Data Security and Privacy: Contractual Considerations

Presented by:

Sarah Hutchins, CIPP/US

November 19, 2020

Parker Poe

ACC Association of Corporate Counsel

parkerpoe.com

Webinar Housekeeping

- **Audio** – Select your listening preference in the Audio pane. Listen through your computer system or by dialing in on the phone.
- **Questions** – Type your questions for the speaker into the Questions pane (right side of your screen), and we will address at the end of the webinar.
- **Resources** – A replay of the webinar and the slides will be emailed following the webinar.
- **Continuing Education** – The ACC-CLT Chapter will submit CLE in NC and provide attendance certificates for out-of-state submissions. Contact us if you want to have your attendance submitted for CLE to SC or GA at ParkerPoe@ParkerPoe.com.

Webinar Housekeeping

- **Legal disclaimer** - Portions of this communication may qualify as “Attorney Advertising” in some jurisdictions. However, Parker Poe intends for this communication to be used for educational and informational purposes only. This communication is not intended and should not be construed as legal advice. For questions, contact us at ParkerPoe@parkerpoe.com.

Today's Presenter

Sarah Hutchins, CIPP/US

Parker Poe

SarahHutchins@parkerpoe.com

704.335.6639

- Legal practice includes business litigation, government investigations, and data privacy
- Recognized by the IAPP as a Certified Information Privacy Professional/United States (CIPP/US), which is the gold standard for privacy professionals in America

Session Overview

- Select Statutory Requirements
- General Contractual Principles
- Privacy Notice
- Employer/Employee Interactions
- Litigation
- M&A

Contractual Requirements in the Law

- Federal Regulations
  - Health: HIPAA
  - Financial Institutions: FCRA/FACTA/GLBA
  - FTC Act
- State Statutes
  - CCPA
- International Data Protection Laws
  - GDPR
- *Plus Civil Litigation*

Federal: HIPAA

- Covered Entity:
  - Health plans
  - Health care clearinghouses
  - Health care providers
- Business Associates:
  - A person or organization
  - Not a covered entity
  - Performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.
- Business Associate Agreements:
  - Covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.

Federal: Financial Institutions

- FCRA: Fair Credit Reporting Act
  - *Furnishers* that send information to CRAs regarding creditworthiness must develop written policies and procedures regarding accuracy and integrity of information furnished
  - *Users* may need written authorization to request a report
- FACTA: Fair and Accurate Credit Transactions Act
  - Red Flag Rules: financial institutions and creditors are required to create and implement a written Identity Theft Prevention Program to help detect and prevent identity theft.
    - Creditors and financial institutions are to take “reasonable measures to protect against unauthorized access to or use of consumer information” by means of proper disposal.
- GLBA: Gramm-Leach-Bliley Act
  - Written Information Security Program
  - Safeguards Rule and Privacy Rule
    - Vendor due diligence and required contract provisions to third parties permitted access to financial institution’s customer
    - Written contracts with joint marketers/ third parties provided non public personal information

Federal: FTC Act

- Bars unfair and deceptive acts and practices in or affecting commerce
  - Violations of consumers' privacy rights
  - Instances where consumers have been mislead
  - Failure to maintain security for sensitive consumer information
- Enforcement actions and Consent Orders
  - *November 9, 2020* Consent Order with Zoom
    - Security features
    - Collection practices
    - Protection of Covered Information from unauthorized access
    - Information Security Program and document compliance

Federal: The Future

- Many contenders
  - Republican sponsored Consumer Data Privacy and Security Act of 2020 (USCDPA) and SAFE Data Act
  - Democrat sponsored Consumer Online Privacy Rights Act (COPRA)
  - COVID associated bills
- Differences
  - Preemption
  - Private Right of Action

State: California Consumer Privacy Act (CCPA)

The CCPA applies to a business entity if it:

1. Operates for profit;
2. Collects personal information of California residents;
3. Does business in California (including online sales and marketing); and
4. Satisfies at least one of the following:
   a) Has annual gross revenues in excess of $25 million;
   b) For a commercial purpose, collects, buys, sells, or shares the personal information of 50,000 or more California residents, households, or devices on an annual basis; or
   c) Derives 50% or more of its annual revenues from selling California residents' personal information.

State: CCPA

Contractually focused requirements

- Covered Entities and Service Providers
  - Absence of a contract indicates that information is not being shared with a “service provider”
  - Contract must include
    - Service provider will not retain, use, or disclose personal information for any purpose other than performing contract services
    - Limit the collection, **sale**, or use to that necessary for a “business purpose”
    - Read and understand CCPA requirements
  - Third Party Sharing
    - May require disclosures to a customer
    - Notice must be provided before “selling” personal information

State: CCPA

Contractually focused requirements continued

- Privacy Policy and other notices
  - Right to request disclosure of collection and sales
  - Right to a copy of specific personal information collected in the 12 months prior
  - Right to deletion
  - Do Not Sell
  - Protection from discrimination
  - Annual Update
- Existing Law (California Online Privacy Protection Act)
  - categories of personally identifiable information collected/third parties receiving information
  - describe how a site visitor can access and change information previously submitted
  - describe how the operator notifies consumers of changes to the privacy policy
  - effective date
  - describes how the operator responds to do-not-track signals from a user's browser
  - disclose interaction with third party websites

State: Other Considerations

- Industry Specific
  - *e.g.* New York Department of Financial Services Cybersecurity Regulation
- Privacy Policies
- Written Breach Response Plans
  - Massachusetts (written information security program)
- Data Brokers
  - Vermont (annual registration and security program)
- Employee Interaction
  - FCRA
  - Monitoring

International Laws: GDPR

- Data Processing Agreements:
  - Article 28 of the GDPR generally requires a written contract between a “controller” and “processor” to govern the processing of personal data
    - subject matter and duration
    - nature and purpose
    - type of personal data and categories of data subject
    - controller’s rights and obligations
    - commitment of confidentiality
    - processor will comply with the GDPR and assist with the controller’s GDPR compliance
    - process personal data only on the documented instructions
    - “adequate security”
    - assist with data subject rights
    - appropriate breach notification
    - end of contract terms
    - audits and inspections
- Data Transfers

Data Agreement Clauses

- Permitted Use and Disclosure
  - Categories of information: confidential versus PI
- Security and Confidentiality Protections Required*
  - Collection
  - Storage
  - Destruction
  - Audit
- End of Contract Terms
- Data Breach Protocol*
- Contract Breach and Remedies
- Indemnification*
- Liability Caps*
- Insurance
- Choice of Law

Vendor Due Diligence Questions

- Referrals and references
- General financial viability/business continuity/insurance
- What type of training programs/privacy policies does the company use?
- Company certifications?
- Company breaches in the past?
- Company and network infrastructure
- IT controls
- Where is the data being transferred/stored? Within U.S. or outside?
- Technology in use for collection, etc.
    - Automated phone calls, emails, video/web conferencing tools, network

Contract Terms: Security and Breach

- Security
  - Authorized Personnel and oversight
  - Categories of data/personal information/confidential information
  - Standard of Care
    - appropriate use, storage, retirement, and destruction
  - Sharing and sub-contractors
  - Security contact
  - Compliance with the law
  - Compliance with ISO, PCI-DSS, NIST encryption standards
- Data Breach Notification
  - Define Security Breach
    - Act or omission that compromises data, unauthorized access, etc.
  - Notice (time, method)
- Data Breach Investigation and Remediation
  - Cooperation, Access, Interviews, Relevant Records, Logs, Reporting, etc.
  - Expenses

Contract Terms: Indemnification

Indemnification. Service Provider shall defend, indemnify, and hold harmless Customer [and Customer's parent company] and [its/their] subsidiaries, affiliates, and [its/their] respective officers, directors, employees, agents, successors, and permitted assigns (each, a "**Customer Indemnitee"**) from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any Customer Indemnitee arising out of or resulting from Service Provider's failure to comply with any of its obligations under [this Section/[SECTION NUMBER]].

Data Security Contract Clauses for Service Provider Arrangements (Pro-Customer), Practical Law Standard Clauses 2-505-9027

Contract Terms: Liability Cap

- Monetary Limitation
  - Set amount or based on duration of fees on a contract term
  - Notification costs/Substitute Notice
- Damage Type Limitation
  - Direct
  - Consequential, Lost Profit, Punitive, Special, Indirect, Reputational Harm
- Confidentiality versus Data Breach
- Enforceability

Privacy Policies:
Contracts with Your Consumers and Customers

- Presentation
  - Accessible and Layered
- Type of information collected and the purpose
- Data storage, security, access, and sharing
- Use of Cookies
  - Consider separate Cookie Policy
  - Information collected and purpose of collection
- Use of third-party service providers (Google Analytics, Salesforce, etc.)
- Affiliated sites
- Opt-Out and Logistics
  - Provide individual use information and delete throughout the network
- Contact information

Employment:
Contracts and Policies with Your Employees

- Employment Agreement
  - Confidentiality
  - No unauthorized data
  - Training
- Computer Use Policies
- Mobile Device Policies (BYOD and MDM)
- Data Storage Policies
- External drives and cloud storage
- International Travel Policies
- Document Retention Policy
- Breach/Disaster Response Plan

Employment:
Computer Use

- Approved Uses
- Outline Security Measures
  - Storage
  - Labeling
  - Encryption
  - Lost/Compromised device or material
  - Portable Devices
  - External Sites (Gmail, DropBox)
- Require Approvals
  - for Internet downloads to make system changes, to run executable files or to add/delete programs
- Prevent introduction of “anti-forensics” and other harmful programs
- Standardize workstations to mitigate against introduction of malware/viruses

Litigation

- Confidentiality Agreements
- Protective Orders
- Data Security Agreements
- Protected Transfers
- Metadata
- Public Records Disclosure
- Data Destruction & Returns

Mergers and Acquisitions

- All policies and procedures that govern data security and privacy
- Categories of personal information collected
- Reports from third-party vendors
- Identification of third-party vendors with whom personal information is shared
- Demands, complaints, claims, litigation, or enforcement actions related to data security, information privacy, or data management
- Data breach history
- Network topology map
- Employee personal device usage
- Encryption practices
- Cyber Insurance
- Compliance efforts
- Automated marketing efforts

Contact

Sarah Hutchins, Partner

sarahhutchins@parkerpoe.com | 704.335.6639

linkedin.com/in/sarah-hutchins-504a2938

Parker Poe Adams & Bernstein

620 S Tryon St., Suite 800

Charlotte, NC 28202

Tel: (704) 372-9000