Akamai Checklist

# From Proposal to Practice: The 2026 HIPAA Readiness Guide

Can you demonstrate Zero Trust enforcement across your environment?

## What's changing

The U.S. Department of Health and Human Services (HHS) Notice of Proposed Rulemaking (NPRM) **represents one of the most important shifts in healthcare cybersecurity** since the original Health Insurance Portability and Accountability Act (HIPAA) introduction.

The proposed 2026 HIPAA Security Rule shifts expectations toward operational proof of security controls. Regulators are focusing on whether controls are active, visible, and testable in real environments. Use this checklist to assess whether your environment can meet that standard.

## 1. Segmentation of ePHI systems

Many healthcare environments still rely on flat networks or basic VLAN segmentation, which makes it difficult to control or show how systems interact. Regulators are looking for clear separation of systems handling ePHI, along with visibility into how those systems communicate.

**Be able to verify that:**

- ☐ Systems that store or process ePHI are separated from other systems
- ☐ Unnecessary system-to-system traffic is blocked
- ☐ Only required connections between systems are permitted
- ☐ You can see which systems are communicating and how often

Akamai

## 2. Access control and MFA enforcement

MFA is often applied inconsistently, especially across legacy systems or exceptions. Access isn't always aligned with user roles. Regulators expect strong authentication and clear control over who can access sensitive systems.

**Be able to verify that:**

- ☐ MFA is required for all users accessing ePHI systems
- ☐ Login activity and access attempts can be reviewed
- ☐ Users only have access to systems required for their role
- ☐ Older systems or exceptions don't bypass MFA requirements

## 3. Asset inventory and network visibility

Many organizations rely on static inventories that don't reflect what's actually happening in the environment. Regulators expect a current, accurate view of all systems handling ePHI and how they interact.

**Be able to verify that:**

- ☐ You have a complete list of systems that store or process ePHI
- ☐ Unknown or unmanaged devices can be detected
- ☐ You can see how those systems communicate with each other
- ☐ Visibility extends across cloud, on-prem, and remote environments

## 4. Incident containment and lateral movement control

In many environments, isolating a compromised system requires broad shutdowns or manual intervention. Regulators expect organizations to limit how far an attack can spread, and to protect critical systems during an incident.

**Be able to verify that:**

- ☐ A compromised system can be isolated without shutting down large parts of the network
- ☐ Critical systems can remain protected during an incident
- ☐ Controls are in place to stop attackers from moving between systems
- ☐ Response actions can be executed quickly and consistently

## 5. Recovery readiness and 72-hour restoration capability

Recovery plans often exist but aren't regularly tested, and system dependencies aren't always well understood. Regulators expect organizations to restore critical systems within defined time frames.

**Be able to verify that:**

- ☐ Critical systems can be restored within required timelines
- ☐ System dependencies are understood before recovery begins
- ☐ Recovery procedures are tested regularly
- ☐ You have evidence from past tests showing recovery performance

## 6. Ability to demonstrate enforcement during audits

Many organizations have documentation in place, yet struggle to produce clear evidence that controls are working. Regulators expect organizations to demonstrate how controls are applied in real environments.

**Be able to verify that:**

- ☐ You can provide real examples of controls being enforced
- ☐ Controls are applied consistently across environments
- ☐ Logs or reports show system and user activity
- ☐ You can walk an auditor through how controls are applied

## Where to start

Start by validating what's actually happening in your environment today. Then focus on strengthening controls that improve visibility, restrict unnecessary access, and limit how far an incident can spread.

Akamai helps healthcare organizations improve segmentation, visibility, and access control enforcement across hybrid environments.

**Connect with our team to assess your current state and identify gaps.**

© 2026 Akamai Technologies | Support |
| Published 04/26