ELISITY

FORRESTER
WAVE STRONG PERFORMER 2024
Microsegmentation Solutions

WHITEPAPER

# 2025 HIPAA Security Rule Update: Network Segmentation Implementation Guide

Learn how to meet 2025 HIPAA Security Rule network segmentation requirements with identity-based microsegmentation. Get expert guidance on implementation and compliance.

## Understanding the 2025 HIPAA Security Rule Top Requirements

- Mandatory network segmentation
- Comprehensive asset inventory and network mapping
- 72-hour system restoration requirements
- Regular vulnerability scanning and penetration testing
- Enhanced risk analysis and management

# Executive Summary

The Department of Health and Human Services (HHS) has proposed significant updates to the HIPAA Security Rule for 2025, representing the first major overhaul in over a decade. Published on January 6, 2025, the proposed rule transforms network segmentation from an "addressable" specification to a mandatory requirement for healthcare organizations. This shift comes in response to the alarming rise in healthcare cyberattacks, with over 167 million patient records compromised in 2023 alone.

Key changes include mandatory technical controls for preventing lateral movement within networks, comprehensive asset inventory and network mapping requirements, 72-hour system restoration mandates following security incidents, regular vulnerability scanning and penetration testing, and enhanced risk analysis specifications. Traditional approaches like VLANs and static firewall rules will no longer suffice—organizations must implement dynamic, identity-based controls that adapt to modern healthcare environments.

The rule also strengthens workforce security management, requiring prompt notification when user access changes and annual verification of business associate security measures. These changes fundamentally alter how healthcare organizations approach cybersecurity, requiring a strategic shift from compliance-focused to risk-based security programs.

While the proposal has received industry criticism regarding implementation costs and timeframes, healthcare organizations should begin preparation now, as the final rule is expected by late 2025 or early 2026. Elisity's identity-based microsegmentation platform enables healthcare organizations to meet these requirements while maintaining operational efficiency and protecting patient care.

## Top New Requirements

- Network segmentation becomes mandatory rather than "addressable" under the new rule
- Organizations must implement technical controls to prevent lateral movement within networks
- 72-hour system restoration requirement following security incidents
- Required continuous monitoring and risk analysis capabilities
- Regular vulnerability scanning and penetration testing mandated

## Timeline

**January 6, 2025**
Proposed rule published

**March 7, 2025**
Comment period ends

**Today**
Organizations should begin planning implementation now to ensure compliance

**Late 2025 / Early 2026**
Final rule expected

# Meeting New HIPAA Security Rule Network Segmentation Requirements

The Department of Health and Human Services (HHS) has proposed significant updates to the HIPAA Security Rule for 2025, introducing mandatory network segmentation requirements and strengthening cybersecurity controls for healthcare organizations. With a compliance deadline approaching and cybersecurity challenges growing, healthcare organizations need effective solutions that can be implemented without disrupting critical care operations.

## Overview

### Understanding the HIPAA Security Rule

For the first time in over a decade, HHS has proposed major updates to the HIPAA Security Rule.

**Key changes include:**

- Mandatory network segmentation with technical controls
- Comprehensive asset inventory and network mapping requirements
- 72-hour system restoration requirements following incidents
- Regular vulnerability scanning and penetration testing
- Enhanced risk analysis and management specifications

## People

### Healthcare Teams Adapt Security Roles

From a people perspective, the new HIPAA Security Rule places greater emphasis on workforce security management and accountability. Organizations must implement more rigorous access control processes, including prompt 24-hour notifications when workforce member access changes. Security teams will need enhanced training to manage new requirements around incident response, compliance auditing, and security testing. The rules also strengthen requirements around business associate relationships, requiring annual verification of security measures and written certifications from subject matter experts, fundamentally changing how organizations manage their security partnerships and vendor relationships.

## Process

### Structured Documentation Builds Compliance Framework

Process changes form the backbone of the new requirements, with organizations needing to implement more structured and documented approaches to security management. Annual compliance audits become mandatory, along with detailed risk analyses that must be thoroughly documented. Organizations must maintain formal incident response plans with regular testing, establish standardized configuration management processes, and implement patch management programs with specific timelines for critical vulnerabilities. The rules require organizations to develop and maintain comprehensive documentation of all security measures, conduct regular effectiveness testing, and update security policies at least annually.

## Technology

### Technical Controls Prevent Lateral Movement

On the technology front, organizations must implement several new mandatory technical controls. Network segmentation becomes a required technical control to prevent lateral movement, while encryption must be deployed for all ePHI both at rest and in transit. Multi-factor authentication becomes mandatory across systems, with limited exceptions. Organizations must deploy enhanced monitoring capabilities, implement anti-malware protection, and maintain separate technical controls for backup and recovery of ePHI with 72-hour restoration requirements. Regular technical testing becomes mandatory, including vulnerability scanning every six months and annual penetration testing, supported by comprehensive asset inventory and network mapping tools to maintain visibility across the environment.

# Specific HIPAA Security Rule Requirements

## Asset Inventory and Network Mapping

Elisity's IdentityGraph™ revolutionizes how healthcare organizations approach asset management and network visibility. The platform continuously discovers and classifies all network-connected assets, providing real-time visibility into IT, IoT, OT, and IoMT devices across your environment. This comprehensive discovery process enriches device profiles with detailed context from multiple sources including Claroty/Medigate and Armis.

## System Recovery and Business Continuity

Modern healthcare environments require constant uptime and rapid recovery capabilities. Elisity's architecture fundamentally transforms how healthcare organizations approach system resilience and recovery. By leveraging existing network infrastructure and implementing granular, identity-based policies, the platform ensures critical systems remain available during both normal operations and recovery scenarios.

## Risk Analysis and Management

The 2025 HIPAA Security Rule mandates a more rigorous approach to risk analysis and management. Elisity's platform provides healthcare organizations with continuous risk assessment capabilities through real-time monitoring and analysis of network behavior. The IdentityGraph™ constantly evaluates device relationships, access patterns, and security posture changes, enabling organizations to maintain an accurate and current risk profile.

---

# Network Segmentation: A Core HIPAA Security Requirement

**The 2025 HIPAA Security Rule explicitly mandates network segmentation as a fundamental security control, marking a significant shift from previous guidance where segmentation was considered an addressable specification. Under the new requirements, healthcare organizations must implement technical controls that effectively segment their networks to protect electronic Protected Health Information (ePHI).**

Healthcare organizations must now implement segmentation controls that can adapt to dynamic clinical workflows while maintaining strict security boundaries. The requirement goes beyond traditional approaches like VLANs and static firewall rules, demanding solutions that can provide granular control over network access based on identity and context.

Traditional network segmentation approaches often fall short in meeting these new requirements, particularly in healthcare environments where clinical workflows cross traditional network boundaries and many devices cannot support endpoint security agents. Identity-based microsegmentation addresses these challenges by creating security policies based on the identity and context of users, devices, and applications rather than network location or IP addresses.

# Action Plan for CISOs Navigating the 2025 HIPAA Security Rule

As the first major update to the HIPAA Security Rule in over a decade approaches, healthcare security leaders need a clear strategy to meet these new requirements while maintaining operational efficiency. Here's a comprehensive action plan for CISOs and security architects in healthcare organizations:

| | |
|---|---|
| **Understand** the New HIPAA Security Rule Requirements | The 2025 HIPAA Security Rule introduces significant new cybersecurity requirements including mandatory network segmentation, encryption, multi-factor authentication, and specific timeframes for security testing. These changes reflect the evolving threat landscape and the need for stronger protection of electronic Protected Health Information (ePHI). Security leaders should carefully review the new requirements and assess their current security posture against these enhanced standards. |
| **Implement** Network Segmentation | The new rule specifically requires network segmentation to prevent lateral movement of threats within healthcare environments. Organizations must implement technical controls to segment their electronic information systems in a reasonable and appropriate manner. This approach helps contain potential breaches and prevents attackers from moving freely between different parts of the network, such as from a compromised point-of-sale system to an electronic health record system. |
| **Enhance** Device Visibility and Risk Management | Under the new rule, organizations must maintain comprehensive asset inventories and network maps. This includes developing and maintaining an accurate inventory of all technology assets and creating detailed maps showing how ePHI moves throughout the organization's systems. These documents must be reviewed and updated at least every 12 months or when significant changes occur in the environment. |
| **Meet** Compliance Deadlines and Requirements | The proposed rule introduces specific timeframes for security measures that organizations must follow. This includes implementing procedures to restore data within 72 hours of an incident, conducting vulnerability scans every six months, and performing annual penetration testing. Organizations must also conduct annual security audits to ensure ongoing compliance with these requirements. |
| **Integrate** Security Controls | The new requirements emphasize the need for comprehensive, integrated security controls. Organizations should focus on implementing solutions that work together seamlessly to provide complete coverage of their environment. This includes ensuring that security measures can effectively protect both modern and legacy systems while maintaining critical healthcare operations. |
| **Establish** Continuous Monitoring and Validation | The updated rule requires ongoing security validation and monitoring. Organizations must implement systems for continuous monitoring of network activity and regular testing of security controls. This includes maintaining detailed audit trails and implementing automated systems to detect and respond to potential security incidents. |
| **Plan** for Long-term Success | While meeting the initial compliance deadline is important, organizations need to develop a sustainable approach to security that can evolve with changing threats and requirements. **This includes:**<br><br>• **Creating a systematic approach to implementing new security controls, starting with the most critical systems**<br>• **Developing processes for regular review and updates of security measures**<br>• **Building internal expertise and capabilities for ongoing security management**<br>• **Establishing partnerships with vendors and service providers who understand healthcare's unique requirements**<br><br>Security leaders should approach these new requirements as an opportunity to strengthen their overall security program rather than viewing them simply as a compliance exercise. By taking a methodical, risk-based approach to implementation, organizations can build a more resilient security posture while meeting regulatory requirements. The changes to the HIPAA Security Rule represent a significant shift in how healthcare organizations must approach cybersecurity. Success will require careful planning, adequate resources, and a commitment to ongoing security improvement. Organizations should begin preparing now to ensure they can meet these enhanced requirements while maintaining efficient healthcare operations. |

# Elisity: Transforming Network Security for Healthcare

Elisity delivers identity-based microsegmentation that revolutionizes how healthcare organizations protect electronic Protected Health Information (ePHI). Our platform transforms your existing network infrastructure into a powerful Zero Trust enforcement engine, eliminating the need for new hardware or disruptive network changes.

## Discover All Users, Workloads, and Devices

Elisity provides continuous visibility into every user, workload, and device, identifying and mapping risks in real-time. It enriches this data by correlating metadata from asset databases, identity providers, and CMDBs while analyzing network flow data from switches to provide deep contextual intelligence and analytics.

This ensures security teams have a single, dynamic view of all connected entities, reducing blind spots and providing the confidence teams and the platform needs to implement secure access policies.

- **Automated discovery and profiling of all users, workloads, and devices**
- **Real-time asset inventory and network mapping through IdentityGraph™**
- **Integration with Claroty/Medigate and Armis for enhanced IoT/IoMT visibility**
- **Continuous monitoring and enrichment of device context**

## Control Least Privilege Access Policies

Users of the Elisity platform can create and simulate identity-based least privilege access policies. Elisity prevents lateral movement and enforces policies without relying on VLANs, ACLs, or endpoint agents. Policies are dynamically updated based on real-time intelligence, ensuring access controls remain in sync with user behavior, risk posture, and device compliance status.

- **Dynamic policy creation based on identity and context**
- **Granular access controls aligned with clinical workflows**
- **Real-time policy enforcement at the network edge**
- **Automated response to security posture changes**

## Implement, Scale, and Manage Microsegmentation

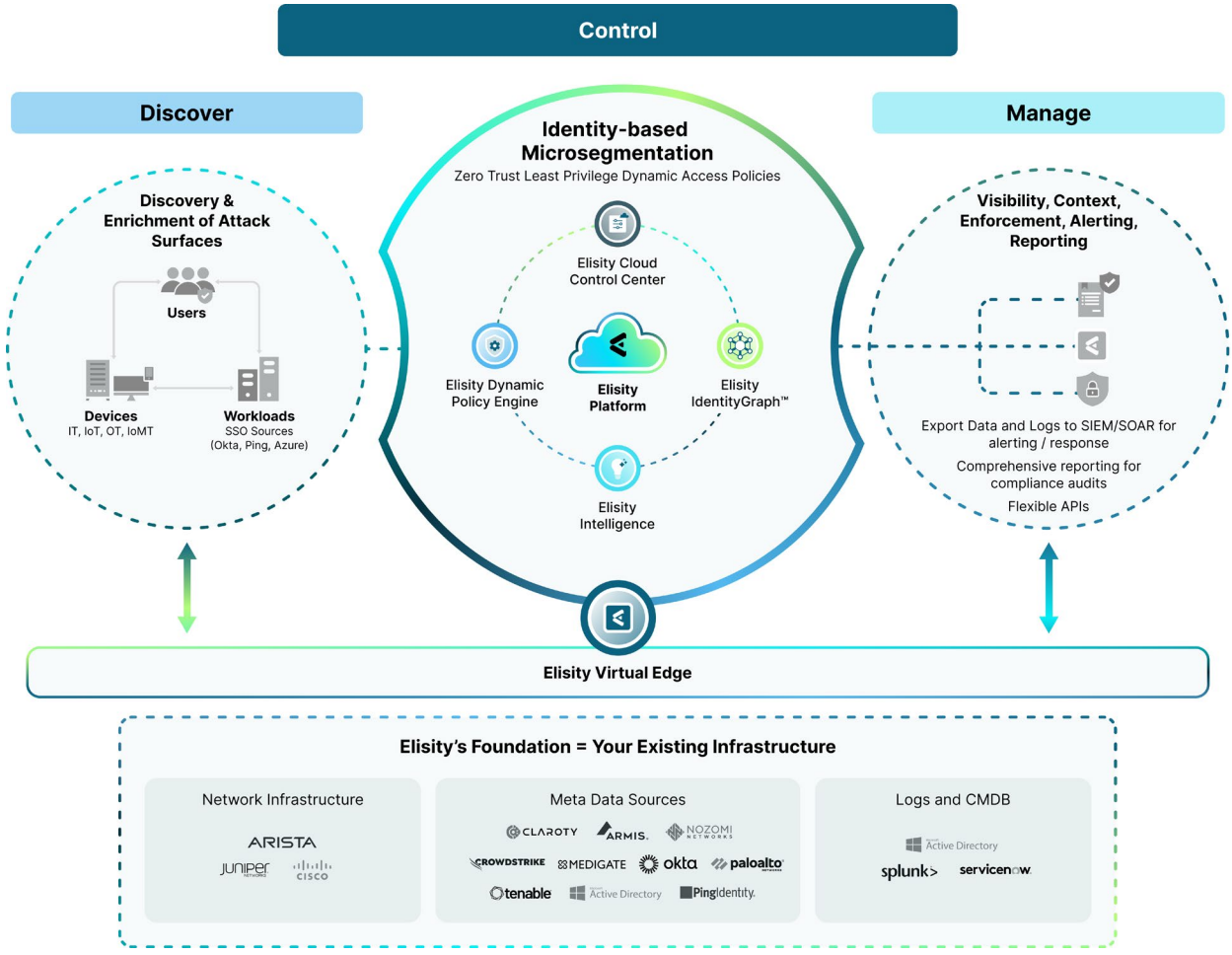
Elisity's microsegmentation platform deploys through the Cloud Control Center which transforms your existing network switches into policy enforcement points. The solution uses Distribution Zones to efficiently scale policy across thousands of devices based on hardware capabilities, while maintaining comprehensive audit logs for compliance reporting.

The Virtual Edge can be deployed as a hypervisor-hosted VM or container on supported Cisco Catalyst 9000 switches, leveraging existing infrastructure to enforce identity-based policies with continuous traffic-flow visibility. Through the Cloud Control Center, it ensures consistent policy distribution across multi-vendor environments without network changes or downtime.

- **Zero-downtime implementation using existing infrastructure**
- **Centralized policy management across all environments**
- **Integration with existing security tools and workflows**
- **Comprehensive audit and compliance reporting**

# Microsegmentation Architecture Overview

Elisity's platform leverages your current network and tech stack investments, providing a comprehensive Zero Trust security solution that spans Discovery, Control, and Management functions without requiring hardware or network changes, agents or complex deployments.




**Elisity's Approach to HIPAA Security Rule Compliance**

# Case Study: Bupa Cromwell Hospital

> “In my 30 years of working in technology and security, I’ve never delivered a product into an environment and got instant benefit like we did with Elisity and Claroty’s Medigate.”
>
> **Paul Haywood, CISO, Bupa**

Paul Haywood, CISO, Bupa

Bupa

## OVERVIEW

Bupa Cromwell Hospital’s Implementation of Elisity and Claroty’s Medigate

## CHALLENGE

Healthcare institutions like Bupa’s Cromwell Hospital are often at the forefront of cybersecurity, with a plethora of connected devices, highly sensitive patient data, and essential services. Medical devices like MRI and CT scanners often operate on legacy systems, making them challenging to protect with traditional IT security measures. Bupa Cromwell Hospital, a state-of-the-art facility in London specializing in complex procedures and advanced care, was keen to improve its security posture against a new wave of threats, without disrupting operations. Bupa Group CISO Paul Haywood emphasized the company’s dedication to patient data protection and its journey toward a cloud-dominant environment, which required effective management of policy and access.

## SOLUTION

To address these challenges, Bupa Cromwell Hospital partnered with Elisity and Medigate to develop an advanced security solution for their infrastructure management. Elisity provided identity-based microsegmentation for the existing access layer switching infrastructure, requiring no additional hardware or network downtime. The Identity Graph by Elisity created context for effective security policy management by understanding users, devices, apps, and their relationships on the network.

Medigate, on the other hand, offered award-winning device discovery and risk assessment capabilities. By integrating these two platforms, the team identified policy gaps and developed microsegmentation and least privilege access policies mapped to device classes and user groups. This integration streamlined device identification, asset management, and ongoing policy maintenance while reducing the risk of security breaches for medical and IoT devices.

## RESULTS

The Elisity and Medigate joint solution significantly benefited Bupa Cromwell Hospital. It delivered real-time visibility into medical devices, assessed vulnerabilities, and provided policy recommendations for efficient enforcement by Elisity. This streamlined policy management ensured a reliable approach to infrastructure management and protected patient information.

Cromwell Hospital CISO Alma Kucera reported that the implementation allowed them to manage traffic going into their medical devices and introduced layers of mitigation in defense and depth around the key risks identified.

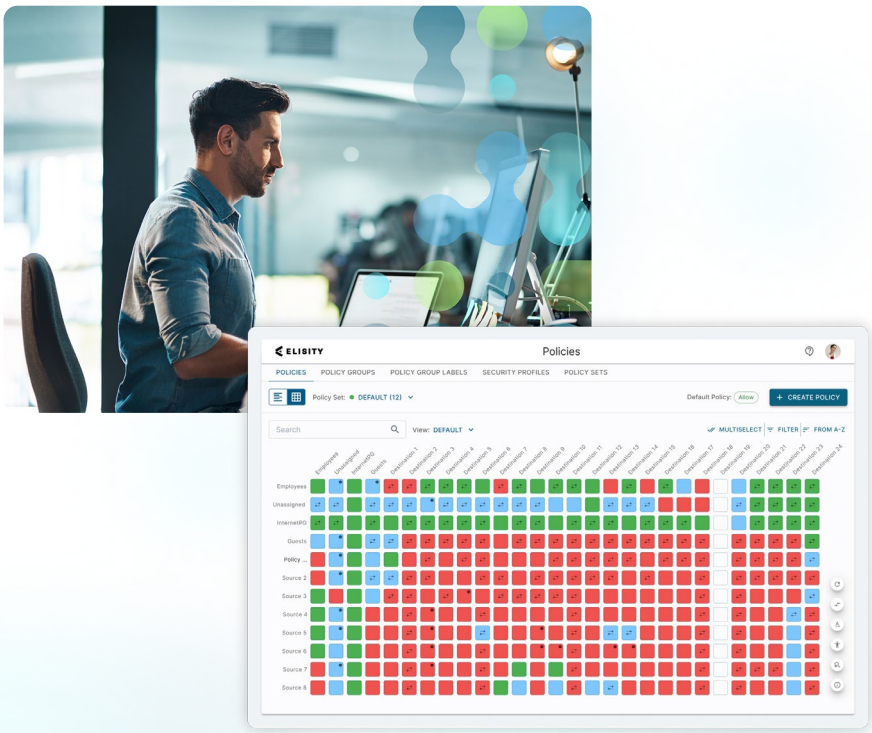
According to Paul Haywood, Bupa’s CISO, “In my 30 years of working in technology and security, I’ve never delivered a product into an environment and got instant benefit like we did with Elisity and Claroty’s Medigate.”

This case study is an excellent example of how combining identity-based microsegmentation with device discovery and risk assessment capabilities can significantly improve healthcare organizations’ cybersecurity posture, even in complex environments with a variety of connected and unmanaged devices.

# Network Segmentation Solution Requirements Recap

**Chief Information Security Officers (CISOs) and IT decision-makers within health-care organizations should:**

- Implement identity-based microsegmentation to meet new requirements
- Deploy solutions that can discover and classify all IT, IoT, OT, and IoMT devices
- Ensure segmentation solutions understand clinical workflows to avoid disrupting care
- Leverage existing network infrastructure rather than purchasing new hardware
- Choose solutions that provide continuous monitoring and automated policy enforcement
- Integrate with existing security tools and medical device security platforms
- Implement solutions that can be deployed without downtime




**Elisity Microsegmentation Policy Matrix Dashboard**

# Next Steps

The 2025 HIPAA Security Rule changes represent a significant shift toward mandatory network segmentation and enhanced cybersecurity controls. Elisity's identity-based microsegmentation platform enables healthcare organizations to meet these requirements while improving their security posture and maintaining operational efficiency.

Be sure to read our view of the Forrester Wave™ Microsegmentation Solutions Q3 2024 Healthcare IT View and learn how modern identity-based microsegmentation platforms like Elisity are enabling enterprises to reduce risks by preventing lateral movement and closing attack surface gaps.

To learn more about how the Elisity platform can help protect your organization meet Zero Trust goals and enhance your overall security posture, contact us for a conversation or a personalized demo.

## Let's Discuss Your Microsegmentation Plan — Learn More and BOOK A DEMO