Comprehensive Resource Guide: Federal and State Cybersecurity Requirements (United States)

Table of Contents:

This guide provides a detailed, section-by-section summary of the latest federal and state cybersecurity legal requirements, enforcement mechanisms, and compliance best practices. It is designed to help in-house counsel understand, implement, and monitor compliance with evolving data security obligations.

1. State and Federal Law Updates

State Law Developments

New York Department of Financial Services (NYDFS) Cybersecurity Rule (23 NYCCRR Part 500)

- Amendments (November 2023):
  NYDFS amended its cybersecurity regulations for financial services companies and other covered entities. The changes are set to become effective on a rolling basis over the next two years.

- Implementation Timelines:
  NYDFS has published implementation timelines for Small Business, Class A Businesses, and Covered Entities.

- Definitions:
    - *Class A Companies*: Over $20 million in annual revenue and either over 2,000 employees, or $1 billion in revenue.
    - *Small Businesses*: Fewer than 20 employees, less than $7.5 million in gross annual revenue, or less than $15 million in year-end total assets.
    - *Covered Entities*: Any financial institution regulated by the NYDFS.

NY SHIELD Act (N.Y. Gen. Bus. Law §§ 899-aa and 899-bb)

- Effective Date: October 23, 2019.

- Key Changes:
    - Expanded definition of private information.
    - Changed definition of "breach."
    - Added requirements for businesses that own or license NY residents' private information to implement and maintain security safeguards.
    - Mandates development, implementation, and maintenance of reasonable safeguards to protect the security, confidentiality, and integrity of private information, including data disposal.

  - Requirements include reasonable administrative, technical, and physical safeguards.
  - For small businesses, requirements must be "appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

- Examples of Safeguards:
  - Administrative: Designate security coordinators, risk identification, sufficiency assessment, employee training, vendor management, program adjustment.
  - Technical: Network/software risk assessment, information processing risk assessment, attack/system failure response, regular testing/monitoring.
  - Physical: Storage/disposal risk assessment, intrusion response, unauthorized access prevention, timely data destruction.

- Enforcement and Penalties:
  - Failure to comply is a violation of section 349, with the Attorney General empowered to seek injunctions and civil penalties under section 350-d.
  - Civil penalties up to $5,000 per violation.
  - Breach notification failures: $20 per instance, capped at $250,000.
  - No private right of action.

California Privacy Protection Agency (CPPA) (Cal. Civ. Code § 1798.100 et seq.) – Proposed CCPA Regulations

- Recent Developments:
  The CPPA has released modified draft CCPA regulations in response to public feedback, focusing on cybersecurity audits, risk assessments, automated decision-making technology (ADMT), and sensitive data.

- Cybersecurity Audits:
  - New definition of "Cybersecurity Audit Report" clarifies documentation required for annual audits under Article 9.
  - Expanded scope to include third-party systems used by service providers or contractors.
  - Establishes deadlines for completing the first audit based on risk assessment.
  - Details on audit scope and documentation retention for both businesses and auditors.
  - Examples provided for describing audit scope (processes, activities, components of the information system assessed).
  - Extends document retention requirements to both the business and its auditor.

- Risk Assessments:
  - Updates roles, disclosures, and safeguards.
  - Identifies individuals responsible for reviewing and approving risk assessments.
  - Requires identification of the individual with authority to determine whether the business will proceed with the associated data processing activity.
  - Sets deadlines for assessments of ongoing data processing activities.

- Automated Decision-Making Technology (ADMT):

  - Requires notification to service providers when consumers opt out of specific ADMT uses.
  - Removes requirement for quality documentation in ADMT risk assessments.
  - Expands definitions of sensitive data categories, including "neural data."
  - Exempts non-identifiable physical or biological traits from certain definitions.

- Notice at Collection – AR/VR and Device-Based Interactions:
  - Allows notice to be provided before or at the time of data collection in dynamic tech environments.
  - Removes requirements for agency complaint information and certain notification obligations to streamline compliance.

Federal Law Developments

Federal Trade Commission (FTC)

- Authority:
  The FTC regulates cybersecurity under Section 5 of the FTC Act (15 U.S.C. § 45), which prohibits "unfair or deceptive acts or practices in or affecting commerce."

- Key Case: *FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 236 (3d Cir. 2015) affirmed the FTC's authority to regulate cybersecurity.

- Safeguards Rule:
  - Requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.
  - "Customer information" includes any record containing nonpublic personal information about a customer, in any form, handled or maintained by or on behalf of the institution or its affiliates.

- Information Security Program Requirements:
  - Must be written and appropriate to the size and complexity of the business, nature and scope of activities, and sensitivity of information.
  - Objectives: ensure security and confidentiality, protect against anticipated threats or hazards, and protect against unauthorized access that could result in substantial harm or inconvenience.

- Nine Elements of a Reasonable Information Security Program (Section 314.4):
  1. Designate a Qualified Individual to implement and supervise the program.
  2. Conduct a risk assessment.
  3. Design and implement safeguards to control identified risks.
  4. Regularly monitor and test safeguards.
  5. Train staff.
  6. Monitor service providers.
  7. Keep the program current.
  8. Create a written incident response plan.
  9. Require the Qualified Individual to report to the Board of Directors.

Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 C.F.R. §§ 160, 164(A), (C))

- Scope: Applies to covered entities (health plans, health care clearinghouses, providers transmitting health information electronically) and business associates. Protects electronic protected health information (ePHI) maintained or transmitted by electronic media.

- Proposed Regulations (January 6, 2025):
  - Address shortcomings identified in the Office of Inspector General's November 2024 report.
  - Goal: improve audit effectiveness by expanding the scope and depth of security assessments.
  - High-level changes: updated definitions and requirements (including MFA and enhanced technical safeguards), clarification of compliance obligations, and establishment of a baseline for security measures.
  - Comment period ended March 7, 2025, with over 4,000 comments submitted.

- Key Takeaways from Proposed Regulations:
  - Annual Technical Inventory and Data Mapping:
    - Requires written inventories of assets (hardware, software, electronic media, data, etc.) capable of creating, receiving, maintaining, or transmitting ePHI, and a map showing ePHI movement. Must be updated at least annually or upon certain events (e.g., threats, incidents, legal changes, tech acquisitions).
  - More Rigorous Security Risk Assessments:
    - Must include technology asset inventory, threat/vulnerability identification, documentation of security measures, policies for tracking risks, and documented "reasonable determinations" of threat likelihood and impact.
  - Rigorous Vendor Oversight:
    - Requires assessment of downstream business associate agreements (BAAs) based on written verifications, validated by a cybersecurity expert and certified by an authority at the business associate.
  - Mandatory Authentication Controls:
    - MFA required on all technology assets, with limited exceptions for certain legacy systems and pre-March 2023 FDA-approved medical devices (if a transition plan is in place).
  - Mandatory Encryption Standards:
    - Requires encryption of ePHI on servers, laptops, mobile devices, and during transmission, with limited exceptions (e.g., individual requests for unencrypted ePHI).
  - Formalized Incident Response Planning:
    - Incident response plans must be reviewed and tested at least once every 12 months and modified as appropriate.
  - Disaster Recovery and Backups:
    - Requires "criticality analysis" to prioritize restoration, exact backup copies of ePHI, restoration within 72 hours, and 24-hour notification to upstream covered entities upon contingency plan activation. Annual compliance audits required.
  - Workforce Security Access Management:

        - Written procedures for access based on role, authorization consistent with the Minimum Necessary Rule, and access termination within one hour of employment end.
    - Network Testing, Segmentation, and Configuration:
        - Vulnerability scanning at least every six months, penetration testing at least annually, network segmentation, anti-malware deployment, and removal of unsupported software.

Cybersecurity & Infrastructure Security Agency (CISA) – CIRCIA

- Role: CISA, part of the U.S. Department of Homeland Security, is responsible for cybersecurity and infrastructure across all levels of government, coordinating with states, and improving protections against private and nation-state hackers.

- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA):
    - Requires CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments.
    - Goal: enable CISA to quickly deploy resources, analyze trends, and warn other potential victims.
    - Covered entities: businesses exceeding the small business size standard (13 C.F.R. § 121) or meeting sector-based criteria (generally critical infrastructure or public/governmental entities).

Cybersecurity Maturity Model Certification (CMMC)

- Purpose:
    - Ensures defense contractors safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

- Applicability:
    - Applies to all Department of Defense (DoD) contracts and subcontracts where FCI or CUI is processed, stored, or transmitted, except for certain federal information systems operated by contractors on behalf of the government.

- Requirements:
    - Organizations seeking certification must undergo assessments to achieve a CMMC status.
    - Three levels of cybersecurity maturity, depending on the criticality of FCI and CUI.
    - Applies to all tiers of subcontractors; prime contractors must ensure subcontractor compliance.
    - Effective December 16, 2024 (32 C.F.R § 170).

Federal Information Security Modernization Act (FISMA)

- Scope: Applies to federal agencies and contractors managing or operating information systems on behalf of federal agencies.

- Requirements:
    - Agency-wide information security programs, including protections for contractor-operated systems.

- DHS role in policy administration, compliance oversight, and technical assistance.
- Incident reporting to Congress, streamlined reporting, and new requirements for major incidents.

Executive Orders (2025)

- Key Takeaways:
  - January 16, 2025 (Biden Administration): Identifies China as the biggest threat to U.S. cybersecurity, enhances secure technology practices, continues secure software development and internet routing efforts, maintains post-quantum cryptography (PQC) transition schedule, and frames AI as private-sector driven with greater federal adoption and vulnerability management.
  - June 6, 2025 (Trump Administration): Continues and expands on prior efforts.

2. Practical Takeaways for In-House Counsel

1. Monitor Implementation Timelines:
   - Many requirements (NYDFS, CMMC, HIPAA) have rolling or future effective dates. Track and plan for compliance deadlines.

2. Tailor Safeguards to Business Size and Risk:
   - Ensure security programs are risk-based and scaled to the size, complexity, and sensitivity of your organization's data and operations.

3. Strengthen Vendor and Third-Party Management:
   - Review and update contracts to require appropriate safeguards.
   - Implement rigorous oversight and verification, especially for business associates and service providers.

4. Maintain Comprehensive Documentation:
   - Keep detailed records of risk assessments, audits, incident response plans, and compliance activities.
   - Ensure documentation meets regulatory retention and audit requirements.

5. Update and Test Incident Response and Disaster Recovery Plans:
   - Regularly review and test plans.
   - Ensure rapid notification and recovery capabilities.

6. Implement Technical Controls:
   - Deploy MFA, encryption, vulnerability scanning, penetration testing, and network segmentation as required.
   - Remove unsupported software and maintain anti-malware protections.

7. Conduct Regular Training and Board Reporting:
   - Train staff on security practices and procedures.
   - Ensure regular reporting to the Board of Directors on security program status.

8. Stay Informed on Regulatory Developments:
   - Track updates to state and federal regulations, proposed rules, and enforcement trends.

- Engage in public comment periods and industry groups as appropriate.

9. Prepare for Audits and Assessments:
    - Schedule and document annual audits and risk assessments.
    - Ensure readiness for both internal and external reviews.

10. Address New Technologies and Data Types:
    - Update policies for AR/VR, device-based interactions, and new categories of sensitive data (e.g., neural data).
    - Ensure compliance with evolving notice and opt-out requirements.

3. Questions and Further Guidance

For further clarification or to address specific scenarios, consult the full text of the referenced laws and regulations, and consider engaging with outside counsel or regulatory experts as needed.