BERNSTEIN DATA
Operationalizing Information Governance

NYS Department of Health Hospital Cybersecurity Rule

Section 405.46 Compliance Awareness Checklist

Leadership focus: This checklist highlights the breadth of compliance obligations for hospital senior management, including governance, information lifecycle, NPI scope, risk assessment, vendor, reporting, and documentation duties that often sit outside traditional Information Security ownership. A concise summary of specific cybersecurity requirements appears in Section 9.

PART I ACCOUNTABILITY, INFORMATION GOVERNANCE, AND RISK ASSESSMENT

Primary focus areas for hospital leadership: ownership, scope, NPI classification, lifecycle management, and examination readiness.

1. ORGANIZATIONAL ACCOUNTABILITY AND GOVERNING BODY OVERSIGHT

Category	Description	Rule reference
Requirement	Hospital maintains and implements policies and procedures to protect information systems and NPI and to preserve continuity of business and operations.	§405.46(d)(1)
Requirement	Governing body has approved the cybersecurity policy upon CISO recommendation.	§405.46(d)(2)
Requirement	CISO designated from senior- or executive-level staff and qualified by training, experience, and expertise.	§405.46(e)(1)
Requirement	If the CISO is employed by a third-party or contract vendor, the governing body approves the contract annually.	§405.46(e)(2)
Requirement	CISO reports in writing at least annually to the governing body on required program, risk, policy, incident, and NPI/system security topics.	§405.46(e)(3)(i)-(v)
Readiness	All §405.46 requirements inventoried and mapped to accountable/responsible departments, including obligations outside Information Security.	*Supports §405.46(d)(1)-(3)*
Readiness	Non-InfoSec owners assigned for data governance, records/ILM, business continuity, physical/environmental controls, patient privacy, vendor management, and training coordination.	*Supports §405.46(d)(3)*
Readiness	Leadership decision log maintained for NPI scope, information-system scope, classification thresholds, and business-related NPI materiality.	*Readiness evidence*
Readiness	Requirements and Responsibilities Matrix or RACI maintained for governing-body reporting and NYSDOH examination readiness.	*Supports §405.46(e)(3), (n)(2)-(3)*

2. NONPUBLIC INFORMATION SCOPE — RULE CATEGORIES AND HIPAA GAP

Category	Description	Rule reference
Requirement	NPI scope covers business-related electronic information whose compromise would cause material adverse impact to hospital business, operations, or security.	§405.46(b)(8)(i)
Requirement	NPI scope covers PII, including SSNs, driver/non-driver IDs, financial account or access data, biometric data, and username/email plus password or security Q&A.	§405.46(b)(8) [PII clause]
Requirement	NPI scope covers PHI as defined under 45 CFR 160.103 and the Rule's PHI clause.	§405.46(b)(8) [PHI clause]
Requirement	Publicly available information exclusions are applied only where the hospital has a reasonable basis for the exclusion and disclosure would not violate HIPAA or other law.	§405.46(b)(11)
Readiness	Existing HIPAA/ePHI inventories mapped against §405.46; gaps documented for PII outside HIPAA and business-related NPI.	*Supports §405.46(b)(8), (h)(1)*
Readiness	HR, Finance, Payroll, Facilities, Security Operations, and other non-clinical repositories assessed for PII and NPI outside HIPAA programs.	*Supports §405.46(b)(8)*
Readiness	Material-adverse-impact methodology documented for business-related NPI, including whether materiality is assessed proactively or during incident analysis.	*Supports §405.46(b)(5), (b)(8)(i), (m)(2)(v)*
Readiness	NPI definitions embedded in classification, inventory, risk assessment, vendor, disposal, and incident response processes.	*Supports §405.46(c)(5), (d)(3), (h)(1), (j), (m)*

3. INFORMATION SYSTEMS AND REPOSITORY SCOPE

Category	Description	Rule reference
Requirement	Risk assessment addresses changes to information systems, NPI, and business operations supported by those systems.	§405.46(h)(1)
Requirement	Cybersecurity policy addresses asset inventory and device management.	§405.46(d)(3)(iii)
Readiness	The hospital applies the Rule's broad definition of information system: electronic information resources plus specialized systems such as process controls, PBX/telephone switching, and environmental controls.	*Supports §405.46(b)(6), (d)(3)(iii)*
Readiness	Systems inventory includes clinical apps, EHR, non-clinical apps, OT/process controls, phone/PBX, environmental controls, and electronic repositories.	*Supports §405.46(b)(6)*
Readiness	File shares, network drives, email archives, document management systems, collaboration platforms, and unstructured	*Supports §405.46(b)(6), (b)(8)*

		repositories assessed for NPI and scope.	
	Readiness	CMDB gap analysis identifies non-CMDB repositories, non-application systems, repository owners, and systems excluded from current inventories.	*Supports §405.46(d)(3)(iii)*
	Readiness	Dual scoping methodology documented using both system/application criticality and data classification level; thresholds approved by leadership.	*Supports §405.46(b)(6), (b)(8), (h)(1)*
	Readiness	Vendor-managed platforms holding hospital NPI or connecting to hospital systems are included in scoping analysis.	*Supports §405.46(b)(6), (j)*

4. RISK ASSESSMENT METHODOLOGY AND NON-CYBER RISK DOMAINS

	Category	Description	Rule reference
	Requirement	Annual accurate and thorough risk assessment covers risks and vulnerabilities to NPI confidentiality, integrity, and availability; business/operations continuity; and information systems sufficient to inform program design.	§405.46(h)(1)
	Requirement	Risk assessment is updated as reasonably necessary and at least annually, including changes to information systems, NPI, or business operations.	§405.46(h)(1)
	Requirement	Risk assessment is carried out in accordance with written policies and procedures and is documented.	§405.46(h)(2)
	Requirement	Written methodology includes criteria for evaluating and categorizing risks, vulnerabilities, and threats.	§405.46(h)(2)(i)
	Requirement	Written methodology includes criteria for assessing existing controls, likelihood, impact, risk level, and mitigation or acceptance decisions.	§405.46(h)(2)(ii)-(iii)
	Readiness	Written methodology finalized before the assessment is conducted; existing HIPAA or other risk assessments extended only where they meet §405.46 requirements.	*Supports §405.46(h)(1)-(2)*
	Readiness	Domain owners outside InfoSec engaged for business continuity, vendor management, patient data privacy, physical/environmental controls, records/ILM, HR/training, and operations.	*Supports §405.46(d)(3), (h)(1)*
	Readiness	Likelihood, impact, and material-adverse-impact thresholds defined precisely enough to reduce subjectivity across application, repository, and business owners.	*Supports §405.46(h)(2)(ii)*
	Readiness	Risk assessment results are linked to policy updates, control revisions, disposal priorities, and the remediation roadmap.	*Supports §405.46(h)(1)-(2), (n)(3)*

5. DATA GOVERNANCE, CLASSIFICATION, AND INVENTORY

	Category	Description	Rule reference
	Requirement	Cybersecurity policy addresses data governance and classification.	§405.46(d)(3)(ii)
	Requirement	Cybersecurity policy and related domains are based on the hospital risk assessment.	§405.46(d)(3), (h)(1)
	Readiness	Data governance/classification approach supports identification of NPI and systems requiring protection under the Rule.	*Supports §405.46(b)(6), (b)(8), (d)(3)(ii)*
	Readiness	Data classification taxonomy expanded beyond ePHI to cover all NPI categories: business-related NPI, PII, and PHI.	*Supports §405.46(b)(8), (d)(3)(ii)*
	Readiness	Classification levels and in-scope system thresholds approved by Legal, Compliance, Information Security, data governance, and senior leadership.	*Supports §405.46(d)(3)(ii), (h)(1)*
	Readiness	System/application-level data inventory records classification, data types, department, owner/steward, repository/system, vendor status, and retention/disposal owner.	*Supports §405.46(d)(3)(ii)-(iii)*
	Readiness	File/object-level inventory for unstructured repositories such as file shares, collaboration platforms, and email archives.	*Supports §405.46(b)(6), (b)(8), (d)(3)(ii)*
	Readiness	Data inventory supports risk assessment, incident NPI scoping, vendor management, and disposal decisions.	*Supports §405.46(c)(5), (h)(1), (j), (m)(2)(v)*

6. INFORMATION LIFECYCLE MANAGEMENT AND SECURE DISPOSAL

	Category	Description	Rule reference
	Requirement	Cybersecurity program includes policies and procedures for periodic secure disposal of identified NPI no longer necessary for business operations or other legitimate business purposes.	§405.46(c)(5)
	Requirement	Disposal process accounts for NPI that must be retained by law/regulation or where targeted disposal is not reasonably feasible due to the manner in which information is maintained.	§405.46(c)(5)
	Readiness	Records retention schedule covers all NPI categories, not only HIPAA-era ePHI guidelines.	*Supports §405.46(c)(5), (b)(8)*
	Readiness	Secure disposal procedures documented for structured data and unstructured data, including file shares, email archives, and collaboration platforms.	*Supports §405.46(c)(5)*
	Readiness	Periodic disposal review cycle established with frequency, triggers, owners, approvals, legal-hold checks, feasibility determinations, and evidence of disposal.	*Supports §405.46(c)(5), (n)(2)-(3)*
	Readiness	Disposal activities, exceptions, and remediation status documented for CISO annual reporting and NYSDOH examination.	*Supports §405.46(c)(5), (e)(3), (n)(2)-(3)*
	Readiness	Organization-wide inventory and disposal rollout roadmap established for multi-year execution across in-scope systems and repositories.	*Readiness evidence*

7. THIRD-PARTY SERVICE PROVIDER GOVERNANCE

Category	Description	Rule reference
Requirement	Written policies and procedures ensure security of information systems and NPI accessible to, or held by, third-party service providers and are based on the risk assessment.	§405.46(j)(1)
Requirement	Third-party service providers are identified and baseline assessed where applicable.	§405.46(j)(1)(i)
Requirement	Minimum cybersecurity practices required for third parties to do business with the hospital are documented.	§405.46(j)(1)(ii)
Requirement	Due diligence and contractual protections address access controls, encryption/protection of NPI, incident notice, and cybersecurity representations/warranties.	§405.46(j)(2)(i)-(iv)
Readiness	Vendor inventory identifies providers with access to hospital systems/NPI or holding hospital NPI, including vendors outside traditional IT procurement channels.	*Supports §405.46(j)(1)*
Readiness	Vendor management owner assigned and coordinated across Procurement, Legal, Compliance, Privacy, and Information Security.	*Supports §405.46(d)(3)(xii), (j)*
Readiness	Contract templates, review playbooks, and renewal processes updated for §405.46 access, encryption, incident-notice, and evidence requirements.	*Supports §405.46(j)(2)*
Readiness	Third-party risk results feed the annual risk assessment, CISO report, and remediation tracking.	*Supports §405.46(e)(3), (h)(1)-(2), (n)(3)*

8. DEPARTMENT REPORTING AND EXAMINATION READINESS

Category	Description	Rule reference
Requirement	Hospital or designee notifies the Department as promptly as possible and no later than 72 hours after determining a cybersecurity incident has occurred.	§405.46(n)(1)
Requirement	Required and supporting documentation, including records, schedules, reports, and data, is maintained for at least six years and submitted for examination as the Department requires.	§405.46(n)(2)
Requirement	Material improvements, updates, redesign, and remedial efforts are documented, available for inspection, and maintained for at least six years.	§405.46(n)(3)
Readiness	Event-to-incident decision process documented, including ransomware trigger, material-adverse-impact analysis, and when an event becomes a reportable incident.	*Supports §405.46(b)(5), (m)(2)(v), (n)(1)*
Readiness	Reporting roles, business/off-hours contacts, escalation timelines, and Legal/Compliance review are documented and tested.	*Supports §405.46(m)(2)(ii)-(iii), (n)(1)*
Readiness	Evidence repository includes policies, risk assessments, inventories, CISO reports, testing records, vendor assessments, training evidence, disposal records, and remediation records.	*Supports §405.46(n)(2)-(3)*
Readiness	Current data inventory and classification framework support rapid NPI scoping and documentation during incident response.	*Supports §405.46(b)(8), (h)(1), (m)(2)(v)-(vi)*
Readiness	Confidentiality handling for information provided to the Department is coordinated with Legal and Compliance.	*Supports §405.46(o)*

PART II CYBERSECURITY REQUIREMENTS SUMMARY

The following table is a summary only of specific cybersecurity controls, testing, education, staffing, and incident response requirements. Detailed control validation should be completed with Information Security and other cybersecurity functions.

9. CYBERSECURITY REQUIREMENTS SUMMARY

Category	Description	Rule reference
Requirement	Cybersecurity program established within policies and procedures, based on the risk assessment, and designed to identify, protect, detect, respond, recover, and fulfill reporting obligations.	§405.46(c)(1)-(2)
Requirement	Cybersecurity policy addresses all required domains, including information security, access/identity, business continuity, systems operations/security/monitoring, app development, physical/environmental controls, privacy, vendors, risk assessment, training, and incident response.	§405.46(d)(3)(i)-(xv)
Requirement	Access controls enforce least privilege, periodic access reviews, prompt departure termination, privileged-account separation/limits, and secure configuration or disabling of remote-control protocols.	§405.46(c)(3), (k)(3)-(9)
Requirement	MFA, risk-based authentication, or compensating controls protect access to NPI or information systems; MFA is used for external access unless CISO-approved compensating controls are documented.	§405.46(k)(1)-(2)
Requirement	NPI is protected in transit and at rest using encryption or CISO-approved compensating controls, with feasibility and effectiveness reviewed and documented at least annually.	§405.46(c)(6)(i)-(iii)
Requirement	Secure development procedures exist for in-house applications and security evaluation/testing procedures exist for externally developed applications, with annual CISO/designee review and attestation.	§405.46(c)(4)
Requirement	Controls mitigate electronic mail-based threats such as spoofing, phishing, and fraud and are reviewed and updated regularly.	§405.46(c)(7)
Requirement	Monitoring and testing include annual penetration testing, vulnerability scans or manual/automated reviews, and timely risk-based remediation.	§405.46(f)(1)-(2)
Requirement	Systems, security/maintenance records, audit trails, and audit-trail-system records are securely maintained for at least six years and based on the risk assessment.	§405.46(g)(1)-(3)
Requirement	Authorized-user activity monitoring detects unauthorized access, use, or tampering; cybersecurity awareness training is regular, risk-based, and updated to reflect the risk assessment.	§405.46(l)(1)-(2)
Requirement	Written incident response plan covers goals, roles/authority, business/off-hours contacts, communications, remediation, response/materiality process, documentation/reporting, and post-event review.	§405.46(m)(1)-(2)

	Requirement	Qualified cybersecurity personnel, affiliates, or third-party providers are sufficient to manage cybersecurity risks and perform or oversee core cybersecurity functions.	§405.46(i)(1)-(2)

Identified gaps? Bernstein Data can help.

Bernstein Data helps NYS hospitals address the information governance, data identification, and risk assessment obligations in §405.46 — **the requirements that extend beyond traditional cybersecurity programs.**

Our modular services move hospitals from gap identification to documented, demonstrable compliance.

www.bernsteindata.com

Matthew Bernstein
Bernstein Data
www.bernsteindata.com
linkedin.com/in/matthewcbernstein

This checklist is provided for informational and awareness purposes only and does not constitute legal or regulatory advice.