TEXASLAW

UT LAW CLE

Regulatory and Ethical Considerations for Handling Sensitive Electronic Information

Adrian Senyszyn, Brin & Brin P.C.

Shawn E. Tuma, Spencer Fane, LLP

TEXASLAW

UT LAW CLE

Overview

- Federal Laws Applicable to Sensitive Electronic Information
  - Federal Trade Commission Act
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §1301 et seq.) and HITECH provisions of the American Recovery and Reinvestment Act of 2009 ("ARRA")
- Notable Texas Laws Applicable to Sensitive Electronic Information
- Other Considerations when Handling Sensitive Electronic Information

FTC Act

Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act)

- Consumer protection law that prohibits unfair or deceptive practices
  - Fights consumer fraud and identity theft
  - Telemarketing and internet scams or deceptive practices
  - Applied to offline and online privacy and data security policies
    - Spam, spyware, social networking, pretexting, peer-to-peer sharing
- InMobi Settlement
  - Singapore-based mobile adverting company
  - $950,000 civil fines and penalties
  - Deceptively tracking customers – including children – without consent

Source: https://www.ftc.gov/reports/privacy-data-security-update-2016 (last visited July 9, 2018)

TEXASLAW UT LAW CLE

FTC Act

Federal Trade Commission Act (Continued)

- Data Security
  - Companies engaged in unfair or deceptive practices that place consumers' personal data at unreasonable risk
  - Requirement to notify consumers in the event of a data breach
    - Hacker takes personal information from computer
    - Insider who steals consumer information
    - Sensitive information accidentally posted online
  - Other Requirements
    - Secure operations
    - Fix the vulnerability
    - Determine other legal requirements

Source: https://www.ftc.gov/reports/privacy-data-security-update-2016 (last visited July 9, 2018)

FTC Act

Federal Trade Commission Act (Continued)

- Health Breach Notification Rule (Gap Filler for HIPAA)
  - Purpose to require businesses not covered by HIPAA to notify customers and others if there a breach of unsecured, individually identifiable electronic health information
  - Rule applies to vendors of personal health records (PHR), PHR-related entity, or a third-party service provider
  - Notification requirement triggered if there is an unauthorized acquisition of PHR that is unsecure and in a health record
    - Each affected U.S. citizen or resident
    - Federal Trade Commission
    - Media, in some cases

Source: 16 CFR 318; https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule (last visited July 9, 2018); https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/health-breach-notification-rule (last visited July 9, 2018);

TEXASLAW UT LAW CLE

HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §1301 et seq.) and HITECH provisions of the American Recovery and Reinvestment Act of 2009 (ARRA)

- Regulates protected health information (PHI)
- Requires notification if there is a breach of PHI resulting in more than a low probability of harm to the information
- "Breach" is an impermissible use or disclosure that compromises security or privacy of unsecured protected health information (PHI)

Title search: Regulatory and Ethical Considerations for Handling Sensitive Electronic Information

Also available as part of the eCourse
2018 Advanced Texas Administrative Law eConference

First appeared as part of the conference materials for the
13th Annual Advanced Texas Administrative Law Seminar session
"Regulatory and Ethical Considerations for Handling Sensitive Electronic Information"