Clearwater | Holland & Knight

New York Hospital Cybersecurity:

A Look at the Proposed Regulations, Implementation, & Grant Impact

Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording and final slides shared within 48 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Agenda

- Introductions
- A Review of the Proposed Regulations
  - What we know
  - How it differs from HIPAA
  - Potential pitfalls for hospitals
- Timeline and Implementation
- Grant Money
  - What we know about who might qualify
  - What you can do now
- Resources

Jon Moore

Jon Moore, MS, JD, HCISPP

Chief Risk Officer and Senior Vice President Consulting and Customer Success

- 25+ Years Executive Leadership, Technology Consulting and Law
- 14+ Years Data Privacy & Security
- 10+ Years Healthcare
- Former PwC Federal Healthcare Leadership Team
- Former IT Operational Leader PwC Federal Practice
- BA Economics Haverford College, MS E-Commerce Carnegie Mellon University, JD Dickinson Law Penn State University, HCISPP
- Speaker and Published Author on Security, Privacy, IT Strategy and Impact of Emerging Technologies

Mark Francis

Mark Francis

Partner | New York | Data Strategy, Security & Privacy

- Tech and data lawyer working on cybersecurity, privacy, intellectual property, data eco-systems, artificial intelligence and other emerging tech
  - Counseling and compliance
  - Services agreements and tech transactions
  - Crisis management and incident response
  - Litigation and regulatory investigations
- Governance Committee Chair, New York Metro InfraGard
- Data Privacy and Integrity Advisory Committee (DPIAC), Department of Homeland Security

HK https://www.hklaw.com/en/professionals/f/francis-mark-h

https://www.linkedin.com/in/markhfrancis/

Clearwater | Holland & Knight

Hospital Cybersecurity Requirements

- Announced by Governor Hochul on Nov. 13, 2023: Adds Section 405.46 to Title 10 NYCRR
- Subject to approval by the NYS Public Health and Health Planning Council ("PHHPC")
  - PHHPC discussed the regulations on November 16, 2023, and will revisit them on January 25, 2024
- Key changes intended to supplement the HIPAA Security Rule:
  - Broader scope of covered information
  - Requires a CISO and qualified personnel/contractors
  - Prescriptive security control requirements (e.g., MFA)
  - Annual risk assessment; audit trails and record keeping requirements
  - Report material adverse cyber incidents to the NYS Department of Health within 2 hours
- Hospitals can apply for state funding ($500M allocated in the FY 2024 budget) to upgrade their cybersecurity programs for the new requirements

Need and Benefit of Legislation

The legislative objectives of PHL Article 28 include the protection of the health of the residents of the State by promoting the efficient provision and proper utilization of high-quality health services at a reasonable cost.

Healthcare Targeted

The healthcare industry is one of the most targeted communities for cybersecurity scams and breaches due to the significant amount of sensitive and financially lucrative information healthcare facilities collect.

Hospitals Particularly Vulnerable

Cybersecurity events at hospitals can have significant, far-reaching, and long-term impacts to the provision of patient care and operation of the facility.

Benefits of Regulation

These regulations will ensure hospitals are required to maintain a minimum level of readiness to prepare for, respond to, and quickly recover from cybersecurity incidents.

Organizations Subject to the Regulations

Section 405.46 (a) identifies all general hospitals in New York State as subject to the regulations.

"This section shall apply to all general hospitals licensed pursuant to article 28 of the Public Health Law, referred to throughout this section as 'hospitals.'"

Impacted organizations:

- **15 Small Hospitals** (<10 Acute Care/ICU Beds)
- **62 Medium Hospitals** (10-100 Acute Care/ICU Beds)
- **114 Large Hospitals** (>100 Acute Care/ICU Beds)

Important Terms Defined

Section 405.46 (b) defines key terms, including:

(5) "Cybersecurity incident" means a cybersecurity event that:

i. has **a material adverse impact** on the normal operations of the hospital, or;

ii. has a **reasonable likelihood of materially harming** any material part of the normal operation(s) of the covered entity; or

iii. results in the **deployment of ransomware within a material part** of the hospital's information systems.

(8) "Nonpublic information" means all electronic information that is not publicly available information and is:

i. a hospital's **business-related information**, the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of such hospital;

ii. any information concerning a natural person which because of name, number, personal mark, or other identifier can be used to identify such natural person. This includes any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired, in combination with any one or more of the following data elements: . . .

(emphasis added)

Cybersecurity Program Requirements

Section 405.46 (c) defines protocols, procedures, and core functions of a hospital cybersecurity program

	Element	Summary Description
1	Program Based on Risk	Establish within its policies and procedures a cybersecurity program based on the hospital's risk assessment.
2	Supplement HIPAA	Supplement HIPAA and shall not replace any provisions of the HIPAA Security Rule (45 CFR part 160 and subparts A and C of part 164).
3	Core Functions	Identify risks, establish defensive infrastructure, policies and procedures, detect events, respond to events, recover from events and incidents, fulfill statutory and regulatory obligations.
4	Limit User Access	Limit user access privileges to information systems that provide access to nonpublic information.
5	Secure Development Practices	Procedures for secure development applications developed by hospital and for evaluation, assessing and testing third-party developed applications.
6	Secure Disposal of Info	Policies and procedures for the secure disposal, on a periodic basis, of any nonpublic information identified.
7	Security Controls (Encryption)	Implement security measures and controls, including encryption, to protect nonpublic information held or transmitted by the hospital.

Cybersecurity Policy and Procedures

Section 405.46 (d) requires policies based on a risk assessment covering a large scope of cyber topics

"Maintain and implement policies and procedures... Developed by the CISO and hospital information security/information technology staff"

"[C]ybersecurity policy, upon recommendation by the CISO shall be approved by the hospital's governing body"

Cybersecurity policies shall be based on hospital's risk assessment and at a minimum address the following topics:

i. Data governance and classification
ii. Asset inventory and device management
iii. Access controls and identify management
iv. Business continuity and disaster recovery planning
v. Systems operations and availability concerns
vi. Systems and network security
vii. Systems and network monitoring
viii. Systems and application development and quality assurance
ix. Physical security and environmental controls
x. Patient data privacy
xi. Vendor and third-party service provider management
xii. Risk assessment as defined in subdivision (h)
xiii. Training and monitoring as defined in subdivision (l)
xiv. Overall incident response as defined in subdivision (m)

Chief Information Security Officer

Section 405.46 (e) requires a Chief Information Security Officer responsible for creation, implementation, and oversight of the cybersecurity program

Designate CISO	Employee or Vendor	Responsible for Enforcement	Annual Report
Designate an individual from senior- or executive-level staff, qualified in training, experience, and expertise, to serve as the hospital's Chief Information Security Officer	CISO may be an employee of the facility, or an employee of a third-party or contract vendor. If the CISO is a third-party, the governing body, shall approve the contract on an annual basis	CISO shall be responsible for developing and enforcing the hospital's cybersecurity policy and overseeing and implementing the hospital's cybersecurity program	CISO of each hospital shall report in writing, at least annually to the hospital's governing body, on the hospital's cybersecurity program and material cybersecurity risks

Testing and Vulnerability Assessment

Section 405.46 (f) requires testing and vulnerability assessments

"Cybersecurity program for each hospital shall include monitoring and testing, developed in accordance with the hospital's risk assessment, designed to assess the effectiveness of the hospital's cybersecurity program and assess changes in information systems that may create or indicate vulnerabilities."

Minimum Requirements:

i. Penetration testing of the hospital's information systems by a qualified internal or external party at least annually

ii. Automated scans or manual or automated reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the hospital's information systems based on the risk assessment

Audit Trails and Record Maintenance and Retention

Section 405.46 (g) outlines audit trails, records maintenance and retention requirements

System Documentation

Records pertaining to systems design, security, and maintenance supporting such normal operations shall be maintained for a minimum of six years.

Audit Trails

Securely maintain . . . audit trails designed to detect and respond to cybersecurity . . . and cybersecurity incidents as defined herein. Records pertaining to such audit trail systems shall be maintained for a minimum of six years.

Design Based on Risk Assessment

Designs for the security systems and audit trails required pursuant to paragraphs (1) and (2) of this subdivision shall be based on the hospital's risk assessment.

Risk Assessment

Section 405.46 (h) proscribes risk assessment requirements

Scope and Frequency

- Annual risk assessment of risks and vulnerabilities to CIA of nonpublic information
- Updated as reasonably appropriate but no less frequently than annually and address changes in information, systems and business processes
- Allow for revision in controls to respond to technological advancements
- Risk assessments performed for other regulatory purposes ok as long as meet requirements

Policy and Procedures

- Criteria for categorization of risks, vulnerabilities and threats
- Criteria for confidentiality, integrity, security and availability of systems and information including identification and adequacy of controls, likelihood and impact of threat occurrence and determination of level of risk
- Requirements on how risks and threats will be mitigated or accepted based on the risk assessment and how the policies and programs will address risks

Cybersecurity Personnel

Section 405.46 (i) provides cybersecurity personnel requirements

Requirement	Description
Sufficient Personnel	Utilize qualified cybersecurity personnel of the hospital, an affiliate or a third-party service provider sufficient to manage the hospital's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in subdivision (c) of this section and in accordance with the hospital's risk assessment
Third-Party Provider	Each hospital may utilize an affiliate or qualified third-party service provider to assist in complying with the requirements set forth in this section

Policies for Third-Party Service Providers

Section 405.46 (j) provides requirements for third-party service providers

Requirement	Description
Policies and Procedures	• Identification and baseline assessment • Minimum cybersecurity practices required to be met by third-parties to do business with hospital
Due Diligence Guidance and Contractual Provisions	• Provider's policies and procedures for access controls are consistent with industry standards • Policies and procedures for use of encryption or another method for information in transit or at rest • Notice to be provided to hospital in the event of cybersecurity incident impacting hospital systems or nonpublic information • Representations and warranties addressing third-parties' cybersecurity policies and procedures that relate to hospital's nonpublic information or information systems

Risk-Based Authentication

Section 405.46 (k) includes multi-factor authentication (MFA) procedures

MFA or Risk Based Authentication	Access from External Network
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	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

Training and Monitoring

Section 405.46 (l) requires employee training and system monitoring

Activity Monitoring

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

Regular Cybersecurity Awareness Training

Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the hospital in its risk assessment, which may include annual phishing exercises and training/remediation for employees

Incident Response Plan

Section 405.46 (m) imposes incident response plan requirements

"[E]ach 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."

The IRP must address:

- Goals of plan
- Roles, Responsibilities and contact info and levels of decision-making authority
- External and internal information sharing about incidents
- Identification of requirements for remediation of weaknesses in systems or controls.
- Internal processes for responding to an event
- Documentation and reporting of events and incident response activities
- Evaluation and revision of plan following an even

Department Reporting

Section 405.46 (n) imposes new regulatory reporting and record-keeping requirements

2 Hour Reporting

CISO or their designee shall notify the department within two hours of a determination that a cybersecurity incident, as defined herein, has occurred and has had a material adverse impact on the hospital, in a manner prescribed by the department

Maintain and Submit Documentation

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 documentation. . . supporting the required documentation by this section

Remediation Documentation

[H]ospital shall document the identification and the remedial efforts planned, and underway, . .. Such documentation must be available for inspection by the department, in such time and manner as prescribed by the department

Compliance Period

Regulation will become effective upon publication of the Notice of Adoption in the State Register:

- Section 405.46 (p) provides hospitals one (1) year from the date of adoption to comply with the new regulatory requirements

- EXCEPT that hospitals will need to immediately begin reporting incidents to the DOH as required by 405.46 (n)

Costs to Regulated Parties

The costs associated with the implementation by regulated facilities are expected to vary significantly due to the varying levels of cybersecurity programs and policies hospitals currently have in place

	Implementation	Ongoing
Small Hospital	$250k-$10M	$50k - $200k/year
Medium Hospital	$250k-$10M	$200k - $500k/year
Large Hospitals	$250k-$10M	$2M year

Grant Funding

The Department will soon be issuing a request for application for a new $500M Health Care Technology Capital program

Funding for this program was appropriated in the FY24 budget, with the intention of supporting facilities' technological needs, including for cybersecurity purposes

The funding is intended to help facilities cover the costs of coming into compliance with the new regulations

How to Get Started

Given the immediate change in incident reporting and short timeline for compliance, covered organizations should begin preparing the road to compliance

1. Update Incident Response to account for 2HR reporting and documentation requirement
2. Conduct a gap analysis of existing program relative to the new requirements
3. Create an action plan to come into compliance within the applicable timeline
    - ❑ Identify anticipated costs (internal resources, new technology, external consulting/compliance/legal)
    - ❑ Apply for grant; budget internally
4. Execute action plan and track 1-year enforcement deadline
    - ❑ Policy and procedure changes
    - ❑ Operational changes
    - ❑ Vendor changes (contractual/technical)

Additional Resources

- Governor Hochul Announces Proposed Cybersecurity Regulations for Hospitals Throughout New York State
- Draft 405.46 Title 10 Regulations
- Notice New York State Register (Copy of Draft Regulations)

Q&A

Upcoming Events

Clearwater's Monthly Cyber Briefings | January 11

What can healthcare organizations learn from other industries about cybersecurity? | December 19 – Hosted & Presented by HIMSS

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Twitter | @clearwaterhipaa

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.