SILVERFORT

How to Comply with New York State Department of Health's Section 405.46 of Title 10 NYCRR with Silverfort

Executive Summary

Introduced by the New York State Department of Health (DOH) in 1999, 10 NYCRR 405.46 initially focused on protecting patient rights in hospital settings, particularly regarding the use of restraints and seclusion. This regulation evolved in response to pressing cybersecurity concerns. Currently, 405.46 requires healthcare facilities to implement strict cybersecurity measures, including data encryption, controlled access, and continuous electronic health records (EHR) monitoring. This ensures that hospitals maintain rigorous standards for protecting sensitive patient data, reinforcing both patient privacy and healthcare system resilience against cyber threats.

New York State’s New Cybersecurity Mandates for Hospitals: 10 NYCRR 405.46

The New York State Department of Health's regulation 10 NYCRR 405.46, effective October 2, 2024, mandates stronger cybersecurity protections across New York’s 195 general hospitals. Full compliance is required by October 2, 2025, though hospitals must begin reporting cybersecurity incidents within 72 hours as of October 2024. This regulation targets protection for patient health information (PHI) and personally-identifying information (PII) against cyber threats.

Key Components:

- **Cybersecurity Program:** Hospitals must implement a robust cybersecurity program that includes network monitoring, incident response, training, and policy development.
- **Chief Information Security Officer (CISO):** Hospitals are required to appoint a CISO, either as a direct employee or a third-party contractor, to oversee cybersecurity measures.
- **Testing and Vulnerability Assessments:** Regular testing, including scans and penetration assessments, is required to manage cybersecurity risks.
- **Audit Trails and Records:** Hospitals must maintain audit trails to detect and respond to cyber incidents and securely retain records.
- **Incident Response:** A detailed response plan is mandatory, with incident reporting to the Department of Health within 72 hours.
- **Access Control Measures:** Requirements include enforcing multifactor authentication (MFA) for external systems, limiting privileged account use, annual access reviews, and tailored cybersecurity training.

Mandates and State Support:

Annual Access Review: Hospitals must annually review and remove unnecessary user access, posing challenges for legacy accounts.

Funding and Insurance Impact: New York has allocated $500 million to support compliance, with potential impacts on cyber insurance terms.

Through these mandates, New York aims to strengthen healthcare cybersecurity and support hospitals in protecting patient data from evolving cyber threats.

Which Healthcare Services Are Required to Comply With Section 405.46 of Title 10 NYCRR

- General Hospitals
- Emergency Department Medical Staff
- Trauma Centers
- Pediatric Emergency Departments
- Mental Health Professionals in Emergency Settings
- EMS and Ambulance Providers (within the hospital context)
- Critical and Intensive Care Units (ICUs)
- Labor and Delivery Staff
- Pharmacists and Pharmacy Services in Emergency Departments
- Infectious Disease Control Personnel
- Administrative and Compliance Officers in Hospitals

Silverfort Unified Identity Security Platform

Silverfort equips hospitals to meet New York's new cybersecurity mandates with efficient, cost-effective solutions tailored to healthcare. It streamlines compliance through multi-factor authentication (MFA) and privileged access security controls which is essential for regulatory adherence. With rapid incident detection, Silverfort helps hospitals meet the 72-hour reporting requirement by swiftly identifying cybersecurity incidents.

Additionally, it supports thorough risk assessments and offers valuable tools for newly appointed CISOs to manage comprehensive security programs. Designed with healthcare environments in mind, Silverfort addresses industry-specific threats and prepares hospitals for future regulations by implementing scalable identity security controls that are aligned with security best practices.

Multi-Factor Authentication

Extend MFA protection to command-line access, legacy apps, IT infrastructure, and other critical resources that couldn't be protected before.

Continuous Monitoring

All-access requests are continuously monitored to detect anomalies and prevent malicious access in real-time.

Securing Privileged Users

Enforce MFA or access block policies on all privileged users, both human admins and service accounts.

Detect and Respond to Identity Threats

Detect common credential access, privilege escalation and lateral movement attacks, and respond automatically with real-time blocking.