon Helps

Gigamon network telemetry generates rich network metadata of all conversations. This can be seen as an additional source of telemetry and logging in case existing systems or infrastructure is under duress and cannot accurately log.

- RETAIN

Description of 164.312(d) Retain

The covered entity or business associate must deploy technology assets and/or technical controls to retain records of all activity in its relevant electronic information systems as determined by the covered entity's or business associate's policies and procedures for information system activity review.

How Gigamon Helps

Network telemetry can take the form of metadata, which can reduce storage requirements for logs when the alternative is full traffic capture and storage. This can be seen as an additional source of telemetry and logging in case existing systems such as DNS servers or infrastructure is under duress and cannot accurately log.

- SCOPE

Description of 164.312(d) Scope
Activity includes creating, accessing, receiving, transmitting, modifying, copying, or deleting any of the following: (A) Electronic protected health information. (B) Relevant electronic information systems and the information therein.

How Gigamon Helps
Activities that accessing, receiving, transmitting, modifying, and copying data often have a network component and fall within scope of what should be recorded and logs retained. It is not always obvious as to what systems and information retention should be within scope. Observation of large data transmissions, network telemetry and metadata around that are critical for properly sizing the scope of what needs to observed. Day-to-day operations should fall into an operational cadence with behaviors outside of that may need to be investigated or scope reassessed. Gigamon telemetry can observe this behavior on the network. This can include known and unknown applications and which devices/IoT are interacted with. Gigamon offers a bottom-up view of network traffic in motion.

- MAINTENANCE

Description of 164.312(d) Maintenance
Review and test the effectiveness of the technology assets and/or technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

How Gigamon Helps
Gigamon network telemetry can provide critical data for reporting on some controls and network Performance. in the ongoing collection of metadata and telemetry in the above 164.312(d) sections you can see which systems are performing, if communication patterns are with in norms of if there are a lot of changes ongoing. This kind of telemetry makes running reports and assessments easily.

164.312(e) Integrity

Description of 164.312(e) Integrity
Deploy technical controls to protect electronic protected health information from improper alteration or destruction, both at rest and in transit; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

How Gigamon Helps
Gigamon network telemetry can observe communication protocols and encryption in use on the network. Proper encryption ensures message integrity which proves data in transit was not altered during transmission on the network level.

164.312(f) Authentication

- Information access management policies
- Multi-factor authentication
- Exceptions
- Alternative measures
- Compensating controls
- Maintenance

164.312(g) Transmission security

164.312(h) Vulnerability management

- Vulnerability scanning
- Monitoring
- PENETRATION TESTING

Description of 164.312(h) Penetration testing
Perform penetration testing of the covered entity's or business associate's relevant electronic information systems by a qualified person.

- A qualified person is a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of electronic protected health information.
- Penetration testing must be performed at least once every 12 months or in accordance with the covered entity's or business associate's risk analysis required by § 164.308(a)(2), whichever is more frequent.

How Gigamon Helps

Penetration testing is often complex and involved. Testers will have an array of tools to use to test the security of applications and access around the network. Gigamon network telemetry is critical for helping detect penetration testing. Moving laterally in the network is critical because certain systems are only subject to certain tests. Detecting the Pen testers is often a pass criterion of the test. The Pen testers use novel techniques for lateral movement that can help detect potential vulnerabilities. These novel techniques such as non-standard port usage are effectively undetectable via classic logging methodologies. Gigamon is not a security solution, it is a telemetry and visibility solution with its deep observability pipeline offering a unique view of what is going on including the non-standard port and other novel network techniques that often improperly identified. This visibility is external to the state of any devices under test and therefore not subject to many of the obfuscation techniques commonly used. During pen tests the testers often need to get close enough to a target to launch the test. If the testers cannot get close enough to launch a test that is considered a pass.

- Patch and update installation

164.312(i) Data backup and recovery

- Data backup
- Monitor and identify
- Record
- Testing

164.312(j) information systems backup and recovery

Conclusion

With the 2025 HIPAA updates raising the bar for cybersecurity and compliance, healthcare organizations face growing pressure to safeguard patient data and ensure operational resilience. The Gigamon Deep Observability Pipeline delivers the network visibility and telemetry needed to meet regulatory requirements while optimizing the performance and security of critical systems.

CONTRIBUTOR

Stephen Goudreault
Cloud Security Evangelist, Gigamon

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations.

To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com