IROQUOIS HEALTHCARE ASSOCIATION

BUSINESS ASSOCIATE EDUCATIONAL WEBINAR SERIES

Review of NY Cybersecurity Regulations for Healthcare

Introductions

IROQUOIS Healthcare Association

Johnathan Buice – MBA, MIS, CISSP, CISM, CISA, Assoc CCISO

Senior Security Solutions Architect - CloudWave

CloudWave

Disclaimer

The information shared here is meant to be a general overview of our interpretation of the New York Cybersecurity for Healthcare regulation and is not meant to be legal advice. You should validate the information to determine the appropriate actions for your organization.

Note: details in this presentation are paraphrased from the regulation documentation for discussion purposes. Please refer to the actual regulations document for all-inclusive details.

For a detailed recap of the regulations, and a link to the regulation, see this HIPAA Journal Article.

Agenda

- Legislative Objective
- General guidelines
- Key compliance areas
- How to approach meeting the regulations
- Example timeline
- Maturity Models vs Risk Assessments
- Q&A

Beyond New York

- HHS Cybersecurity Proposed Bill: Senate bill eyes minimum cybersecurity standards for health care industry | CyberScoop
  - Bill requires HHS to proactively audit cybersecurity practices of at least 20 regulated entities each year.
  - Allows larger financial penalties by removing the statutory cap of fining authorities
  - Executives need to show compliance to the new standards annually
  - CEOs that lie to the government about their cybersecurity could face jail time
  - Funding for Rural and urban safety net hospitals $800M and $500M for others

Legislative Objective

Public Health Law (PHL) 28 – To define minimum cyber requirements for all hospitals to protect:

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- non-public information.

The regulation was presented citing the need to safeguard and secure patient PHI and PII.

The department of Health responded to more than 1 cyber incident per month on average in 2023.

GENERAL GUIDELINES

- Requirements are based on the risk assessment findings (meaning step one is to perform a risk assessment)
- Proactive cybersecurity program to address emerging threats.
- All requirements refer to “non-public” information
- One year to comply (Oct 2, 2025) to be reviewed annually
- Must report any material cybersecurity incident within 72-hours of discovery

NY Cybersecurity Regulation Requirements

Event vs. Incident

- **Event:** An observable action or occurrence within a system or network, which may be routine (e.g., login attempts, file access) or suspicious (e.g., repeated failed logins, unusual file transfers). Not all events indicate a security issue but may require monitoring.

- **Incident:** A confirmed event or series of events that compromise, or have the potential to compromise, information security, operational functionality, or data integrity. Incidents often trigger a response plan and may include breaches, unauthorized access, or malware infections.

NY Cybersecurity Regulation Requirements

- Establish a cybersecurity program based on hospital risk assessment to protect nonpublic information and ensure business continuity.

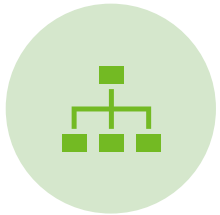
- Definition of non-public information:
  - A hospital's business-related information, the tampering with which, or unauthorized disclosure, access or us of which, would cause a material adverse impact to the business operations or security of such hospital
    - PII
    - PHI

Core Functions of the Cybersecurity Program

IDENTIFY & ASSESS RISKS

EVALUATE INTERNAL AND EXTERNAL CYBERSECURITY RISKS.

ENSURE THE SECURITY AND INTEGRITY OF NONPUBLIC INFORMATION.



MAINTAIN BUSINESS CONTINUITY.

DEFENSIVE MEASURES

IMPLEMENT INFRASTRUCTURE, POLICIES, AND PROCEDURES TO PROTECT INFORMATION SYSTEMS FROM UNAUTHORIZED ACCESS AND MALICIOUS ACTS.

CloudWave

Detect, Respond, and Recover

Detect Cybersecurity Threats

- Monitor systems for potential cyber threats

Respond to Cybersecurity Incidents

- Mitigate the impact of identified threats

Recover Operations

- Restore normal business operations post-incident

Regulatory Reporting

- Fulfill any legal or regulatory obligations

Access Control and Secure Development

Access Privilege Limitation

- Restrict user access based on risk assessment and regulatory requirements (HIPAA)
- Periodic reviews of access privileges

Secure Application Development

- Develop and test secure in-house applications
- Assess and test externally developed applications
- Annual review by CISO

Data Disposal and Encryption

Secure Disposal of Data

- Dispose of unnecessary nonpublic information unless required by law or regulation

Encryption & Security Controls

- Implement encryption for data in transit and at rest
- Security measures based on the hospital's risk assessment

Security Controls: Email

Mitigate risks for email threats

- Spoofing
- Phishing
- Fraud
- Others

Review controls on a regular basis to ensure effectiveness against evolving threats

Cybersecurity Policy

Objective:

- Maintain and implement policies for protecting information systems and nonpublic information.
- Ensure business continuity in compliance with risk assessments and legal regulations.

Development, Implementation, and Enforcement

- Hospital is responsible for developing and enforcing its cybersecurity policy.
- Oversee the hospital's cybersecurity program.
- Ensure compliance with State and Federal laws.

Policy Approval

- Recommended by the Chief Information Security Officer (CISO).
- Approved by the hospital’s governing body.
- A specialized committee may present the policy for approval.

Key Topics in the Cybersecurity Policy

Information Security	Data Governance & Classification	Asset Inventory & Device Management	Access Controls & Identity Management	Business Continuity & Disaster Recovery
Systems Operations & Availability	Systems & Network Security	Systems & Network Monitoring	Application Development & Quality Assurance	Physical Security & Environmental Controls
Patient Data Privacy	Vendor & Third-Party Provider Management	Risk Assessment	Training & Monitoring	Incident Response

CISO

Designation of CISO

- Senior or executive-level staff member.
- Must be qualified through training, experience, and expertise.
- Responsible for overseeing the hospital's cybersecurity policy and program.
- May be a hospital employee or third-party contractor/vendor

Roles of the CISO:

- Must report annually in writing to the hospital's governing body about the hospital's cybersecurity program and risks. Some things to include:
  - Policies and procedures and status of implementation
  - Cybersecurity Risks
  - Overall effectiveness of the cybersecurity program
  - Any incidents
  - Testing and vulnerability assessments

Monitoring and Testing Minimum Requirements

Must include:

- Pen Testing annually
- Automated scans
- Manual or automated review of scans
- Timely remediation of vulnerabilities
- Audit trail and records maintenance
- Records must be maintained for 6 years
- Must perform annual risk assessment of hospital's potential risks and vulnerabilities

Key Components of the Risk Assessment

Evaluation Criteria for Cybersecurity Risks

Categorize risks, vulnerabilities, and threats to the hospital.

Assessment of Information Systems

Evaluate confidentiality, integrity, security, and availability.

Assess the adequacy of existing controls and the likelihood of threat occurrence.

Determine potential impact and risk levels.

Risk Mitigation and Acceptance

Outline how risks and threats will be mitigated or accepted.

Ensure that cybersecurity policies address identified risks.

CloudWave

Cybersecurity Personnel Requirements

Utilization of Qualified Cybersecurity Personnel

Hospital staff, affiliates, or third-party providers should manage cybersecurity risks and oversee core functions.

Third-Party Service Provider Assistance

Hospitals may use third-party providers to assist with cybersecurity compliance.

Security Policies for Third-Party Service Providers

Policy Requirements

Develop policies to protect information systems and nonpublic information accessible to third-party service providers.

Base policies on risk assessments.

Third-Party Provider Evaluation

Identify and assess third-party providers.

Set minimum cybersecurity practices for third parties to do business with the hospital.

Third-Party Service Provider Guidelines

Due Diligence and Contractual Protections

Ensure third-party access controls align with industry standards.

Require encryption for data in transit and at rest.

Establish notification procedures for cybersecurity incidents affecting hospital data.

Include representations and warranties for third-party cybersecurity policies.

Identity & Access Management

- Must use multi-factor authentication to protect against unauthorized access to nonpublic information or information systems
  - Used for individual accessing hospital's internal network from external network
- Limit user access privileges to only to those necessary to perform user's job
- Separate non-privileged and privileged accounts
- Limit the number of privileged accounts to only when performing functions requiring such access
- Annually review all user access privileges and update
- Implement training, monitoring and incident response of unauthorized access

Crosswalk that compares New York's healthcare cybersecurity regulations with HIPAA

Requirement	HIPAA	New York Regulations
Risk Assessment Frequency	Periodic (no specific frequency)	Annual requirement
Scope of Coverage	Primarily ePHI (electronic Protected Health Information)	Expanded to include NPI (nonpublic information), PII, and business information
Penetration Testing	Not required (optional best practice)	Mandatory annual penetration testing
Vulnerability Assessments	Recommended but not specified	Mandatory annual vulnerability assessments
Incident Reporting	60-day breach reporting for incidents affecting 500+ individuals	72-hour reporting to NYSDOH for significant incidents
Chief Information Security Officer (CISO)	Not required, only a 'security official'	Mandatory CISO with board-level reporting
Access Controls & Multi-Factor Authentication (MFA)	Access controls required, MFA recommended but not mandated	MFA required, especially for external network access
Third-Party Security Standards	Requires Business Associate Agreements (BAAs) but lacks specifics	Minimum security standards required for third-party contracts
Audit Trails & Record Retention	6-year retention primarily for ePHI policies	6-year retention for all cybersecurity-related audit trails

NY CYBERSECURITY REGULATIONS REVIEW

Crosswalk that compares New York's healthcare cybersecurity regulations with Cyber Insurance Top 10

Requirement	New York Healthcare Regulations	Cyber Insurance Top 10 Measures
Multi-Factor Authentication (MFA)	MFA required for external access, especially for privileged users	Required for remote, email, privileged access
Backups	Data recovery plans; aligns with offline backups as best practice	Offline backups necessary to qualify for ransomware coverage
Endpoint Detection and Response (EDR)	Incident detection focus; EDR tools encouraged	Required for continuous endpoint monitoring
Patch Management	Annual vulnerability assessments and penetration testing required	Regular patching required; vulnerability scanning also used in assessments
Incident Response Plan	Formal incident response plan with 72-hour reporting to NYDOH	Incident response and business continuity plans are mandatory
Cybersecurity Training	Employee cybersecurity awareness and monitoring required	Cybersecurity awareness training, including phishing exercises
Chief Information Security Officer (CISO)	Mandated CISO role with reporting to hospital leadership	Not required explicitly by insurers
Extended Audit Trails	6-year retention for cybersecurity event audit trails	No specific retention period, only essential event logging
24/7 Security Operations Center (SOC)	Continuous monitoring required, though not explicit for 24/7 SOC	Typically required for eligibility; continuous monitoring encouraged

Recommended Timing

Month 1 – Evaluate requirements and make a plan for Evaluation/Risk Assessment

Month 2 – 3 – Perform Risk Assessment or Maturity Model Assessment

Month 4 – Based on Risk Assessment Results, identify:

Gaps

Priorities

Budget

Document plan

Months 5 – 12 – Begin implementation of processes, technology, and training

Compliance Deadline: October 2, 2025

Cost Estimates

- Depending on level of measures already implemented, New York State estimates the following costs:
  - Initial Expense: $250k – $10 Million
  - Annual Expense:
    - < 10 beds: $50k - $200k
    - 10 – 100 beds: $200k - $500k
    - 100 + beds: Up to $2M
- $650 M in funding was released earlier this year.
- Covered entities can apply for a grant to cover some of the cost

Summary of Regulations

- Conducting an accurate and thorough annual security risk assessment of the hospital's information systems.
- Establishing and maintaining a detailed incident response plan
- Appointing a Chief Information Security Officer (CISO)
- Implementing multifactor authentication on all external facing systems.
- Conducting regular cybersecurity tests, including scanning for vulnerabilities and penetration tests
- Maintaining an audit trail that allows cybersecurity incidents to be detected and responded to rapidly
- Reviewing all user access privileges at least annually and removing any access that is no longer necessary.
- Providing regular cybersecurity awareness training to the workforce and ensuring that training is updated regularly to include risks identified through the hospital's risk assessments.

Note: These is a high-level summary and may not be all inclusive of the requirements. Please see the New York State Regulation documentation for full details.

CloudWave

Maturity Model vs Risk Assessments

Goal	Maturity Model	How?
Achieve Boardroom-to-Basement Alignment	☑	Non-technical easy-to-understand dashboard, nomenclature and tools.
Actionable Findings & Recommendations	☑	Clear findings and recommendations that are prioritized and included task level recommendations.
Create Foundation for Strategy & Investment	☑	Provides a foundational understanding of your maturity – which allows you to then determine risk tolerance and strategic approaches.
Identify Current State as Quickly as Possible	☑	Most programs can be completed within just a few weeks.
Integrate with Current Security Efforts	☑	Cross-walked to NIST-CSF, NIST 800-53, HIPAA. and NY Regulations
Support Compliance & Regulatory Requirements	☑	Provide full risk assessments suitable for compliance and regulatory needs (NY)
Decrease Liability & Increase Defensibility	☑	Develop a pathway to ultimately reduce liability and increase post-breach defensibility.

Maturity Models can be completed rapidly vs. months like Traditional Risk Assessments

CloudWave

Maturity Model Domains

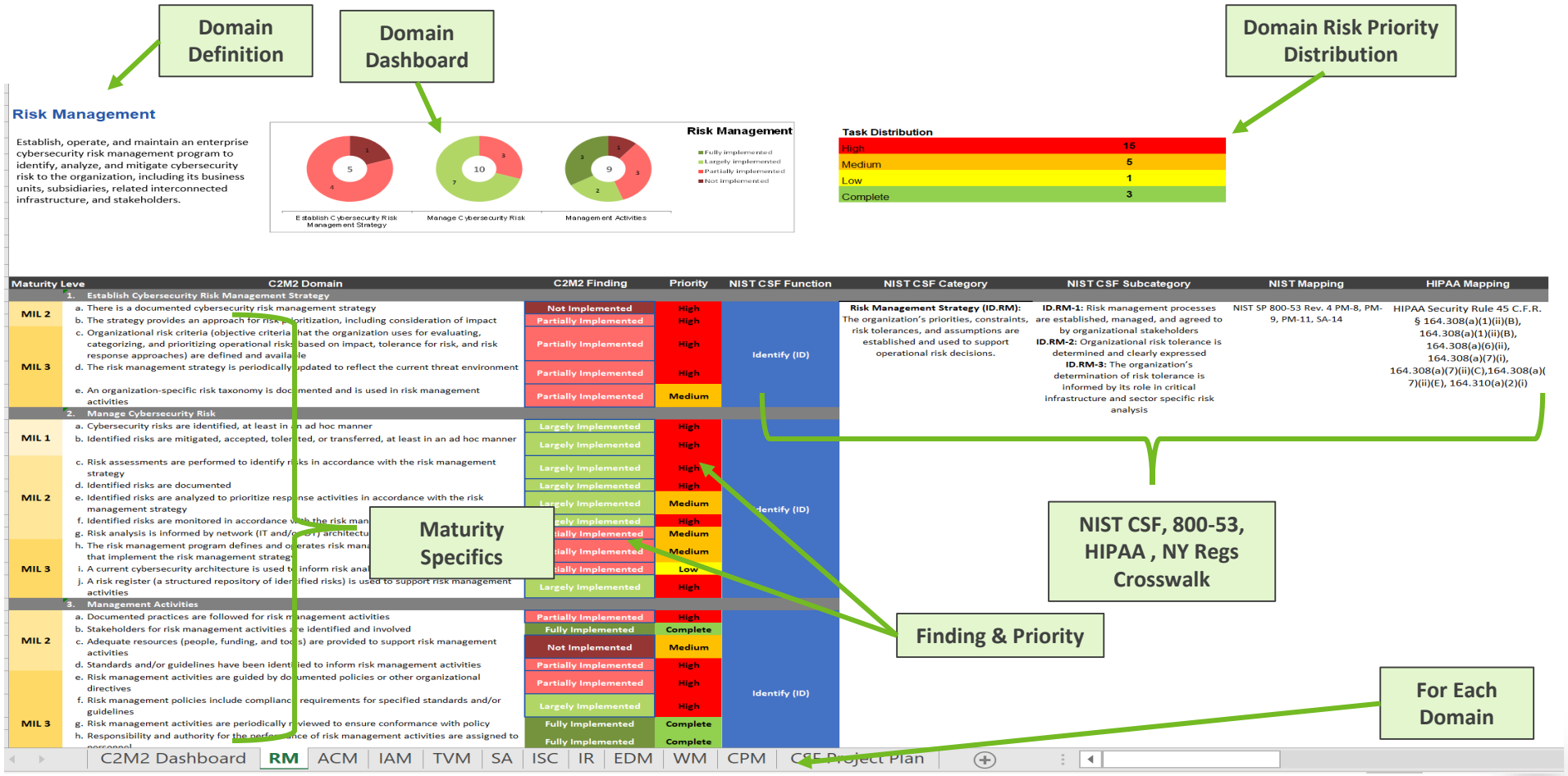
RM	Risk Management	ACM	Asset, Change, and Configuration Management	IAM	Identity and Access Management	TVM	Threat and Vulnerability Management
SA	Situational Awareness	ISC	Information Sharing and Communications	IR	Event and Incident Response, Continuity of Operations	EDM	Supply Chain and External Dependencies Management
WM	Workforce Management	CPM	Cybersecurity Program Management				

Domains are logical groupings of cybersecurity practices

Each domain has an acronym that cross references with the evaluation toolkit

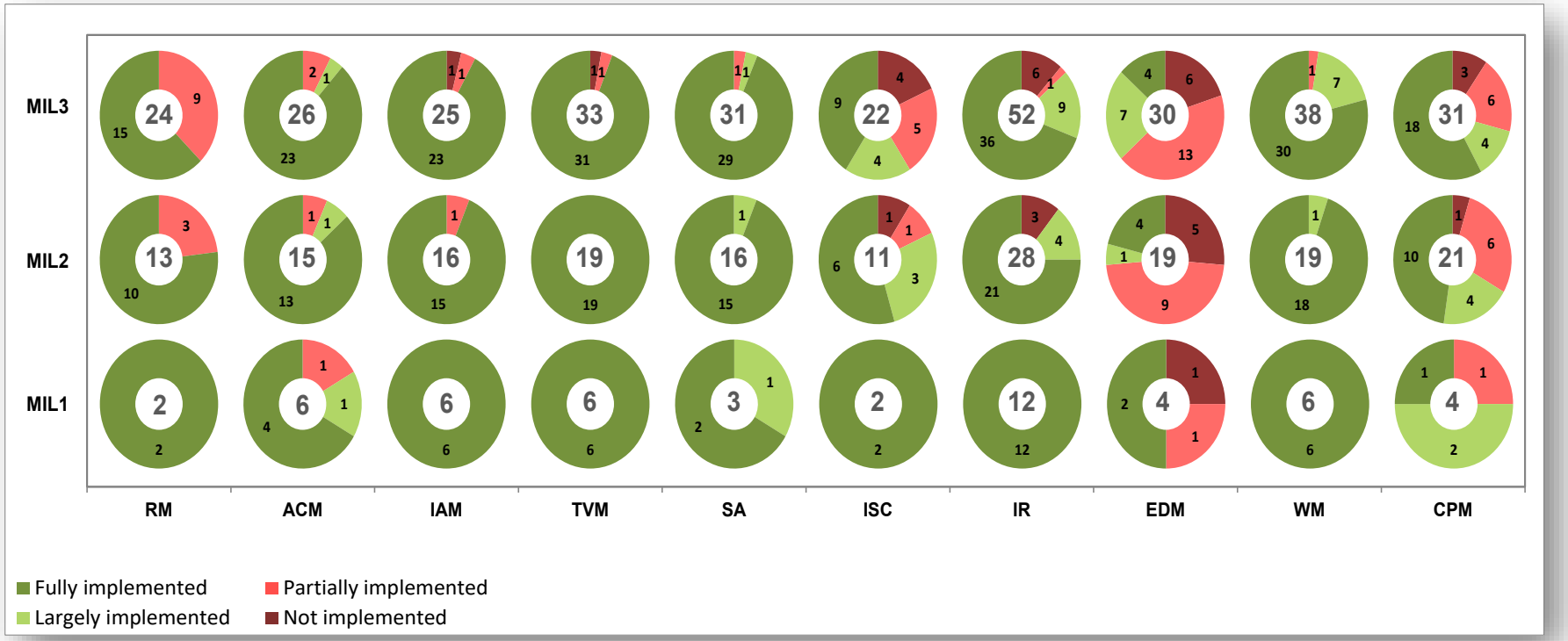
CloudWave

Maturity Model Outcomes



CloudWave

Maturity Model – Domains & Dashboard



Maturity Modeling + Targeted Measures for Compliance

- **Speeds Up Progress Tracking:**
  Structured assessments identify gaps quickly, setting clear improvement goals aligned with NY's phased compliance timeline.

- **Builds Capabilities Over Time:**
  Incremental improvements help meet NY-specific requirements (e.g., annual testing, audit trails) without overwhelming resources.

- **Prioritizes Resources Effectively:**
  Directs focus to critical areas, ensuring efficient budget use and faster action on compliance essentials.

- **Adapts to Evolving Threats:**
  Regular re-assessments support the need for adaptive controls, especially for new threats like email-based attacks.

- **Ensures Sustained Compliance:**
  Moves beyond “point-in-time” assessments, establishing ongoing improvement and resilience.

Resources

- New York Cybersecurity Regulations – Effective Oct 2, 2024
- HIPAA Journal Regulations Recap
- HHS Cybersecurity Proposed Bill
- Cybersecurity Insider Program – Free Insider Sessions, educational info and Threat Intelligence

Contact: customersfirst@gocloudwave.com or Kate Macaleer at kmacaleer@gocloudwave.com for individual discussions.

CloudWave

CloudWave

Thank You.