Protecting Critical Health Data with Network Assurance for HIPAA Compliance

ipfabric.io ↗

HIPAA and Network Assurance

HIPAA, the (Health Insurance Portability and Accountability Act) of 1996, is a U.S. law designed to protect sensitive patient health information and to ensure its privacy, portability, standardization, and security. HIPAA protections are tied to both PHI (Patient Health Information) and electronic PHI (or ePHI) that are handled by **covered entities** and **business associates**, regardless of the patient's nationality. HIPAA applies primarily to healthcare organizations, health plans, and service providers operating in the U.S. but also covers non-US entities such that they handle patient data on behalf of U.S.-based covered entities.

For this patient data to be useful, it must transit wired and wireless networks to reach its point of use. Healthcare professionals and other agents or systems all use this data for a variety of reasons, and HIPAA strives to ensure that patient's information is protected from unauthorized access and misuse. **This means the network represents one of the broadest attack surfaces for sensitive data** while also being a beneficial strategic and tactical layer for mitigating threats and adhering to compliance requirements.

Network assurance is a critical concept not just in the healthcare sector but anywhere that network services' integrity, security, and reliability directly impact patient care or operational efficiency. Assurance involves a systematic approach to validating that network configurations, services, and policies align with both operational goals and regulatory requirements, particularly those outlined by frameworks such as HIPAA. In this paper, we will see how network assurance provided by IP Fabric accelerates and maintains HIPAA compliance by providing:

- → Centralized end-to-end visibility/observability
- → Validated state, configurations, and changes
- → Closed-loop automation SoT (Source of Truth) capabilities
- → Accelerated compliance readiness and reporting

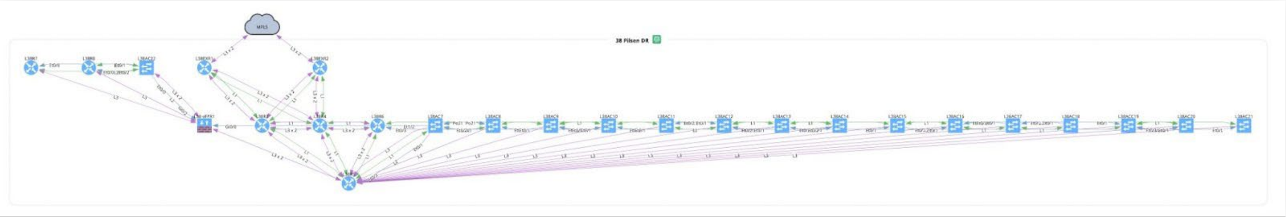


Image 1: Automatic visibility and mapping. IP Fabric is vendor-agnostic and understands your network end-to-end!

HIPAA Rules and Controls

HIPAA’s regulations are implemented and enforced through various rules, primarily codified under **Title 45 of the Code of Federal Regulations (CFR)**. Title 45, specifically within **Subtitle A, Subchapter C**, contains the provisions that outline HIPAA’s key requirements, including the:

→ Privacy Rule

→ Security Rule

→ Breach Notification Rule

In summary, HIPAA establishes the **legal framework** for protecting patient health information, while **Title 45 of the CFR** contains the **detailed regulatory requirements** and enforcement mechanisms for HIPAA. These regulations work together to ensure that healthcare entities comply with federal standards for data privacy and security.

HIPAA was established in 1996, with recent additions in April 2024 concerning reproductive personal health information.

It is broken down in Title 45 as three sets of Controls or Safeguards:

→ Administrative

→ Physical

→ Technical

Many of these controls or safeguards pertain to the reliability and protection of healthcare IT networks. These are highlighted green in the breakdown below:

Title 45:	Public Welfare
Subtitle A:	Department of Health and Human Services
Subchapter C:	Administrative Data Standards and Related Requirements
Part 164:	Security & Privacy
Subpart C:	Security Standards for the Protection of Electronic Protected Health Information

Standards	Administrative Safeguards	Physical Safeguards	Technical Safeguards
1	✓ **Security management process**	Facility access controls	✓ **Access control**
2	Assigned security responsibility	Workstation use	✓ **Audit controls**
3	Workforce security	Workstation security	Person or entity authentication
4	✓ **Information access management**	Device and media controls	✓ **Transmission security**
5	Security awareness and training		
6	✓ **Security incident procedures**		
7	✓ **Contingency plan**		

Flexibility of Approach:

HIPAA does have a flexibility of approach principle, meaning there is discretion left to the enterprise as to how to execute the principles specified. For example, they won't say "you have to use SSH instead of Telnet" but they will specify that ePHI must be encrypted in transmission. It's up to the enterprises what that means, but they must show that they "" …reasonably and appropriately implement the standards and implementation specification…"

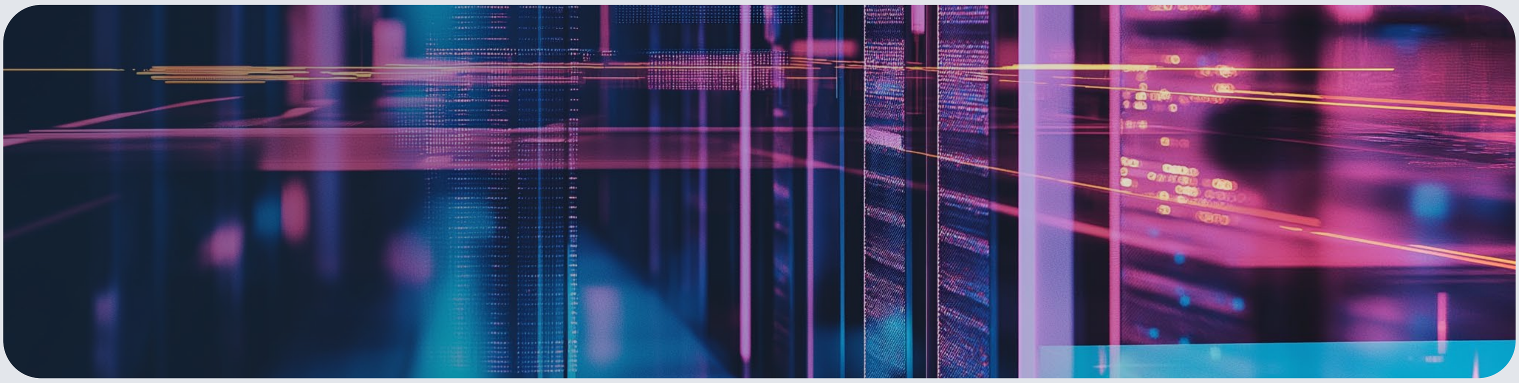
Source: § 164.306(b)

The **Security Rule** within HIPAA outlines standards and requirements for safeguarding ePHI directly impact the design, configuration, and management of an organization's IT network infrastructure.

Key provisions that affect routers, switches, firewalls, network segmentation, and related policies include:

- → **Firewalls** must be configured to enforce secure transmission and access control policies.
- → **Routers and switches** should support encryption and segmentation to protect ePHI.
- → **Network segmentation** and VLANs are vital to isolate sensitive ePHI data from less secure areas.
- → **Access logs** from network devices should be retained for auditing purposes.
- → **Incident response** must involve network monitoring and the ability to trace and mitigate breaches in real-time.

Let's look deeper at specific controls and how IP Fabric's network assurance platform can help fulfill these control requirements.



HIPAA Controls

1. Access Control (45 CFR § 164.312(a)(1))

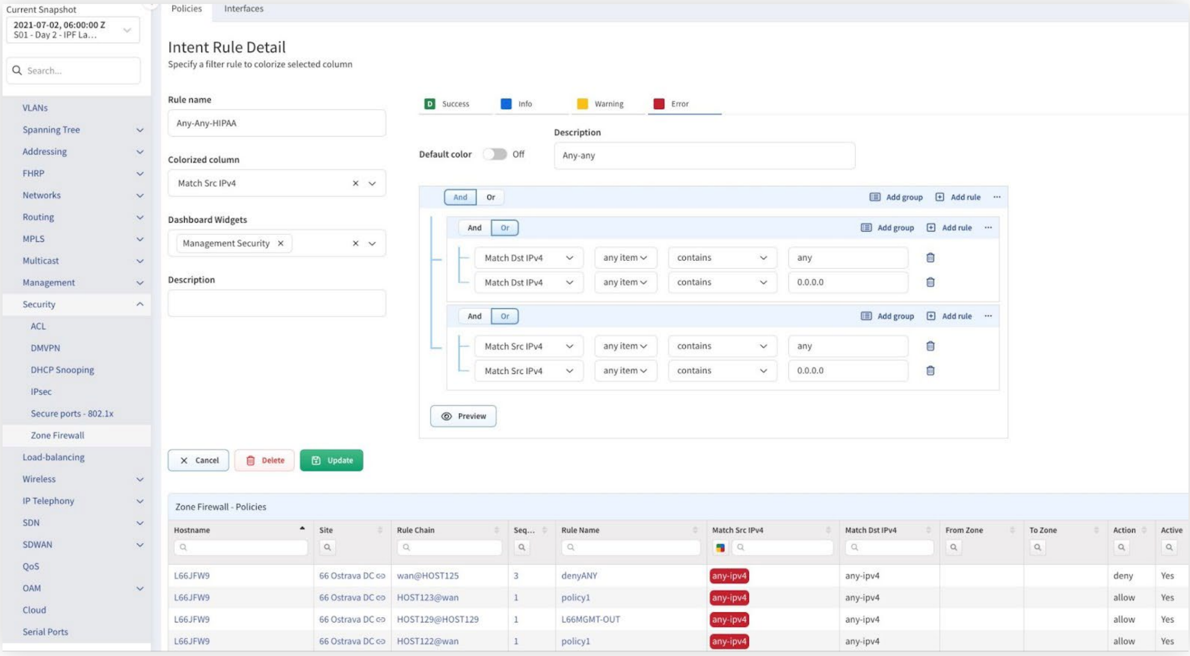
» Link: https://www.ecfr.gov/current/title-45/part-164#p-164.312(a)(1)

HIPAA requires organizations to implement technical policies and procedures to control access to ePHI. This includes:

- **Role-based access**: Network segmentation and VLANs can be used to ensure only authorized personnel have access to sensitive data.
- **Device control**: Routers, switches, and firewalls must be configured to restrict unauthorized devices from accessing the network.
- **Session management**: Systems should be able to automatically log off or terminate sessions after a period of inactivity, which might be enforced through switch/router settings or firewall policies.

IP Fabric:

- Validates and proves that segmentation implemented using VRFs, subnets, VLANs, and firewall policies are operating as expected.
- Generate end-to-end path lookups (routing and reachability) across heterogeneous infrastructure.
- Surface granular detail about every network device's configuration, state, and forwarding behavior over time (including current and historical) from full network snapshots.
- Demonstrates switch/router settings or firewall policies are enforcing automated session management.



Intent Rule Detail

Specify a filter rule to colorize selected column

Rule name: Any-Any-HIPAA

Colorized column: Match Src IPv4

Dashboard Widgets: Management Security

Description:

Default color: Off

Description: Any-any

Match Dst IPv4 | any item | contains | any
Match Dst IPv4 | any item | contains | 0.0.0.0

Match Src IPv4 | any item | contains | any
Match Src IPv4 | any item | contains | 0.0.0.0

Zone Firewall - Policies

Hostname	Site	Rule Chain	Seq...	Rule Name	Match Src IPv4	Match Dst IPv4	From Zone	To Zone	Action	Active
L66JFW9	66 Ostrava DC	wan@HOST125	3	denyANY	any-ipv4	any-ipv4			deny	Yes
L66JFW9	66 Ostrava DC	HOST123@wan	1	policy1	any-ipv4	any-ipv4			allow	Yes
L66JFW9	66 Ostrava DC	HOST129@HOST129	1	L66MGMT-OUT	any-ipv4	any-ipv4			allow	Yes
L66JFW9	66 Ostrava DC	HOST122@wan	1	policy1	any-ipv4	any-ipv4			allow	Yes

Image 2: A central view of all Zones and Firewalls, including key policy information such as any-any checks!

2. Audit Controls (45 CFR § 164.312(b))

» Link: https://www.ecfr.gov/current/title-45/part-164#p-164.312(b)

Organizations must implement hardware, software, and procedural mechanisms to record and examine access and other activity in systems that contain or use ePHI.

- **Network monitoring**: Routers, switches, and firewalls need to generate logs of access and traffic, which must be monitored to detect unauthorized access or anomalies.
- **Configuration tracking**: Changes in the network configurations (like firewall rules or router policies) must be auditable to ensure compliance.

IP Fabric provides:

- Complete, enriched, and contextualized monitoring for lower MTTR (Mean Time To Resolution) and can also ensure that the correct logging and telemetry are configured across all infrastructure via "Intent Check" rules.
- De-risked change management with pre- and post-change network configuration verification, including state validation for quick rollbacks and compliance.

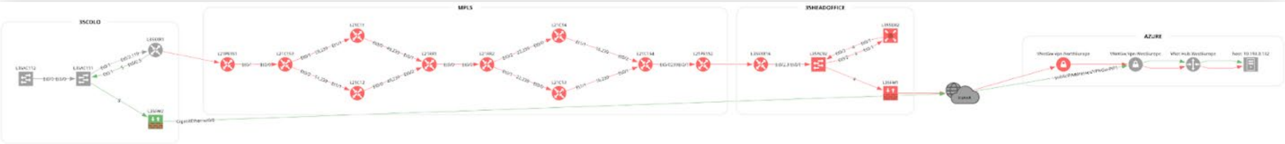
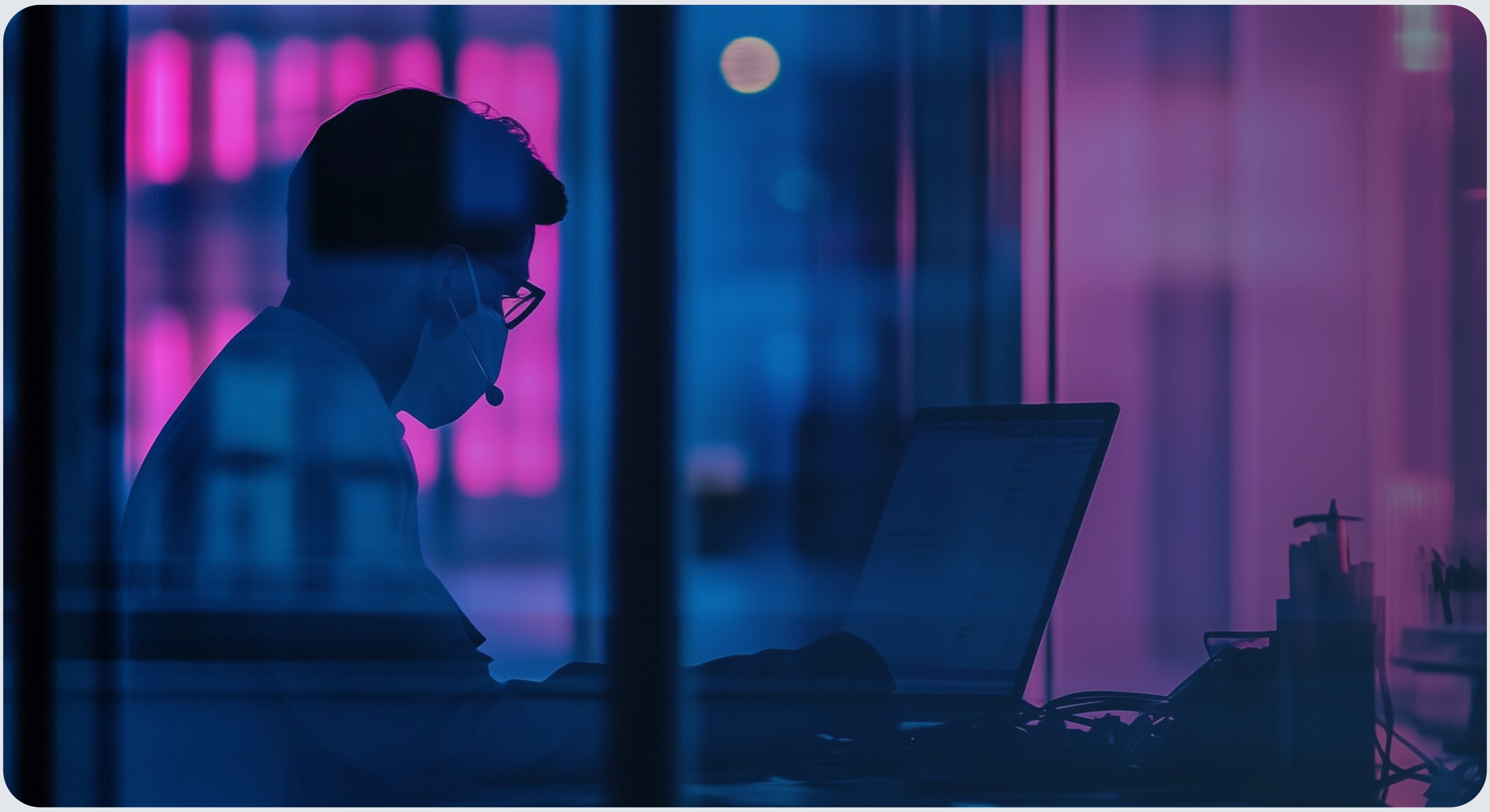


Image 3: Day-to-day network comparisons for monitoring and change management.



3. Integrity Controls (45 CFR § 164.312(c)(1))

» Link: https://www.ecfr.gov/current/title-45/part-164#p-164.312(c)(1)

The integrity of ePHI must be protected from improper alteration or destruction.

- **Firewalls and security policies**: Firewall rules should ensure that only authorized traffic enters and leaves the network, helping to prevent data corruption.
- **Routing policies**: Routers and switches should be configured with appropriate routing policies to prevent data tampering or misdirection.

IP Fabric:

- Discovers, analyzes, and normalizes firewall configuration to provide key security and risk-related context and intent checks across policies, zones, interfaces, and settings.
- Route tables (BGP, MPLS, OSPF, EIGRP, RIP, IS-IS, VRFs), policies, prefix lists, route convergence, forwarding, and behavior revealed using path lookups intent checks, and also visually presented (L2/L3) on auto-generated diagrams (inc. redundancy / reachability issues).

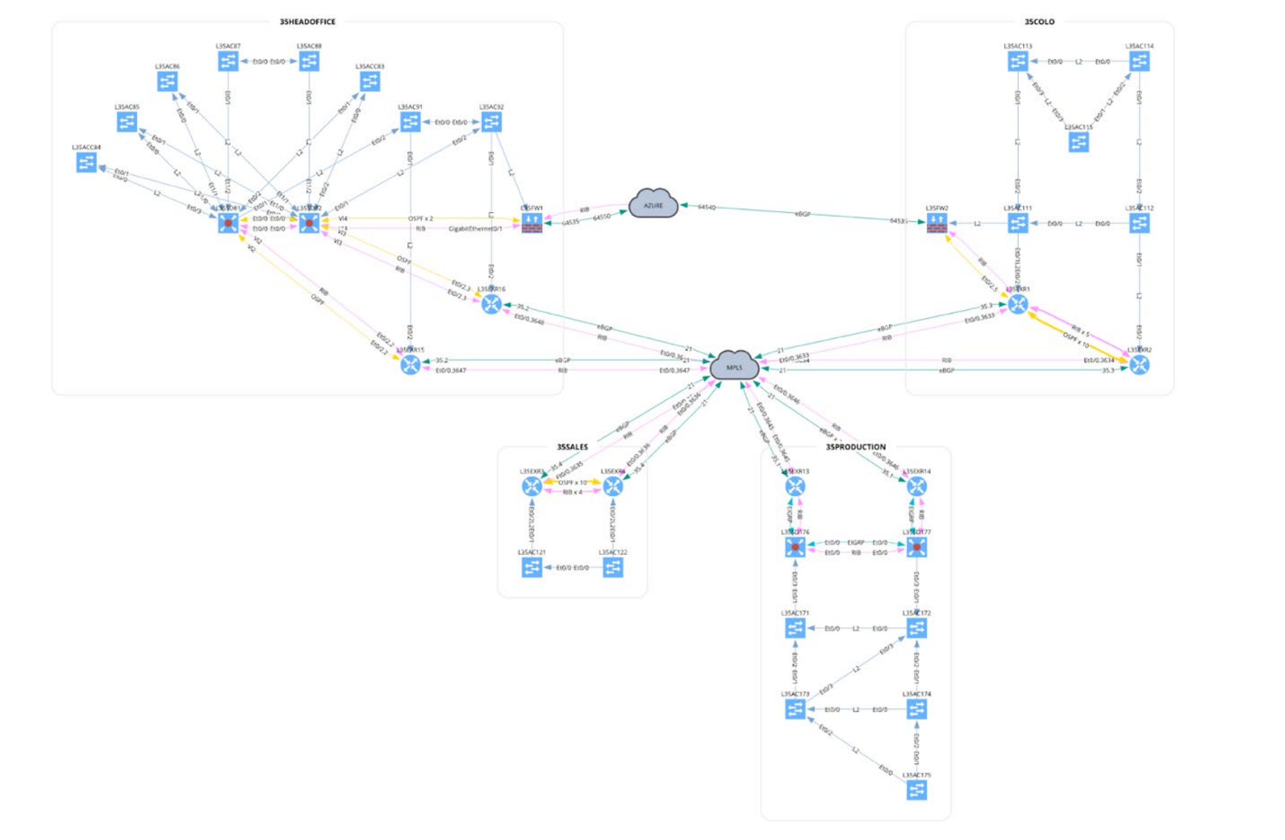


Image 4: Understanding routing, switching, and forwarding behavior in dynamic and flexible diagrams

4. Transmission Security (45 CFR § 164.312(e)(1))

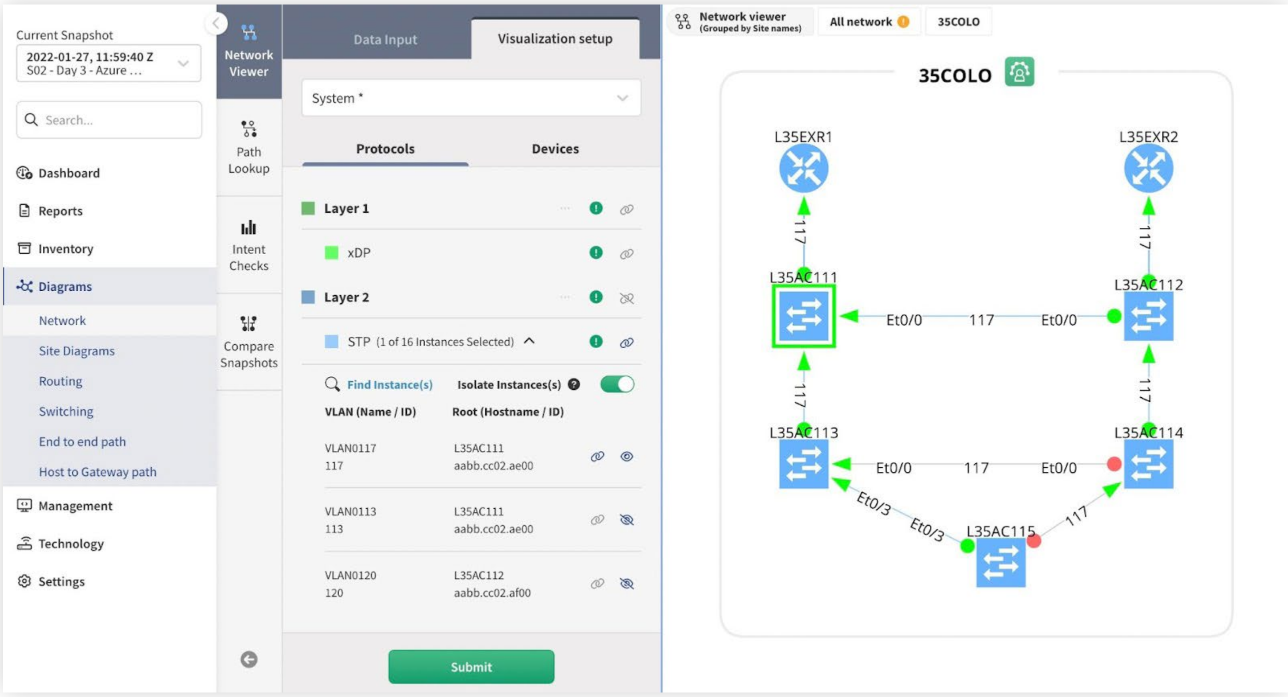
» Link: https://www.ecfr.gov/current/title-45/part-164#p-164.312(e)(1)

HIPAA mandates measures to ensure that ePHI is not improperly modified without detection during transmission and is protected against unauthorized access.

- **Encryption**: Encryption protocols should be used for data transmitted over the network (for example, between routers and switches). Firewalls can help enforce secure protocols like HTTPS and IPsec.
- **Network segmentation**: Segregating sensitive data using network segmentation (such as VLANs or isolated network zones) can prevent unauthorized users from accessing ePHI.

IP Fabric:

- Reveals encryption protocols present on network devices (e.g. firewalls, access edge) at a particular point in time.
- Provides proof of network segmentation (VLANs, subnets, VRFs, zoning) and validates effectiveness.



Current Snapshot: 2022-01-27, 11:59:40 Z S02 - Day 3 - Azure …

Search...

Dashboard
Reports
Inventory
Diagrams
Network
Site Diagrams
Routing
Switching
End to end path
Host to Gateway path
Management
Technology
Settings

Network Viewer | Path Lookup | Intent Checks | Compare Snapshots

Data Input | Visualization setup

System *

Protocols | Devices

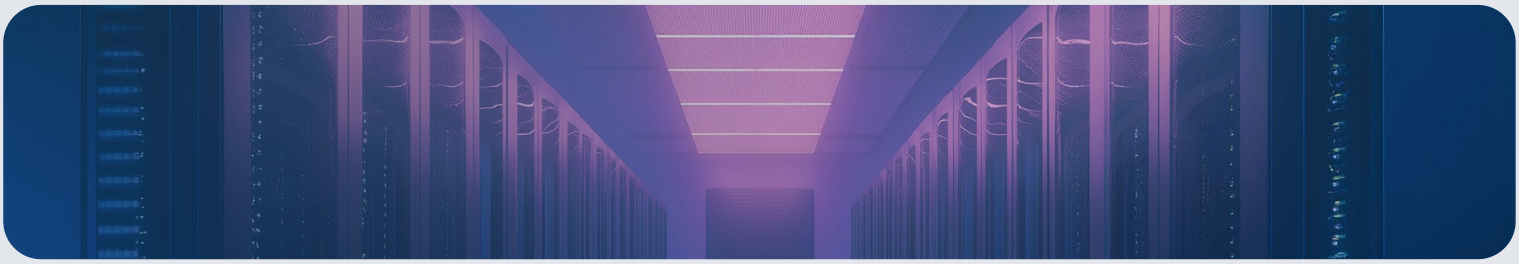
Layer 1
xDP
Layer 2
STP (1 of 16 Instances Selected)

Find Instance(s) | Isolate Instances(s) ●

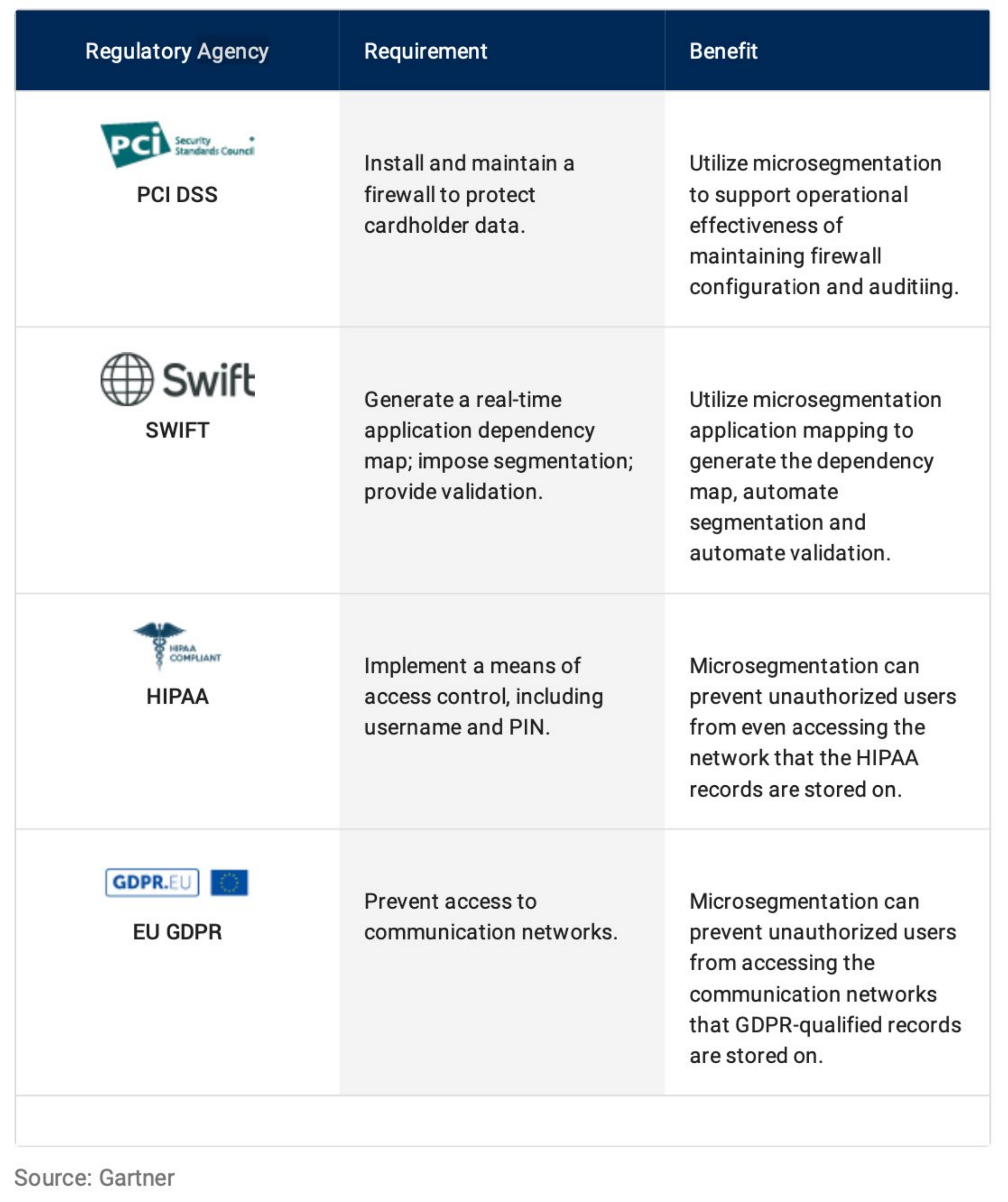
VLAN (Name / ID)	Root (Hostname / ID)
VLAN0117 117	L35AC111 aabb.cc02.ae00
VLAN0113 113	L35AC111 aabb.cc02.ae00
VLAN0120 120	L35AC112 aabb.cc02.af00

Submit

Image 5: Isolated VLAN instances using IP Fabric's dynamic network diagrams



The importance of network segmentation across multiple regulations as outlined by Gartner:



Regulatory Agency	Requirement	Benefit
PCI DSS	Install and maintain a firewall to protect cardholder data.	Utilize microsegmentation to support operational effectiveness of maintaining firewall configuration and auditiing.
SWIFT	Generate a real-time application dependency map; impose segmentation; provide validation.	Utilize microsegmentation application mapping to generate the dependency map, automate segmentation and automate validation.
HIPAA	Implement a means of access control, including username and PIN.	Microsegmentation can prevent unauthorized users from even accessing the network that the HIPAA records are stored on.
EU GDPR	Prevent access to communication networks.	Microsegmentation can prevent unauthorized users from accessing the communication networks that GDPR-qualified records are stored on.

Source: Gartner

5. Configuration Management and Security (Administrative Safeguards - 45 CFR § 164.308(a)(1)(ii)(B))

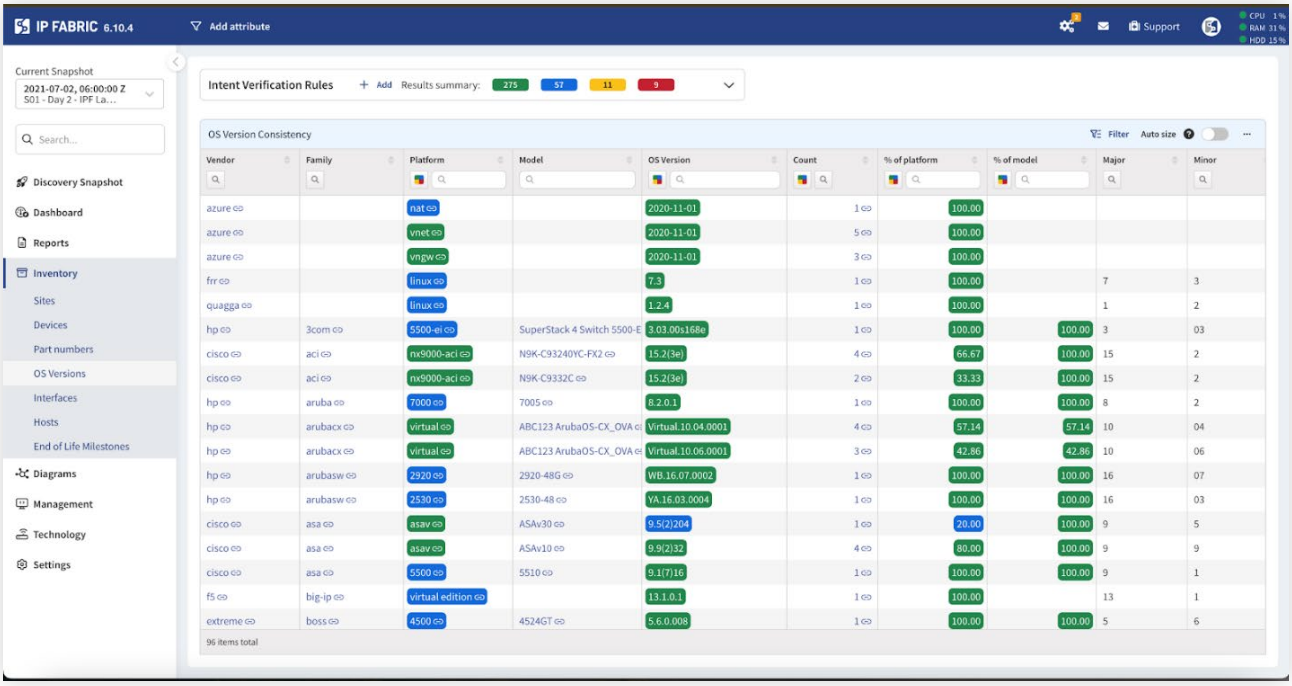
» Link: https://www.ecfr.gov/current/title-45/part-164#p-164.308(a)(1)(ii)(B)

HIPAA requires organizations to implement procedures for overseeing the configuration of network devices.

- → **Secure configurations**: Routers, switches, and firewalls must be configured using secure baselines (e.g., disabling unused services, using strong authentication protocols).
- → **Patch management**: Regular updates and patches to network hardware and software are necessary to mitigate security vulnerabilities.

IP Fabric provides:

- → A clear view, updated with every snapshot, of the authentication protocols and security policies on network devices like routers, switches, and firewalls.
- → A table of all device OS versions present on your network so you can proactively plan for updates and maintenance reconciled with CVE updates.



Current Snapshot: 2021-07-02, 06:00:00 Z S01 - Day 2 - IPF La...

Intent Verification Rules + Add Results summary: 275 57 11 9

OS Version Consistency

Vendor	Family	Platform	Model	OS Version	Count	% of platform	% of model	Major	Minor
azure		nat		2020-11-01	1	100.00			
azure		vnet		2020-11-01	5	100.00			
azure		vngw		2020-11-01	3	100.00			
frr		linux		7.3	1	100.00		7	3
quagga		linux		1.2.4	1	100.00		1	2
hp	3com	5500-ei	SuperStack 4 Switch 5500-E	3.03.00s168e	1	100.00	100.00	3	03
cisco	aci	nx9000-aci	N9K-C93240YC-FX2	15.2(3e)	4	66.67	100.00	15	2
cisco	aci	nx9000-aci	N9K-C9332C	15.2(3e)	2	33.33	100.00	15	2
hp	aruba	7000	7005	8.2.0.1	1	100.00	100.00	8	2
hp	arubacx	virtual	ABC123 ArubaOS-CX_OVA	Virtual.10.04.0001	4	57.14	57.14	10	04
hp	arubacx	virtual	ABC123 ArubaOS-CX_OVA	Virtual.10.06.0001	3	42.86	42.86	10	06
hp	arubasw	2920	2920-48G	WB.16.07.0002	1	100.00	100.00	16	07
hp	arubasw	2530	2530-48	YA.16.03.0004	1	100.00	100.00	16	03
cisco	asa	asav	ASAv30	9.5(2)204	1	20.00	100.00	9	5
cisco	asa	asav	ASAv10	9.9(2)32	4	80.00	100.00	9	9
cisco	asa	5500	5510	9.1(7)16	1	100.00	100.00	9	1
f5	big-ip	virtual edition		13.1.0.1	1	100.00		13	1
extreme	boss	4500	4524GT	5.6.0.008	1	100.00	100.00	5	6

96 items total

Image 6: A centralized overview of OS version consistency (color-coded by Intent Checks)

6. Incident Response and Contingency Planning (45 CFR § 164.308(a)(6))

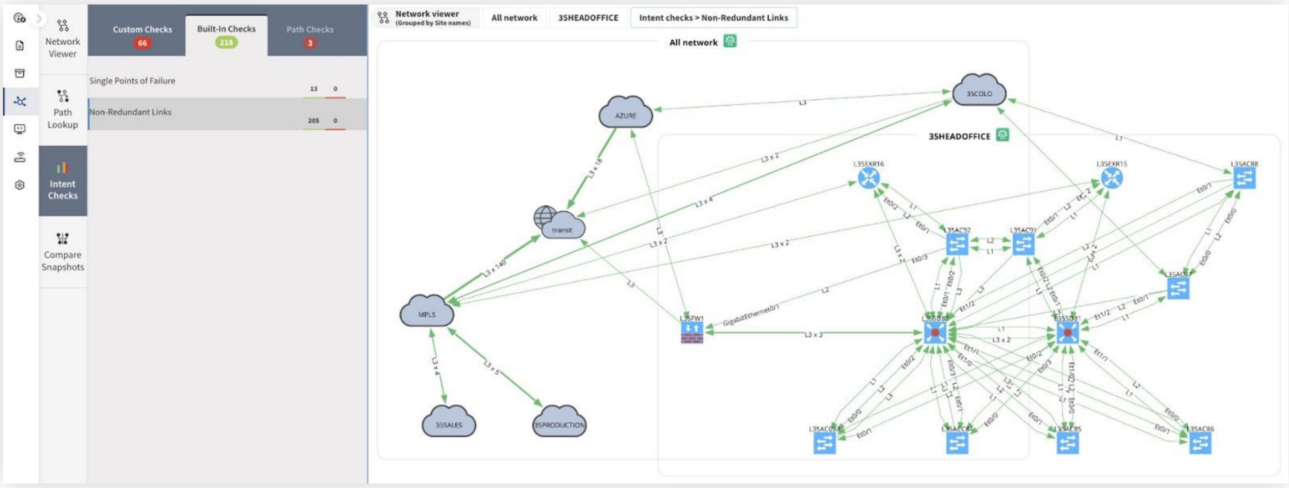
» Link: https://www.ecfr.gov/current/title-45/part-164#p-164.308(a)(6)

Organizations must have policies for responding to security incidents, including any breach that affects ePHI.

- **Firewall and IDS/IPS rules**: Firewalls and intrusion detection/prevention systems (IDS/IPS) should be configured to detect suspicious traffic or network anomalies that could indicate a security incident.
- **Network recovery plans**: Proper network segmentation and redundant configurations (like failover routers) should be in place to ensure network resilience in case of an attack or failure.

IP Fabric provides:

- An overview and granular detail of firewall state, configuration, policies, and forwarding behavior.
- Evidence of network redundancy measures (e.g. failover routers in network topology diagrams).



Single Points of Failure	13	0
Non-Redundant Links	205	0

Image 7: Built-in redundancy checks for single points of failure and non-redundant links.

7. Risk Analysis (45 CFR § 164.308(a)(1)(ii)(A))

» Link: https://www.ecfr.gov/current/title-45/part-164#p-164.308(a)(1)(ii)(A)

HIPAA mandates that covered entities conduct an ongoing risk assessment of their IT environment, which includes the network.

- → **Assessing vulnerabilities**: Routers, firewalls, and switches should be regularly evaluated for vulnerabilities, with any findings addressed through reconfiguration, patching, or upgrades.
- → **Mitigate/Reduce Blast Radius**: Network segmentation can limit the scope of a breach, ensuring that even if one segment is compromised, others are protected.

IP Fabric provides:

- → Reveals your network risk with regular point-in-time snapshots, normalized for consumption so you can focus on risk factors.
- → Validates network segmentation regularly so that if an incident does occur, critical applications are protected.

Daily Peace of Mind with IP Fabric for HIPAA Network Compliance

HIPAA compliance for IT networks focuses on ensuring ePHI confidentiality, integrity, and availability, which can be achieved through proper network configuration, segmentation, and access control. IP Fabric provides the visibility, validation, and evidence required for continuous compliance and regular stress-free network audits.

To see what healthcare network outages can cost your business, visit our blog: Impact Analysis: Healthcare.

Want to know more?

See how IP Fabric can help you to achieve continuous HIPAA compliance.

Try free for 30 days

Contact our experts

IP FABRIC
AUTOMATED NETWORK ASSURANCE PLATFORM

Support & Documentation
https://docs.ipfabric.io

HQ Office Boston
98 North Washington St.
Suite 407
Boston, MA 02114
United States

+1 617-821-3639

IP Fabric UK Ltd.
Gateley Legal,
1 Paternoster Square,
London,
England EC4M 7DX

+020 3714 4000

IP Fabric s.r.o.
Kateřinská 466/40
Praha 2 - Nové Město,
12000
Czech Republic

+420 720 022 997

ipfabric.io