LEGALfuel
The Practice Resource Center of The Florida Bar

Selected Data Privacy Laws Outline

(Presented by the Florida Bar's Standing Committee on Technology)

Table of Contents

I. SELECTED FEDERAL PRIVACY LAWS

1. Health Insurance Portability and Accountability Act (HIPAA)

Under the Health Insurance Portability and Accountability Act (HIPAA), the subsequent Health Information Technology for Economic and Clinical Health (HITECH) Act, and their related regulations, rules exist to govern the privacy and security of individually identifiable health information, referred to as protected health information (PHI). Such information may include medical records of an individual's physical or mental health that also identify the individual to which the records pertain. These regulations apply to covered entities, which include most healthcare providers and health plans, and business associates of those covered entities. Generally, a business associate performs certain activities for a covered entity involving PHI obtained from that covered entity. For example, a law firm may be a business associate of a covered entity if it provides legal services to the covered entity and the provision of those services involves the disclosure of PHI from the covered entity to the law firm. As a business associate, a law firm may be responsible for complying with many of the same privacy and security regulations imposed on covered entities. The HIPAA Privacy Rule requires privacy safeguards for PHI through limitations on its uses and disclosures. In addition, regulations exist for breach notification in the event of an unauthorized use or disclosure of PHI. Under the HIPAA Security Rule, both covered entities and their business associates must implement reasonable administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. The Security Rule outlines general standards for each category of safeguard and identifies which safeguard implementation specifications are "required" or "addressable." The Security Rule provides a flexible approach to determining the extent of necessary security measures based on the size of the entity, the entity's technical infrastructure, and the cost of security measures, among several other factors. Business associate contracts are also created to provide satisfactory assurances to the covered entity that the business associate will safeguard the PHI. All attorneys who may handle PHI for covered entities should be aware of these HIPAA regulations and understand how they may affect their practice.

Resources:

- HIPAA for Professionals Guide from the U.S. Department of Health and Human Services
- "Business Associate Contract" Sample and Guidance
- Key HIPAA Regulations for Attorneys:
  - Definitions: 45 C.F.R. § 160.103
  - Uses and Disclosures of PHI by Business Associates: 45 C.F.R. § 164.502 and 45 C.F.R. § 164.504(e)
  - Breach Notifications by Business Associates: 45 C.F.R. § 164.410
  - Business Associate Contracts: 45 C.F.R. § 164.502(e) and 45 C.F.R. § 164.504(e)
  - Security Rule: Subparts A and C of 45 C.F.R. part 164 and 45 C.F.R. part 160
    - Key Provisions: 45 C.F.R. §§ 164.302-164.318
  - Privacy Rule: Subparts A and E of 45 C.F.R. part 164 and 45 C.F.R. part 160
    - Key Provisions: 45 C.F.R. §§ 164.500-164.534
- Browse HIPAA Regulations: 45 C.F.R. part 160, part 162, part 164

2. Employment Retirement Income Security Act (ERISA)

This law applies to private sector employee benefit plans, such as employee pension and health plans. Where a private employer offers such plans, the ERISA regulates the operations of the plans. Among other requirements under the Act, benefit plans have specific disclosure and record keeping requirements. In addition, plan administrators have a fiduciary obligation to the employees who receive benefits under the plan. As standards for fiduciary obligations evolve with changing technologies, it would be prudent for all ERISA plan administrators, and the attorneys who advise them, to be cognizant of new technologies relevant to plan administration and the privacy of employees' personal information.

Resources:

- 29 U.S.C §§ 1001-1461

- Department of Labor – ERISA Employment Law Guide
- Department of Labor – ERISA Advisory Council Report – Cybersecurity Considerations for Benefit Plans (2016)

3. Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act, protects customer privacy through the regulation of data sharing between financial institutions and affiliates of those institutions. It governs the use of nonpublic personal information, which includes personally identifiable financial information. Among other obligations, it requires financial institutions to provide notice to customers regarding the sharing of nonpublic personal information with affiliates, and it mandates the ability of customers to opt-out of sharing this information with nonaffiliated third parties. Under the Safeguards Rule, financial institutions must implement a comprehensive information security program with administrative, technical, and physical safeguards to ensure the confidentiality and safety of customer information. Financial institutions must also oversee service providers that access their customers' information and ensure that these providers implement safeguards for this information. Law firms that represent financial institutions should be aware of both the obligations placed on the institution and identify which obligations, such as the information safeguard obligations, that may extend to the firm based on its relationship with the institution.

Resources:

- 15 U.S.C. §§ 6801-6809
- 16 C.F.R. part 314
- 12 C.F.R. part 1016
- FTC Guidance - *How To Comply with the Privacy of Consumer Financial Information Rule of the GLBA*
- FTC Guidance - *Financial Institutions and Customer Information: Complying with the Safeguards Rule*
- FDIC Compliance Examination Manual addressing the GLBA

4. Children's Online Privacy Protection Act (COPPA)

Attorneys who advise clients that operate websites or online services, including mobile applications and Internet of Things devices, should be aware of the Children's Online Privacy Protection Act. The COPPA regulates websites and online services that are directed toward children, as well as websites and online services where the operators have actual knowledge of their collection of certain personal information from a child under the age of 13. For instance, it requires children's websites to obtain verifiable parental consent for the collection, use, or disclosure of a child's personal information. In addition, it identifies what should be included in such websites' privacy notices. The Federal Trade Commission enforces violations of this law. However, the COPPA incorporates a self-regulatory Safe Harbor option and a number of approved Safe Harbor organizations exist. For a complete list of these organizations, please refer to the FTC's COPPA Safe Harbor Program website.

Resources:

- 15 U.S.C. §§ 6501-6506
- FTC - COPPA Safe Harbor Program
- FTC Guidance - COPPA
- FTC Guidance – Six-Step COPPA Compliance Plan

5. Telephone Consumer Protection Act (TCPA)

Generally, the Telephone Consumer Protection Act limits unwanted telephone solicitations. It authorized the federal Do Not Call Registry as a system to allow individuals to opt-out of telemarketing calls. In addition, the TCPA places other restrictions on telephone solicitations, such as limitations on unsolicited fax machine advertisements and extensive regulations on the use of automated dialing and prerecorded message systems. In many circumstances, it prohibits the use of an automated dialing system to call cellular telephone numbers for commercial purposes without prior express consent of the called party. Where evolving technologies have made it

easier and less costly for businesses to reach potential customers, attorneys who advise businesses should understand the limitations the TCPA may impose on marketing and other business operations.

Resources:
- 47 U.S.C.§ 227
- 47 C.F.R. § 64.1200
- National Do Not Call Registry
- FCC Guide - TCPA Small Entity Compliance
- FCC Guide – Telemarketing and Robocalls
- FDIC Compliance Examination Manual addressing the TCPA

6. Employee Polygraph Protection Act (EPPA)

The Employee Polygraph Protection Act prohibits private employers from requiring their employees or prospective employees to submit to lie detector examinations. The law may apply to law firms, as well as their clients. The consequences of violating this law include civil penalties, an injunction action by the secretary of labor, and a private civil action for legal or equitable relief. Some exceptions to this general rule exist, such as an exception for investigations of ongoing loss to an employer's business with reasonable suspicion that an employee was involved.

Resources:
- 29 U.S.C. §§ 2001-2009

7. Federal Trade Commission Act

The Federal Trade Commission Act is the source of the FTC's consumer protection authority. The Act prohibits "unfair or deceptive acts or practices in or affecting commerce" and empowers the FTC to enforce this rule. The Act has played a central role in the development and enforcement of consumer information privacy. Deceptive acts prohibited by this law consist of material representations, omissions, or practices that are likely to mislead the consumer acting reasonably in the circumstances. An unfair trade practice includes a practice that causes, or is likely to cause, substantial injury to consumers, which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. The FTC has brought enforcement actions against companies that do not abide by their promises, often in privacy policies, to protect consumer privacy and against companies that engage in unfair trade practices regarding consumers' personal information. Attorneys who advise companies should be aware of the obligations imposed by the FTC for the protection of consumer privacy. As insufficient information security measures can expose a company to liability, companies with the assistance of their counsel should identify practices that may put consumers' personal information at unreasonable risk and take reasonable and necessary steps to safeguard this information.

Resources:
- 15 U.S.C. § 45
- FTC Guidance – A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority
- FTC Guidance – FTC Policy Statement on Deception
- FTC Privacy Report

8. FTC Identity Theft Rule

The FTC Identity Theft Rule, commonly known as "The Red Flags Rule," was issued in 2007 under Section 114 of the Fair and Accurate Credit Transaction Act of 2003. The Red Flags Rule requires certain entities to implement a written identity theft protection program for the purpose of detecting indications (i.e. red flags) of identity theft in the operation of their business.

The Red Flags Rule applies to "financial institutions" and certain "creditors" and requires these entities to periodically evaluate whether they have "covered accounts." A covered account, as explained by the FTC, is:

1. "A consumer account for your customers for personal, family, or household purposes that involves or allows multiple payments or transactions. Examples are credit card accounts, mortgage loans, automobile loans, checking accounts, and savings accounts."
2. "Any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. Examples include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to identity theft. Unlike consumer accounts designed to allow multiple payments or transactions — always considered 'covered accounts' under the Rule — other types of accounts are 'covered' only if the risk of identity theft is reasonably foreseeable."

The applicability of the Red Flags Rules is not industry specific, but is dictated by whether the activities of the business are covered by the relevant definitions of the Rule. If a covered business possesses "covered accounts," it is required to have a written identity theft protection program.

Resources:

- FTC Red Flags Rule (Full Text)
- FTC Red Flags Rule
- Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business

9. Federal Information Security Modernization Act

The Federal Information Security Modernization Act ("FISMA") requires federal agencies to develop and implement an agency-wide program to ensure information security of the agency's data and the systems used by the agency in its operations, even if those systems are managed by another source such as an outside contractor or other federal agency. FISMA also requires each agency—through certain officials—to assess the agency's information security program on an annual basis. FISMA also codified a central information security center (U.S. Computer Emergency Readiness Team (US-CERT)) through which information security incidents must be reported by federal agencies.

Resources:

- Federal Information Security Modernization Act (Full Text)
- US-CERT Federal Incident Notification Guidelines (effective April 1, 2017)

10. Stored Communications Act

The Stored Communications Act ("SCA") was enacted as part of the Electronic Communications Privacy Act of 1986. SCA is a federal law that governs voluntary and compelled disclosure by third-party internet service providers (ISPs) of "stored wire and electronic communications and transactional records." SCA prohibits, and provides criminal penalties for, the unauthorized access, alteration, or prevention of an electronic communication "while it is in electronic storage in a facility through which an electronic communications service is provided." The SCA also prescribes the scenarios in which the government may compel disclosure of customer or subscriber content and information by an ISP.

Resources:

- Stored Communications Act (Full Text)

11. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) is a federal law which forbids the unauthorized access of a protected computer. It also prohibits access in excess of a provided authorization. "Protected" computers may include those used by the United States government, used by a financial institution. or used in interstate foreign commerce. CFAA provides criminal penalties for its violation, as well as a civil private right of action for both individuals and businesses. It is often utilized by companies as a method to protect trade secrets and other proprietary information.

Resources:

- Computer Fraud and Abuse Act (Full Text)

12. Family Educational Rights and Privacy Act (FERPA)

Attorneys who interact with educational institutions should be aware of the responsibilities that these institutions possess regarding the protection of student education records. Privacy and other controls on education records were established in the Family Educational Rights and Privacy Act. The Act provides certain rights over these records to parents of students under the age of 18, students that are over the age of 18, and any student that attends a school beyond high school. It provides for rights regarding the disclosure, review, and correction of educational records. Disclosure of educational records typically requires opt-in consent for disclosure. Some exceptions exist for mere directory information or records disclosure to a school official with a legitimate and educational interest. While there is no private cause of action for a violation of the Act, complaints are reported to and violations are enforced by the U.S. Department of Education.

Resources:

- 20 U.S.C.§ 1232g
- 34 C.F.R. part 99
- Fl. Stat. § 1002.22
- Department of Education: General FERPA Guidance

13. Driver's Privacy Protection Act (DPPA)

This law regulates the disclosure and collection of motor vehicle records and the personal information contained therein. It not only applies to states, who originally possess this information, but also to anyone who obtains, discloses, or uses personal information from a motor vehicle record for a purpose not permitted by the law. Some permissible purposes include uses by insurers for underwriting, uses relating to litigation, and uses by any requester of the motor vehicle record where the requester demonstrates written consent of the individual to whom the information pertains. Civil liability and criminal fines may extend to those who violate this law.

Resources:

- 18 U.S.C. §§ 2721-2725

II. SELECTED STATE PRIVACY LAWS

1. Florida Information Protection Act

The Florida Information Protection Act ("FIPA") imposes legal requirements on covered entities (including lawyers and law firms) that acquire, maintain, store or use personal information of Florida citizens or residents. "Personal information" includes an individual's last name, in combination with certain key identifiers (such as social security number, driver's license number, financial account numbers, insurance policy numbers). It also includes online login account credentials, medical history, mental/physical condition or medical treatment. Note that the statutory definition of "personal information" excludes information that is already public or is encrypted, de-identified,

or otherwise renders the information unusable. FIPA establishes data breach notification requirements, requires "reasonable" data security measures, addresses proper disposal of records, and imposes civil fines and penalties for violations of the statute.

Resources:

- Florida Statutes, Section 501.171 et seq.

2. Computer Abuse and Data Recovery Act

The Computer Abuse and Data Recovery Act ("CADRA") provides a civil remedy to business owners (including lawyers and law firms) who suffer harm or loss due to unauthorized access to their computers or to information stored on their computers. CADRA's prohibitions include unauthorized access to information on a protected computer, causing harm by transmitting a program (i.e. malware, viruses, etc.), code, or command to a protected computer, or trafficking in any "technical access barriers" (i.e. passwords) through which a protected computer might be accessed without authorization. A party bringing suit under CADRA may recover lost profits, economic damages, and profits gained by the violator. It may also seek injunctive relief to prevent further violations. CADRA also provides for reasonable attorney fees to the prevailing party.

Resources:

- Florida Statutes, Section 668 et seq.

3. Student and Parental Rights and Educational Choices statute

Florida's Student and Parental Rights and Educational Choices statute includes a provision that recognizes the rights of parents to assert privacy rights over student records of their children. To the extent that an attorney seeks or maintains such records in the course of practice, this statute should be reviewed.

Resources:

- Florida Statutes, Section 1002.22

III. PRIVACY IN FLORIDA RULES OF PROCEDURE

1. Florida Rule of Judicial Administration 2.425: Minimization of the Filing of Sensitive Information

The Florida Rule of Judicial Administration 2.425 regulates the filing of designated sensitive information with Florida's state courts. Certain sensitive information, such as dates of birth, driver's license numbers, telephone numbers, and taxpayer identification numbers, may have a limited portion filed as prescribed by the Rule. Other sensitive information, such as social security numbers, bank account numbers, and credit card numbers, may not have any portion filed. Certain exceptions exist for these requirements, such as when the information is relevant and material to an issue before a court. A court may order sanctions for a failure to comply with these requirements.

Resource:

- Fla. R. Jud. Admin. 2.425