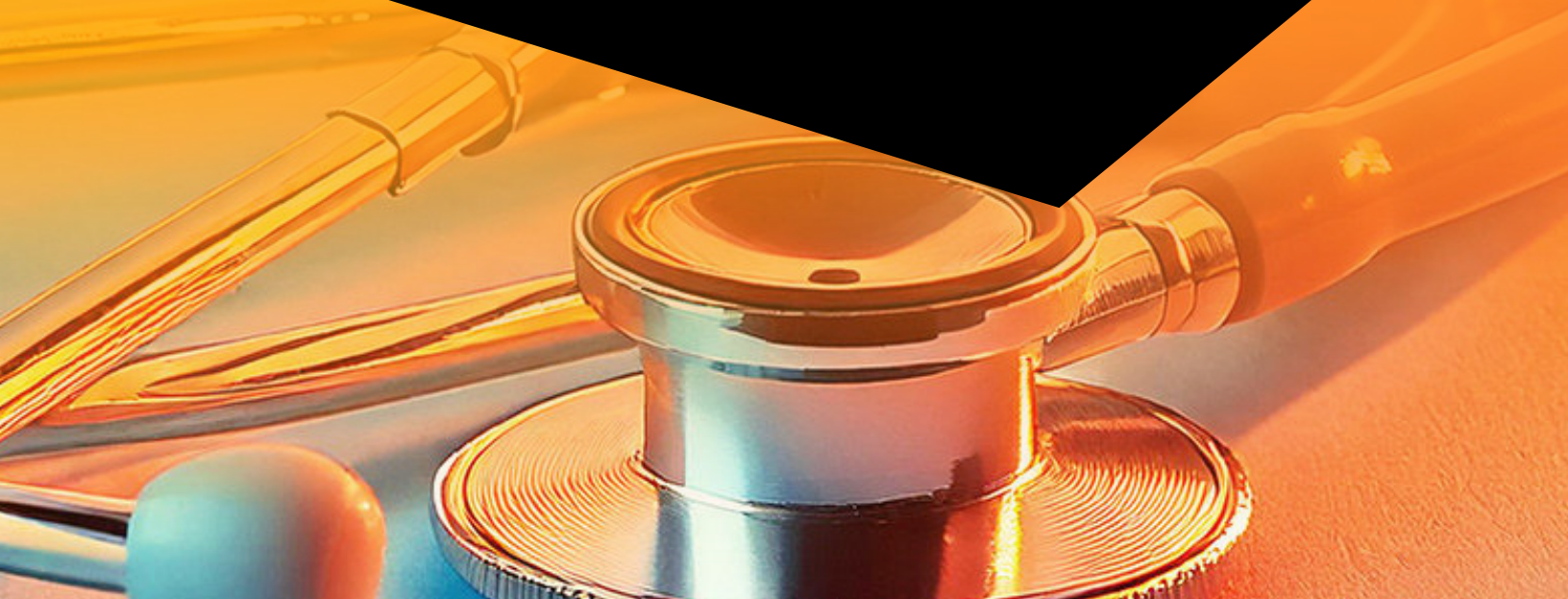
Silverfort

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

Whitepaper



# 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

The New York State Department of Health announced in early October 2024 new regulations to 10 NYCRR 405.46 which mandated 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 2, 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 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 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**

Gain comprehensive visibility into all authentication and access attempts, monitor and review them continuously to detect anomalies and prevent malicious access in real-time.

**Securing privileged users**

Discover, classify, and enforce least privilege and Just-In-Time (JIT) access policies for all your privileged users.

**Detect and respond to identity threats**

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

# Mapping Silverfort Capabilities to Section 405.46 of Title 10 NYCRR

## Cybersecurity program

**Section 405.46 (c)** establishes the requirements for hospitals to have a cybersecurity program and defines protocols, procedures, and core functions of such program.

| DOH regulation | Silverfort security controls |
|---|---|
| **(c) 1.** Each hospital shall establish within its policies and procedures a cybersecurity program based on the hospital's risk assessment. | Using Silverfort's risk report functionality, hospitals can generate a summary of their identity security posture in just one click, providing security teams with deep insight into issues that need to be resolved, and guiding the development of your cybersecurity program. |
| **(c) 2. (i)** The cybersecurity program shall be designed to perform the following core functions: identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the hospital's information systems and the continuity of the hospital's business and operations; | Silverfort detects both internal and external identity security risks by continuously monitoring access activity across all users and devices, using behavior analytics to detect anomalies that could signal potential threats. |
| **(c) 2. (ii)** Use defensive infrastructure and the implementation of policies and procedures to protect the hospital's information systems, the continuity of the hospital's business and operations, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts; | With Silverfort, hospitals can configure access policies based on user rules for both on-prem and cloud environments. These policies can enforce alerting, MFA, or block access upon insecure authentication to protected healthcare systems. |
| **(c) 2. (iii)** detect cybersecurity events; | Silverfort monitors all identity traffic and authentication activities in one place and provides centralized visibility into every authentication and access request across all users, service accounts and resources in an hybrid environment. With complete visibility across all user activity, Silverfort can alert hospitals of the detection of a possible cybersecurity event. |
| **(c) 2. (iv)** respond to identified or detected cybersecurity events to mitigate any negative effects; | Silverfort assists with incident response by providing detailed logs of all authentication and access activities. This allows security teams to respond and understand what occurred during an incident and determine the root cause. Using comprehensive data on user access requests and behaviors, Silverfort facilitates a comprehensive investigation and understanding of the events leading up to and during a security incident. Silverfort's real-time monitoring capabilities detect anomalies and suspicious activities, providing insights into the course of an incident. As a result of this detailed analysis, it is possible to pinpoint the exact nature and origin of the problem. |
| **(c) 2. (v)** recover from cybersecurity events and incidents and restore normal operations and services; | Silverfort aids in recovering from cybersecurity incidents by identifying compromised accounts and risky access attempts in real time, allowing security teams to quickly isolate affected systems and revoke access as needed. Silverfort's integration with incident response workflows also facilitates seamless recovery by automating threat mitigation actions, helping hospitals restore normal operations efficiently and securely. |

## Cybersecurity program (continued)

| DOH regulation | Silverfort security controls |
|---|---|
| **(c) 3.** Each hospital's cybersecurity program shall include policies and protocols to limit user access privileges to information systems that provide access to nonpublic information. Each hospital shall periodically review such access privileges, and such access privileges shall be based on the hospital's risk assessment, and other State and Federal laws, including but not limited to the administrative, physical, and technical safeguards under HIPAA. | Silverfort can enforce **least privilege** access and **just-in-time (JIT)** policies to ensure that users only have access to hospital information systems when necessary and only to the specific resources required for their roles. Silverfort minimizes the risk of unauthorized access to sensitive non-public information. With Silverfort's visibility capabilities, hospitals gain a complete picture of all user activities to determine which policy they would fall under. With the help of Silverfort, hospitals can conduct periodic reviews of user privileges so that they can ensure their access policy is up-to-date and in compliance with industry standards. |
| **(c) 6.** Each hospital's cybersecurity program shall implement security measures and controls, including encryption, to protect nonpublic information held or transmitted by the hospital, both in transit over external networks and at rest, which takes into account necessary controls identified in the hospital's risk assessment. | Silverfort enforces access and security controls to all users and their access requests to resources, including where they involve insecure authentication protocols. By applying concrete security controls to all users, Silverfort helps prevent any unauthorized access in real time, ensuring only authorized users can gain access to specific resources. |

## Cybersecurity policy

**Section 405.46 (d)** defines the cybersecurity policies that general hospitals will need to create and the topics that should be considered after a risk assessment has been performed.

| DOH regulation | Silverfort security controls |
|---|---|
| **(d) 1.** Each hospital shall maintain and implement policies and procedures for the protection of its information systems and nonpublic information stored on those information systems, and the continuity of the hospital's business and operations, in accordance with the hospital's risk assessment and applicable State and Federal laws and regulations. The hospital shall be responsible for developing and enforcing the hospital's cybersecurity policy, and overseeing and implementing the hospital's cybersecurity program, established pursuant to subdivision (c) of this section. | Silverfort enables organizations to enforce the use of unique credentials for every user authorized to store, process, or transmit Criminal Justice Information (CJI). Through integration with existing identity management systems, it ensures all users, including administrators, maintain secure access to systems and networks handling CJI. With Silverfort, user identities can be centrally controlled, which ensures only authenticated and uniquely identified individuals can access sensitive systems, which maintains the integrity and security of CJI. |

## Audit trails and records maintenance

**Section 405.46 (g)** outlines the audit trails and records maintenance and retention requirements of a general hospital's cybersecurity program.

| DOH regulation | Silverfort security controls |
|---|---|
| **(g) 1.** Each hospital shall securely maintain systems that are designed to support normal operations and obligations of the hospital. Records pertaining to systems design, security, and maintenance supporting such normal operations shall be maintained for a minimum of six years. | Silverfort provides hospitals with the ability to securely maintain their systems by continuously monitoring all user activities and requests for access, enforcing access controls, and ensuring that only authorized users have access to the resources they are entitled to. Furthermore, Silverfort's detailed access logs and reporting capabilities facilitate the maintenance of security records related to system design, access, and maintenance, simplifying compliance with the six-year record-keeping requirement. |
| **(g) 2.** Each hospital shall also securely maintain systems to include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operations of the hospital, and cybersecurity incidents as defined herein. Records pertaining to such audit trail systems shall be maintained for a minimum of six years. | Silverfort provides an in-depth identity inventory that displays the types of users and resources in the environment as well as security weaknesses. With Silverfort, all access events across their systems are logged and monitored, enabling quick detection and response to security threats that could negatively impact hospital operations. Audit logs can be securely stored and accessed as needed, implifying compliance with the six-year retention requirement. |

## Risk assessment

**Section 405.46 (h)** sets forth the requirements for cybersecurity risk assessments and the considerations for policies and procedures relative to those risk assessments.

| DOH regulation | Silverfort security controls |
|---|---|
| **(h) 1.** Each hospital shall conduct an accurate and thorough annual risk assessment of the hospital's potential risks and vulnerabilities to the confidentiality, integrity, and availability of nonpublic information, such as electronic protected health information, held by the hospital, and the continuity of the hospital's business and operations, as well as information systems sufficient to inform the design of the cybersecurity program as required by this section. Such risk assessment shall be updated as reasonably necessary, and no less than annually, and address changes to the hospital's information systems, nonpublic information or business operations supported by those 13 information systems. | Silverfort can help hospitals conduct a risk assessment which provides a summary of an organization's identity security posture in a single click. As a result, security teams are provided with clear insights into issues that need to be addressed. Silverfort provides detailed guidance on how to mitigate every detected risk.<br><br>Additionally, the risk assessments detect weaknesses in passwords and authentication-related vulnerabilities across organizational systems. By continuously monitoring authentication mechanisms, Silverfort can identify weak or compromised passwords as well as poor authentication practices. As a result, hospitals are able to proactively detect and mitigate weaknesses while maintaining secure access controls across their systems. With a more data-driven approach, hospitals can make more informed decisions about where to focus security efforts. |

## **Risk assessment** (continued)

| DOH regulation | Silverfort security controls |
|---|---|
| **(h) 2.** The risk assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall, at a minimum include:<br>**(i)** criteria for the evaluation and categorization of identified cybersecurity risks, vulnerabilities, and threats facing the hospital;<br>**(ii)** criteria for the assessment of the confidentiality, integrity, security and availability of the hospital's information systems and nonpublic information, including the identification and adequacy of existing controls in the context of identified risks, the determination of the likelihood of threat occurrence and the determination of the potential impact on threat occurrence, and the determination of the level of risk;<br>**(iii)** requirements describing how identified risks and threats will be mitigated or accepted based on the risk assessment and how the cybersecurity policies and programs will address the risks. | Silverfort can help conduct comprehensive risk assessments by automating processes that align with hospitals' documented policies and procedures. Silverfort evaluates and categorizes identity-based risks, vulnerabilities, and threats with predefined criteria, ensuring that security teams have a clear framework for risk classification. When assessing the confidentiality, integrity, security, and availability of information systems, Silverfort helps determine the likelihood and potential impact of threats on hospital systems, providing real-time insight into the adequacy of existing access controls. |

## Security policies for third-party service providers

**Section 405.46 (j)** sets forth the policies for third-party service providers of cybersecurity programs.

| DOH regulation | Silverfort security controls |
|---|---|
| **(j) 1.** Each hospital shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers. Such policies and procedures shall be based upon the hospital's risk assessment and shall, at a minimum, address the following:<br>**(i)** the identification and baseline assessment (if applicable) of third-party service providers; and<br>**(ii)** minimum cybersecurity practices required to be met by such third-party service providers in order for them to do business with the hospital. | Silverfort provides hospitals with the ability to manage and control all third-party and supply-chain access by enforcing access policies to all third-party users. Silverfort ensures that only authorized personnel can access critical systems and data by enforcing precise access controls and multifactor authentication for third-party users.<br><br>Additionally, Silverfort helps hospitals conduct a baseline assessment of third-party providers, identifying potential risks and monitoring access patterns to detect unusual or unauthorized activities. |

## Identity and access management

**Section 405.46 (k)** sets forth the requirements for identity and access management.

| DOH regulation | Silverfort security controls |
|---|---|
| **(k) 1.** Each hospital shall use multi-factor authentication, risk-based authentication, or other compensating control to protect against unauthorized access to nonpublic information or information systems. | Silverfort can enforce MFA on any access request, whether on-prem, cloud, remote, or third-party, from regular users to privileged admins. In an Active Directory (AD) environment, Silverfort can enforce MFA and block access policies on any LDAP/S, NTLM, and Kerberos authentications. This expands the scope of MFA protection to a wide array of resources and access methods that couldn't have been protected before, such as command-line tools, legacy applications, IT infrastructure, and more.<br><br>Silverfort ensures no access is granted based on passwords alone, and users are required to authenticate through MFA to verify that they are who they claim to be. |
| **(k) 2.** Multi-factor authentication shall be utilized for any individual accessing the hospital's internal networks from an external network, unless the hospital's CISO has approved in writing the use of compensating controls. | Silverfort can enforce MFA protection on all remote access to on-prem and cloud systems and on any third-party application accessed on-prem or via a cloud directory. |
| **(k) 3.** Each hospital shall limit user access privileges to information systems that provide access to nonpublic information to only those necessary to perform the user's job; | Silverfort allows hospitals to enforce security controls on all users, including privileged users, to ensure they are only granted access when necessary. In order to prevent unauthorized access, Silverfort offers security controls such as Multi-Factor Authentication (MFA) and access denied policies.<br>Additionally, hospitals can use Silverfort to implement **least privilege** and **Just-In-Time (JIT)** access policies to accounts to grant access only when needed minimizing persistent access risks and reducing the overall attack surface. |
| **(k) 4.** Each hospital shall separate non-privileged and privileged accounts; | By enforcing role-based access controls and adaptive policies tailored to each account type, Silverfort helps hospitals maintain a clear separation between non-privileged and privileged accounts. Silverfort continuously monitors access activity, ensuring that privileged accounts are used only for necessary functions and are strictly controlled.<br><br>By automatically identifying and segmenting all types of accounts, Silverfort helps hospitals minimize risk exposure, prevent unauthorized privilege escalation, and more. |
| **(k) 5.** Each hospital shall limit the number of privileged accounts and limit the access functions of privileged accounts to only those necessary to perform the user's job; | Silverfort enables hospitals to easily manage and control privileged accounts by **enforcing least privilege and JIT policies** that restrict access functions to only what is necessary for each user's role. Through real-time monitoring and automated policy adjustments, Silverfort can **automatically discover and classify the number** of privileged accounts in use.<br><br>This ensures that these accounts are only granted the specific access required for essential job functions. |

## Identity and access management (continued)

| DOH regulation | Silverfort security controls |
|---|---|
| **(k) 7.** Each hospital shall periodically, but at a minimum annually, review all user access privileges and remove or disable accounts and access that are no longer necessary; | Silverfort can help conduct comprehensive risk assessments by automating processes that align with hospitals' documented policies and procedures. Silverfort evaluates and categorizes identity-based risks, vulnerabilities, and threats with predefined criteria, ensuring that security teams have a clear framework for risk classification. When assessing the confidentiality, integrity, security, and availability of information systems, Silverfort helps determine the likelihood and potential impact of threats on hospital systems, providing real-time insight into the adequacy of existing access controls. |
| **(k) 9.** Each hospital shall promptly terminate access following departures. | Silverfort continuously monitors all user activities and access requests across the environment. This monitoring ensures that any changes in access rights or user roles are promptly detected. When a user leaves the organization, Silverfort's access policies will revoke all access for that user. This will prevent the user from gaining access to any resources. |

## Training and monitoring

**Section 405.46 (l)** sets forth the requirements for training and monitoring of the cybersecurity program

| DOH regulation | Silverfort security controls |
|---|---|
| **(l) 1.** Implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, nonpublic information by such authorized users. | Silverfort assists hospitals in implementing risk-based policies and security controls that continuously monitor authorized user activity and detect attempts to compromise nonpublic information. By leveraging the user's authentication activity and running real-time behavior analysis, Silverfort identifies unusual activity patterns and access attempts that deviate from typical behavior, allowing security teams to quickly respond to potential threats. |

## Incident response plan

**Section 405.46 (m)** defines the requirements for an incident response plan in the event of a cybersecurity incident.

| DOH regulation | Silverfort security controls |
|---|---|
| **(m) 1.** As part of its cybersecurity program, each hospital shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity incident materially affecting the confidentiality, integrity or availability of the hospital's information systems or the continuing functionality of any aspect of the hospital's business or operations. | Silverfort supports hospitals in building an effective incident response plan by providing real-time detection and rapid containment capabilities for cybersecurity incidents. Using Silverfort, the hospital's IR team can detect suspicious access patterns and immediately enforce strict access controls, minimizing the spread and impact of incidents. Silverfort's detailed logs and reports offer critical insights into incident analysis and recovery. This enables hospitals to swiftly restore normal operations while facilitating effective remediation and strengthening security overall. |

## Department reporting

**Section 405.46 (n)** defines the reporting requirements for a general hospital during a cybersecurity incident.

| DOH regulation | Silverfort security controls |
|---|---|
| **(n) 1.** The hospital or their designee shall notify the department as promptly as possible, but no later than 72 hours after determining a cybersecurity incident, as defined herein, has occurred, in a manner prescribed by the department. Notification to the department under this section does not replace any other notifications required under State or Federal laws or regulations. | Silverfort's advanced monitoring and detection capabilities enable hospitals to quickly identify and respond to cybersecurity incidents, supporting the 72-hour reporting requirement. Silverfort provides real-time alerts for suspicious activities and potential breaches, which enables security teams to quickly assess and categorize incidents. Silverfort's detailed incident logs and automated reporting tools streamline the notification process, allowing hospitals to gather and transmit critical information within the required time frame. This proactive approach enables hospitals to meet regulatory requirements effectively, minimizing response delays and supporting timely communication with authorities. |
| **(n) 2.** Each hospital shall maintain and submit for examination, in such time and manner and containing such information, as the department determines to be necessary, including but not limited to any and all documentation, such as records, schedules, reports, and data required and supporting the required documentation by this section. All such documentation must be maintained for a minimum of six years. | Silverfort assists hospitals in maintaining and organizing the necessary documentation for regulatory compliance by automatically logging and storing detailed records of all access events, security incidents, and related activities.<br><br>Silverfort enables long-term storage and secure archiving of these records, ensuring they are accessible and preserved for the required minimum of six years. This capability simplifies compliance with documentation standards and allows hospitals to efficiently provide supporting data for audits or regulatory review. |