Strafford

Presenting a live 90-minute webinar with interactive Q&A

Data Privacy and Security Agreements: Defining, Allocating, and Mitigating Risks From Data Security Breaches

TUESDAY, MARCH 29, 2022

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Michael R. Overly, Partner, **Foley & Lardner LLP**, Los Angeles

Susan L. Ross, Senior Counsel, **Norton Rose Fulbright US LLP**, New York

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

Recording our programs is not permitted. However, today's participants can order a recorded version of this event at a special attendee price. Please call Customer Service at 800-926-7926 ext.1 or visit Strafford's website at www.straffordpub.com.

Data Privacy and Security Agreements: Defining, Allocating, and Mitigating Risks From Data Security Breaches

Michael R. Overly, Esq., CISA, CISSP, COP, CIPP, ISSMP, CRISC
Foley & Lardner LLP

Susan L. Ross
Norton Rose Fulbright US LLP

Agenda

- Introduction
- Overview of Information Security
- Regulatory: Privacy and Security Requirements
- Three Tools for Better Protecting Data Entrusted to Third Parties
  - Vendor Due Diligence
  - Contractual Provisions
  - Information Handling Practices
- Negotiation tips

Information Security Risks Are At An All Time High

- In the last year, there were almost a dozen major incidents in which personal information has been severely compromised.
- According to the FBI, incidence of hacking and **insider** misappropriation or compromise of confidential information is at an all time high.
  - Insiders include not only the company's own personnel, but also its contractors and business partners

Information Security Risks Are At An All Time High

- FTC, OCC, HHS, DHS, SEC, and other regulators increasingly focusing on information security.
  - States becoming increasingly active in this area.
- Possibility of FTC, AG, and other regulatory action at an all-time high.
- Sanctions can scale to the millions of dollars
  - Not only in the U.S., but also European regulators

Overview: Information Security

- Security measures can be divided into three categories:
  - **Administrative**: policies, procedures
  - **Technical**: firewalls, intrusion detection systems, encryption
  - **Physical**: secure doors and facilities, video monitoring, security guards.
- Some privacy/security laws and regulations use this very language.

Privacy and Security Requirements

- HIPAA
- Data breach laws
  - Cybersecurity protection: NY SHIELD Act/California/Mass.
  - CCPA and CPRA
  - CO/VA/Utah
- PCI-DSS credit cards
- FTC Act “Unfair and Deceptive Practices”
- FERPA
- GDPR and personal data belonging to non-US residents

Regulatory Language Should be Treated as a Floor

- Including the HIPAA, GLB, and other statutory/regulatory minimally-required security language, without more, does not adequately protect companies.
- Even the more robust language provided in laws and regulations (e.g., HIPAA Security Rule, GLB Safeguards Rule, etc.) does not provide sufficient protection.
- PCI expressly designed as “floor”

Vendor Contract Protections Not Optional

- Security protections in vendor agreements are required by law:
  - GLB
  - HIPAA/HITECH
  - Massachusetts, California, Colorado, Virginia, etc.
  - New York Cybersecurity Rule for financial institutions
  - PCI DSS
  - GDPR

Types Of Contracts/Relationships

- When do we need to think about info sec?
- Any agreement under which a third party will have access to the company's:
  - Network
  - Facilities
  - Data
- Access can be remote or physical
- Litmus test

Scaling of Security

- Security isn’t an all or nothing proposition.
- Protections must scale to meet the risk.
  - Fees should not be part of the analysis.
- Data security regulations and laws written in terms of scaling.

Scaling of Security

- Massachusetts Data Security Law:

". . . safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information."

Scaling of Security

- New York SHIELD Act:

"Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data."

- New York Attorney General entered into a $600,000 settlement in January of 2022

Scaling of Security

- HIPAA Security Rule: Factors to consider:

  (i) The size, complexity, and capabilities of the Covered Entity.

  (ii) The Covered Entity's technical infrastructure, hardware, and software security capabilities.

  (ii) The costs of security measures.

  (iv) The probability and criticality of potential risks to ePHI.

3 Tools for Better Protecting Data Entrusted to Third Parties

Common errors

- ✓ Failure to involve all relevant stakeholders in the process
- ✓ Failing to assess the unique requirements of the transaction at-hand
  - ✓ Example: Mobile applications
- ✓ Inflexibility

Three Step Approach

1. Vendor due diligence
2. Contractual protections
3. Information handling procedures and requirements, generally in the form of contract exhibits

Step One: Due Diligence

- From the outset, Vendors must be on notice that the information they provide as part of the company's information security due diligence will be (i) relied upon in making a vendor selection; and (ii) part of the ultimate contract.
- To ensure proper documentation and uniformity in the due diligence process, companies should develop a "Vendor Due Diligence Questionnaire."

Step Two: Contractual Protections in Underlying Services Agreement

- NDA or Confidentiality Clause
  - Language should be broadly drafted to include all potential confidential information
- Marking requirements disfavored
- Perpetual protection for NPI
- Ongoing protection of trade secrets
  - Terms on NDAs have been held to limit trade secret protection

Step Two: Contractual Protections

- Standard of care for confidentiality:
  - Vendor shall treat Customer Confidential Information as strictly confidential and shall use the same care to prevent disclosure of such information as it uses with respect to its own most confidential or proprietary information, but in no event less than reasonable care.
  - Vendor shall treat Customer Confidential Information as strictly confidential and shall use the same care to prevent disclosure of such information as it uses with respect to its own most confidential or proprietary information, **which shall not be less than the standard of care imposed by state and federal laws and regulations relating to the protection of such information and, in the absence of any legally imposed standard of care,** the standard shall be that of a reasonable person under the circumstances.

Step Two: Contractual Protections

- Warranties
  - Compliance with best industry security practices
    - The more stringent of applicable law and regulations or best industry practices
  - HIPAA/HITECH compliance
  - GLB compliance
  - Red Flag/Identity Theft

Step Two: Contractual Protections

- Warranties
  - Other state and federal consumer protection/privacy laws
  - Compliance with Privacy policy
  - Personnel not convicted of crimes of dishonesty
  - Performance of services outside the US
    - Beware support personnel located outside the US
    - Do you have any geographic constraints?
  - Transmission of confidential information outside the US or expressly authorized countries.

Step Two: Contractual Protections

- Vendors who are already subject to outside certifications or regulation
  - Vendors who are “PCI DSS Compliant”
  - Vendors who are ISO 27001/27002 certified
  - Vendors who are regulated entities
    - Consumer reporting Agencies
    - Financial services companies under GLB
    - Covered Entities under HIPAA
    - Business Associates under a Business Associate Agreement
    - Processors under GDPR
- Certifications and regulatory obligations are an important **part** of overall protection.

Step Two: Contractual Protections

- Use of subcontractors
  - Strictly limit (exceptions for generic service providers)
  - Approval required
  - Joint and several liability
    - Avoid provisions attempting to prevent actions against suppliers and contractors.
  - Due diligence
  - Check for regulatory requirements: HIPAA, GDPR, CCPA

Step Two: Contractual Protections

- Use of subcontractors to provide critical functions – hosting providers, outsource partners, etc.
  - Far greater need for due diligence
  - Potential use of a “continuity agreement”
  - Control over changes in these types of critical service providers
    - Ample notice of change
    - Assistance in conducting diligence
    - Termination right
    - Transition services

Step Two: Contractual Protections

- For critical subcontractors, even if not required, consider use of specialized “Subcontactor NDA”
  - Creates privity of contract
  - Ensures subcontractor is on notice of obligations
  - Describes relationship between and among the parties
  - Where appropriate, include specific security requirements in addition to baseline confidentiality

Step Two: Contractual Protections

- Personnel due diligence - Background checks and screening
  - Scope restricted by applicable law
  - Generally never want to receive copies of screening results
  - Reassign personnel who fail required check, without disclosure of names
  - Reserve right in relevant engagements to conduct your own background check for onsite vendor personnel.
  - Government contractor requirements

Step Two: Contractual Protections

- Control of Personnel
  - Ability to request removal of non-performing personnel or any personnel that present a security threat.
  - Consistency of staff over the term of the project
    - Immediate notice of termination or reassignment.
  - Question vendor about turnover rates, particularly foreign vendors
  - Reserve right to fingerprint and search all items brought into or out of your facilities.
  - Reserve the right to monitor and review all use of your systems by vendor personnel

Step Two: Contractual Protections

- Control of Personnel
  - Compliance with facility access and security policies
  - Vendor identification card
  - Access scheduling
  - Escorts required
- General Audit Provision
  - Permit audit of vendor compliance with contract terms, including confidentiality, security, personnel, etc.
- No Removal of Data
  - WFH issues

Step Two: Contractual Protections

- General Security Obligations
  - Take all reasonable measures to secure and defend its systems and facilities from unauthorized access or intrusion
  - Periodically test systems and facilities for vulnerabilities
  - Immediate reporting of breaches
    - Define “breach” or “incident” – include insiders
    - Cooperation with customer/forensic investigator
  - Joint security audits
  - Regulatory access and compliance
  - Firewalls, antivirus, use of VPNs, on-demand access
  - Changes in law
- Termination for compliance issues

Step Two: Contractual Protections

- Indemnity -- Protection from third party claims
  - Breach of confidentiality
  - Failure to comply with security requirements
- Exceptions to Limitation of Liability
  - Breach of confidentiality
  - Indemnity
  - Use of name
  - Misappropriation of intellectual property
- Limitations of liability
  - Third party and first party claims

Step Two: Contractual Protections

- Security-specific Exceptions to Limitation of Liability
  - Gross negligence and willful misconduct
  - Damage to, impairment of, disablement of, or loss of use of any computer system, hardware, software, data, tangible property, or any other property caused by an act or omission of vendor
  - Any fines, fees or assessments imposed on licensee by a third party or governmental authority as a result of vendor's actions or inactions

Step Two: Contractual Protections

- Security Breach Notification For PII - - Associated Costs
  - Ensure prompt notice from vendor of potential breach to ensure your ability to comply with applicable laws (i.e., avoiding eleventh hour notices).
  - Control of notice
  - Allocate responsibility for costs to vendor
- Control all other public statements.

Step Two: Contractual Protections

- Insurance
  - Workers Compensation
  - Commercial General Liability
  - Commercial Automobile
  - Commercial Blanket Bond, including Electronic & Computer Crime or Unauthorized Computer Access coverage
  - Professional Liability Insurance (Errors and Omissions)
  - Cyber
  - Blanket bond

Step Two: Contractual Protections

- Due Diligence Questionnaire
  - Attach as an exhibit and incorporate into the agreement.
  - Include means to be notified of material modifications to responses.
  - Ensure vendor will not materially reduce the security protections reflected in the Questionnaire.
- Information Handling Requirements (Step Three)
- Annual certification of compliance

Step Three: Information Handling Requirements

- Where appropriate, attach specific information handling requirements in an exhibit
  - Securing PII
  - Encryption
  - Secure destruction of data
  - Securing of removable media
  - Communication and coordination

Negotiation Tips

- Raise security requirements from the outset, including liability expectations
- The way in which the requirements are presented to the vendor is key
- In many cases, it is necessary to educate the vendor about legal/regulatory requirements
- Major push-back to baseline technical requirements is common and almost never difficult to overcome
- Flexibility is frequently required, but generally only for a narrow range of requirements

Negotiation Tips

- Service levels and service level credits
- Create a ready library of “plug-and-play” alternatives to standard required terms
- Addressing the common argument that “we cannot change the way we secure our systems for a single engagement”
- Addressing the argument that baseline security requirements somehow prevent the vendor from evolving its security standards

Negotiation Tips

- Moving target language
- “Industry best practices” provisions
- Compliance with laws/regulations that may not directly apply to the vendor’s business

Post-Execution Follow-up

- Ongoing policing of vendor performance and compliance is crucial
  - Audit rights
  - Access to third party audit reports (e.g., SAS 70 Type II)
  - Updating of due diligence questionnaire is key
- Annual compliance statement

Questions?

Contact Information

Michael R. Overly, Esq., CISA, CISSP, ISSMP, CIPP
Information Technology and Outsourcing Group
Foley & Lardner LLP
555 South Flower Street
Suite 3500
Los Angeles, California 90071
(213) 972-4533
moverly@foley.com

Contact Information

Sue Ross

Senior Counsel

Norton Rose Fulbright US LLP
1301 Avenue of the Americas,
New York, New York 10019-6022

212-318-3280

Susan.ross@nortonrosefulbright.com

Disclaimer