Appendix D

PRIMARY SECURITY AND PRIVACY MANDATES[1]

Significant federal and state laws, regulations, policies, standards, and guidelines

- Criminal Justice Information Services (CJIS) Security Policy
- Federal Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
  - National Institute of Technology Standards
- Gramm-Leach-Bliley Act (GLB)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- IRS Publication 1075
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)
- Electronic Communications Privacy Act, Stored Communications Act and the PATRIOT Act
- New York State Breach Notification Act: Breach Notification and Incident Reporting | Office of Information Technology Services (ny.gov)
- NYS Cyber Security Policy and related Standards: Policies | Office of Information Technology Services (ny.gov)
- NYS Cyber Incident Reporting: Breach Notification and Incident Reporting | Office of Information Technology Services (ny.gov)
- Minimum Acceptable Risk Standards for Exchanges (MARS-E)

1.1 Criminal Justice Information Services ("CJIS") Security Policy

The CJIS Security Policy represents a shared responsibility between the Federal Bureau of Investigations ("FBI") and CJIS System Agencies ("CSA") and State Identification Bureau ("SIB"). For the State of New York, the NY State Police is the CSA, and the Division of Criminal Justice Services is the SIB. The policy covers the roles and responsibilities for the FBI and the CSA and service providers covered under CJIS security addendums and CJS management control agreements.

CJIS requirements guidance:

- CJIS Security Policy Resource Center — LE (fbi.gov)

1.2 Federal Educational Rights and Privacy Act ("FERPA") - State Ed, Higher Ed

Protects the privacy of student education records. "Education records" are those records, files, documents, and other materials that 1) contain information directly related to a student; and 2) are maintained by an educational institution. Examples: Grades, courses taken, schedule, test scores, advising records, educational services received, disciplinary actions, student identification number, Social Security number, student private email.

FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

[1] Please note that any hyperlinks provided in this document are subject to change and are not exhaustive of all resources available.

FERPA requirements guidance:

- https://studentprivacy.ed.gov/sites/default/files/resource_document/file/An%20Eligible%20Student%20Guide%20to%20FERPA_0.pdf
- Electronic Code of Federal Regulations, Title 34, Part 99

1.3 Federal Information Security Management Act of 2002 ("FISMA")

FISMA requires each federal agency to develop, document, and implement an effective agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. It is Title III of the E-Government Act of 2002. It affects Federal agencies, and other agencies they share data with.

Key requirements/provisions include:

- Periodic risk assessments.
- Policies and procedures based on these assessments that cost-effectively reduce information security risk and ensure security is addressed throughout the life cycle of each information system.
- Subordinate plans for information security for networks, facilities, etc.
- Security awareness training for personnel.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and controls, at least on an annual basis.
- A process to address deficiencies in information security policies.
- Procedures for detecting, reporting, and responding to security incidents.
- Procedures and plans to ensure continuity of operations for information systems that support the organization's operations and assets.

FISMA requirements guidance:

- https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma
- Federal Information Security Modernization Act | CISA

FISMA requires that federal agencies comply with Federal Information Processing Standards (FIPS) developed by the National Institute of Standards and Technology ("NIST"). Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget ("OMB") policy OMB Memorandum M-10-15, directs agencies to follow NIST guidance.

NIST Special Publications: https://csrc.nist.gov/publications/sp

1.4 Gramm-Leach-Bliley Act of 1999 ("GLB")

GLB (also known as the Financial Modernization Act of 1999) includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, the Safeguards Rule, and pretexting provisions.

GLB affects financial institutions (banks, securities firms, insurance companies), as

well as companies providing financial products and services to consumers (including lending, brokering, or servicing any type of consumer loan; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; and collecting consumer debts).

Key requirements/provisions: The privacy requirements of GLB include three principal parts:

- The Financial Privacy Rule: Requires financial institutions to give customers privacy notices that explain their information collection and sharing practices. In turn, customers have the right to limit some sharing of their information. Financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information.
- The Safeguards Rule: Requires all financial institutions to design, implement, and maintain safeguards to protect the confidentiality and integrity of personal consumer information.
- Pretexting provisions: Protects consumers from individuals and companies that obtain their personal financial information under false pretenses, including fraudulent statements and impersonation.

GLB requirements guidance:

- How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act | Federal Trade Commission (ftc.gov)
- Financial Privacy Rule | Federal Trade Commission (ftc.gov)

1.5 Health Information Portability and Accountability Act ("HIPAA")

HIPAA has two major arms: Privacy and Security. Privacy tends to be a business (non-IT) focus, involving the program, HIPAA Privacy Officer and legal. Security tends to be more IT-focused (though it does cover handling of paper records as well).

Many health agencies have compliance requirements that are more stringent than HIPAA – HIPAA is the baseline. For example, the NYS Public Health law has tight requirements regarding AIDS information. The federal regulations at 42 CFR Part 2 guide privacy requirements of substance abuse information. The NYS Mental Hygiene law extends HIPAA consent requirements. Accordingly, meeting baseline HIPAA requirements may not be sufficient in all cases.

HHS (Federal Health and Human Services) HIPAA resources and requirements:

- Privacy rule:https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- Security rule:https://www.hhs.gov/hipaa/for-professionals/security/index.html

Summarized versions:

- https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

HHS Educational Series bulletins:

- https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

AMA summary of violation (HHS Office of Civil Rights (OCR) audits can result in significant fines for not following the rules regardless of the scope of impact from a breach).

- https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

1.6 Health Information Technology for Economic and Clinical Health Act ("HITECH")

HITECH, enacted in 2009, promotes the adoption and meaningful use of health information technology. Subtitle D of HITECH addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

HITECH requirements guidance:

- https://www.hhs.gov/hipaa/for-professionals/security/guidance/hitech-act-rulemakingimplementation-update/index.html

1.7 IRS Safeguard Program, Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities

Publication 1075 contains specific requirements for safeguarding federal tax information (current revision effective on Jan. 1, 2014).

- https://www.irs.gov/privacy-disclosure/safeguards-program
- https://www.irs.gov/pub/irs-pdf/p1075.pdf

1.8 Payment Card Industry Data Security Standard ("PCI DSS")

The PCI DSS is a set of requirements for enhancing security of payment customer account data, developed by the founders of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa to help facilitate global adoption of consistent data security measures. PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The Council also issued requirements called the Payment Application Data Security Standard (PA DSS) and PCI Pin Transaction Security (PCI PTS). PCI DSS affects retailers, credit card companies, and anyone else handling credit card data. Currently, PCI DSS specifies 12 requirements, organized in six basic objectives:

<u>Objective 1: Build and Maintain a Secure Retail Point of Sale System.</u>

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Objective 2: Protect Cardholder Data

- Requirement 3: Protect stored cardholder data.
- Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Objective 3: Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software.
- Requirement 6: Develop and maintain secure systems and applications.

Objective 4: Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know.
- Requirement 8: Assign a unique ID to each person with computer access.
- Requirement 9: Restrict physical access to cardholder data.

Objective 5: Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data.
- Requirement 11: Regularly test security systems and processes.

Objective 6: Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security.

PCI compliance requirements:

- PCI Document Library: https://www.pcisecuritystandards.org/document_library
- PA DSS: PCI Security Standards Council – Protect Payment Data with Industry-driven Security Standards, Training, and Programs
- PCI PTS: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

1.9 Sarbanes-Oxley Act of 2002 ("SOX")

SOX is designed to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. It was enacted after the high-profile Enron and WorldCom financial scandals of the early 2000s. It is administered by the Securities and Exchange Commission, which publishes SOX rules and requirements defining audit requirements and the records businesses should store and for how long. It affects U.S. public company boards, management and public accounting firms.

The Act is organized into 11 titles:

1. Public Company Accounting Oversight
2. Auditor Independence
3. Corporate Responsibility
4. Enhanced Financial Disclosures
5. Analyst Conflicts of Interest
6. Commission Resources and Authority
7. Studies and Reports
8. Corporate and Criminal Fraud Accountability
9. White-Collar Crime Penalty Enhancements

10. Corporate Tax Returns
11. Corporate Fraud Accountability

SOX requirement guidance:

- https://www.congress.gov/bill/107th-congress/house-bill/3763
- https://pcaobus.org/

1.10 The U.S. Electronic Communications Privacy Act, The U.S. Stored Communications Act, The U.S. PATRIOT Act

The Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA) create statutory privacy rights for people's electronic communications stored by a third-party service provider in "electronic," "computer," "temporary" or "intermediate" storage. Certain types of electronic communications (unread mail that is newer than 180 days) may only be obtained by law enforcement from a service provider via a search warrant. Other electronic communications and user information may be more easily obtained by law enforcement from a third-party provider by a court order or subpoena. Any communications may be obtained by law enforcement from a third-party provider if the end user has provided consent. End users should be careful not to give such consent by clicking through a Terms of Use and/or Privacy Policy or by signing a contract. The PATRIOT Act allows law enforcement to obtain or intercept electronic communications and other end user data from third-party service providers for terrorism investigations using protocols that are less stringent than those that would normally apply.

- U.S. Electronic Communications Privacy Act: Electronic Communications Privacy Act of 1986 (ECPA) | Bureau of Justice Assistance (ojp.gov)
- U.S. Stored Communications Act: https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim
- U.S. PATRIOT Act: https://www.justice.gov/archive/ll/highlights.htm