COOLEY LLP PRESENTS

CLOUD COMPUTING IN HEALTHCARE: HIPAA AND STATE LAW CHALLENGES

May 20, 2014

attorney advertisement

Five Palo Alto Square, 3000 El Camino Real, Palo Alto, CA 94306

The information summarized in the chart is related to select public government settlements. It is based solely on public sources on file with author. Contact wgoldstein@cooley.com or lroffman@cooley.com for more information.

Cooley

Cooley LLP

Cloud Computing in Healthcare

Matt Karlyn, Partner, Boston
Phil Mitchell, Special Counsel, New York
Leah Roffman, Associate, New York

May 20, 2014 | Cooley LLP | New York

attorney advertisement

AGENDA

- **Current HIPAA Landscape**
  - Recent HIPAA Enforcement
  - Omnibus Rule Compliance
- **HIPAA and Cloud Computing**
  - HIPAA Considerations of Cloud Computing
  - BAAs with Cloud Computing Vendors
- **Contracting for Cloud-based Services**

Current HIPAA Landscape: Recent HIPAA Enforcement

- **Background on HIPAA Enforcement**
  - Covered Entities vs. Business Associates
  - Office for Civil Rights ("OCR") vs. State Attorney Generals
  - Audits vs. Enforcement Actions
- **OCR Audits**
  - 2012: Pilot Program
    - 115 Covered Entities audited
    - Many had insufficient HIPAA compliance programs
  - 2014: OCR announced plans to resume audit program
    - Survey 800 CE's and 400 BA's to select audit targets
    - Preparation for potential audit

- **Recent OCR Enforcement**

  - 4 public settlements in 2012
  - 6 public settlements in 2013
  - 5 public settlements *thus far* in 2014

    - <u>County fined $215k</u>
      - ePHI of ~1,600 people inadvertently moved to a public server
      - OCR investigation revealed non-compliance
      - 3 year Corrective Action Plan

    - <u>Health Plan fined $250k</u>
      - Unencrypted laptop containing ePHI of ~150 people stolen from employee's car
      - OCR investigation revealed non-compliance
      - 2 year Corrective Action Plan

- **Recent OCR Enforcement**
  - 5 settlements thus far in 2014 (cont'd)
    - Health care company fined $1.7M
      - Unencrypted laptop stolen from a physical therapy center
      - OCR investigation revealed non-compliance
      - 2 year Corrective Action Plan
    - Two providers fined ($1.5M and $3.3M respectively)
      - Computer server errantly reconfigured, resulting in public disclosure of ePHI of ~6,800 people
      - OCR investigation revealed non-compliance
      - 3 year Corrective Action Plan for each provider

- **Themes from recent OCR Enforcement**
  - All types of Covered Entities
  - Security is a key concern – especially encryption
    - Following enforcement actions regarding theft of unencrypted laptops, Susan McAndrew of OCR stated: "Our message to these organizations is simple: encryption is your best defense to these incidents."
  - Non-compliance beyond initial Breach

- **State Enforcement**
  - HITECH Act empowered State Attorney Generals to enforce HIPAA
    - 2013: MA AG fined 4 provider groups and a medical billing practice $140k for disposal of ~67,000 patients' medical records at a public dump
    - 2012: MA AG fined hospital when 472 boxes of unencrypted backup computer tapes containing PHI of ~800,000 patients did not arrive at vendor planning to erase and resell tapes
      - $250k fine; $225k contribution to AG's Education Fund; $275k credit to reflect security measures undertaken
      - Mandatory CAP
    - 2012: MN AG fined debt collector (BA) for theft of laptop containing ~23,000 patients' records
      - $2.5M fine – placed in restitution fund for patients
      - Company barred from doing business in MN for 2 years

Current HIPAA Landscape: Omnibus Rule Compliance

- **Omnibus Rule**
  - Requires certain changes to HIPAA compliance programs
  - Two key changes that apply to both BAs and CEs:
    - Changes to BAAs
      - BAAs entered into pre-Omnibus Rule and not modified since must be updated to comply with the Omnibus Rule by 9/22/14
      - Must include breach reporting, BA's compliance with the Security Rule, BA's compliance with CE obligations where applicable
      - No required notification of HHS upon breach of BAA that cannot be cured

- **Omnibus Rule**
  - Key changes that apply to both BAs and CEs (cont'd):
    - Changes to Breach definition
      - "The acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA which compromises the security or privacy of the PHI"
      - Such improper acquisition, access, use, or disclosure is presumed to be a Breach unless the entity demonstrates a low probability that the PHI has been compromised based on a risk assessment of at least:
        - Nature and extent of the PHI involved;
        - Unauthorized person who used or received the PHI;
        - Whether the PHI was actually acquired or viewed; and
        - Extent to which the risk to the PHI has been mitigated

Cooley LLP

- **Cloud Storage Providers as Business Associates**
  - Omnibus Rule clarified that cloud storage providers are BAs
    - Definition of a BA changed to be an entity that "creates, receives, *maintains, or transmits* protected health information…"
    - "A data storage company that has access to Protected Health Information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis."

HIPAA and Cloud Computing: BAAs with Cloud Computing Vendors

Cooley LLP

- **BAAs with Cloud Storage Providers**
  - Proper documentation
  - Completion of a risk analysis
  - Importance of encryption
  - Assigning liability

Essentials of Cloud Computing

- So what is cloud computing anyway and why do I need to care about my cloud agreements???
- For purposes of this presentation we will talk mostly about Software-as-a-Service (software applications provided to the customer over the internet as a service)
- Other types of cloud-based solutions include Infrastructure-as-a- Service (IaaS), Platform-as-a-Service (Paas), and others

Licensing vs. SaaS

- Traditional license
  - Vendor installs the software in the customer's environment
  - Customer has the ability to have the software or hardware configured to meet its needs
  - Customer retains control of the data
- In SaaS contracts
  - Software is hosted by the provider, typically in a shared environment
  - Software configuration is homogeneous across customer base
- Shift in top priorities
  - From configuration, implementation and acceptance (in the licensing world) to service availability, performance, service levels, data security and control (in the cloud world)

Benefits of SaaS Solutions

- Convenience
  - On demand service with little or no installation, configuration, or maintenance of customer software required
- Lower cost
  - Utility or subscription based charges
  - No upfront capital expenditures or license fees
  - Less equipment means less physical space
  - Lower cost for managing an IT staff
- Better processing capability
  - Collection and storage of large quantities of data
- Greater elasticity
  - Customer can rapidly expand and contract its use without financial impact
- Easy, multi-location access
  - Cloud based solutions

Risks of SaaS Solutions

- Network dependency
  - Exposes customers to service disruptions, data bottlenecks, security vulnerabilities, limitations of the internet
- Customer lack of control over data security, privacy, availability, location of data
- SaaS contracts often disclaim liability for service interruptions, breaches of security, loss of data
- Customer remedies may be limited to service credits or customer may have no remedies at all
- Limited customization
- Unsettled rights of customer associated with provider bankruptcy

Evaluating Cloud Computing Risk: Data Sensitivity and the Criticality of the Service

Cooley LLP

- High Risk
  - Mission critical processes utilizing highly sensitive data
- Medium Risk
  - Generally available data that requires high service levels
- Low Risk
  - Not mission critical and generally available data; can accept outages and variable performance

Solutions must be carefully evaluated to ensure the benefits outweigh the risks.

SaaS Agreements

- The SaaS multi-user model generally favors the SaaS provider's use of a standard form agreement
  - In order to make their products cost-effective (a key benefit of cloud-based applications), providers commonly offer a "one size fits all" service (and a "one size fits all contract)
- This often leaves prospective customers with little, if any, room for negotiation
- Click-wrap agreements are common

SaaS Agreements

- Vendor forms commonly give the vendor the right to:
  - Suspend the customer's access to the service or terminate the agreement for no reason, at any time
  - Condition return of data on compliance with terms and conditions of the agreement, some of which might be established in the future
  - Suspend the service without notice
  - Disclaim liability for data security breaches
  - Change the terms of the agreement at any time
  - Provide no limit on the customer's liability
  - Require the customer to indemnify the vendor for claims relating to the customer's use of the service

Identifying all Contract Documents

- All or some portion of a SaaS agreement may be located on the internet
  - As a result, contract may not be “fixed” (i.e., it may change at any time and the provider may not provide notice)
- Customer should make every effort to “fix” the contract in one document
  - Ask that the web page where contract terms are located be printed and attached as an exhibit to the written agreement
  - Add language to the contract making clear that any future changes in those elements must not (i) materially decrease the level of data protection, service support or SaaS performance existing as of the effective date; or
    (ii) impose any materially new or different obligations on the customer
  - Provider should also be required to provide notice to customer of any changes to the agreement
  - Include a termination right in the event a later change materially decreases the level of data protection, service support, SaaS performance, etc., existing as of the effective date

Pre-Agreement Due Diligence

- Diligence is often one of the few protections customers have when choosing among vendors with non-negotiable contracts
- Can the provider meet your company's expectations?
- Diligence can take many forms: site visits, product demonstrations, discussions with vendor personnel, reference site visits, discussions at user groups, industry groups, as well as due diligence questionnaires
- Require provider to complete a due diligence questionnaire
  - Provider's financial condition
  - Existing service levels
  - Ability of provider to meet service levels
  - Service capacity, including capacity issues provider has encountered
  - Physical and logical security
  - Disaster recovery and business continuity plans
  - Redundancy capabilities
  - Ability to comply with applicable regulations

Diligence Questionnaire Example

	Information Security Policy	
18	A formal, documented, mandated, company-wide information security program, including security policies, standards and procedures (collectively "**Security Policies**"), is in effect, monitored, and enforced for your organization.	☐ Not applicable to my environment/situation ☐ Conscious decision not to deploy this practice ☐ Aware this is needed but no actions taken yet ☐ Planned (within 3 mos)/In development,(if checked, please provided details planned ☐ Yes, this exists or occurs today, (If checked please provide a copy of the Security Policies, subject to Customer's confidentiality obligations).
19 **20**	If "Yes" is checked in question 18, do your Security Policies specifically addresses the confidentiality, integrity, and availability of your facilities, systems, and the information in your possession and control.	☐ Not applicable to my environment/situation ☐ Conscious decision not to deploy this practice ☐ Aware this needed but no actions taken yet ☐ Planned (within 3 mos.)/In development ☐ Yes, this exists or occurs today
	If "Yes" is checked in question 18, do you have a formalized training program for your employees with regard to your Security Policies	☐ Not applicable to my environment/situation ☐ Conscious decision not to deploy this practice ☐ Aware this needed but no actions taken yet ☐ Planned (within 3 mos.)/In development ☐ Yes, this exists or occurs today
21	If "Yes" is checked in question 18, has your organization taken steps to create and maintain security awareness for data processing employees and users of systems and networks (such as awards for suggesting good security ideas)?	☐ Not applicable to my environment/situation ☐ Conscious decision not to deploy this practice ☐ Aware this needed but no actions taken yet ☐ Planned (within 3 mos.)/In development ☐ Yes, this exists or occurs today

- ***This presentation contains examples of language that is commonly found in SaaS agreements.***

- ***These examples are not a substitute for legal advice.***

- ***The language to be used in your transactions depends on the particular circumstances of your transaction.***

Service Availability

- If the provider stops delivering services:
  - The customer will have no access to the services (which may be supporting a critical business function)
  - The customer may have no access to the customer's data stored on the provider's systems
- A customer must be able to continue to operate its business and have access to its data at all times
- Vendor's often view multi-tenancy as the best assurance of service availability
  - Unavailability for one means unavailability for all
  - Greater discipline on vendor than contractual remedies?

Service Availability
Disaster Recovery and Business Continuity

- Risk mitigation
  - Provider's requirement to continue service availability in the event of a disaster, power outage or similar event
  - Review the disaster recovery and business continuity plan
- Example:
  - Provider shall maintain and implement disaster recovery and business continuity plans and procedures to ensure the continuing Availability of the Services in accordance with this Agreement during a Disaster. Customer shall be provided with a copy of each such plan and procedure and any updates thereto during the Term of this Agreement. All requirements of this Agreement, including those relating to security and training, shall apply to the Provider disaster recovery and business continuity, or any other backup, site.

Service Availability
Disaster Recovery Business Continuity (Example)

1. **Disaster Recovery/Business Continuity**. Vendor shall maintain a Business Continuity and Disaster Recovery Plan for the Services (the "**Plan**"), and implement such plan in the event of any unplanned interruption of the Services. On or before the Effective Date, Vendor shall provide Company with a copy of Vendor's current Plan, revision history, and any reports or summaries relating to past testing of the Plan. Vendor shall actively test, review, and update the Plan on at least an annual basis using American Institute of Certified Public Accountants standards and other industry best practices as guidance. Vendor shall promptly provide Company with copies of all such updates to the Plan. All updates shall be subject to the requirements of this Section. In any event, any future updates or revisions to the Plan shall be no less protective than the plan in effect as of the Effective Date. Vendor shall notify Company of the completion of any audit (e.g., ISO 9000) of the Plan and promptly provide Company with a copy of the audit report and reasonable evidence that any identified deficiencies have been corrected. Vendor shall also promptly provide Company with copies of all reports and/or summaries resulting from any testing of the Plan. If Vendor fails to reinstate the Services within the periods of time set forth in the Plan, Company may in addition to any other remedies available hereunder, in its sole discretion, immediately terminate this Agreement as a non-curable default under Section] (Term and Termination). Vendor shall maintain disaster avoidance procedures designed to safeguard Company's data and the data processing capability, and availability of the Services, throughout the Term. The provisions of Section (Force Majeure) shall not limit Vendor's obligations under this section.

Service Availability
Withholding of Services

Cooley LLP

- SaaS agreements commonly contain provisions prohibiting the supplier from withholding services, except in extreme cases (e.g., repeated failure to pay, etc.)
- Example:
  - Provider warrants that, during the Term of this Agreement and during the term of any termination assistance services, it will not withhold Services provided hereunder for any reason, including, but not limited to, a dispute between the parties arising under this Agreement, except as may be specifically authorized herein.
- It is common to carve out the customer's repeated failure to pay undisputed fees in accordance with the terms of the agreement

Service Availability
Financial Stability

- Many SaaS providers are small, emerging companies
- If the customer is not confident in the provider's financial stability, add a provision that enables the customer to identify the provider's financial issues in advance
- Include a termination right if the provider goes bankrupt or experiences a similar event
- Include a transition assistance provision

Service Availability
Financial Stability

- Example:
  - Quarterly, during the Term, Provider shall provide Customer with all information requested by Customer to enable Customer to assess the overall financial stability and strength of the Provider and Provider's ability to fully perform its obligations under this Agreement. Customer may, upon notice to Provider, immediately terminate this Agreement if Customer concludes that Provider does not have the financial ability to fully perform as required hereunder.

Service Levels in SaaS Contracts

- Most common service level issues:
  - service availability
  - service response time
  - simultaneous visitors
  - problem response time and resolution time
  - data return
  - remedies
- Main purposes:
  - ensure that the customer can rely on the services
  - ensure that issues are timely addressed and corrected
  - provide appropriate remedies in case of provider failure
  - provide incentives that encourage the provider to be diligent in addressing issues

Service Availability Requirements

- Require that the services will have an availability of a certain percentage, during certain hours, measured over an agreed period of time
- Ensure service availability is aligned with customer's expectations and business needs (e.g., peak season)

Service Availability

- Downtime
  - Scheduled downtime
    - Receive written documentation of scheduled downtime
    - Ensure the schedule creates no issues for the customer's business
  - Downtime monitoring
    - Provider should be proactive in detecting downtime (e.g., require the provider to constantly monitor the "heartbeat" of all its servers through automated "pinging")
  - Measurement window
    - Providers tend to want longer measurement windows (e.g., quarterly)
      - Dilutes the effects of a downtime and thus masks periodic performance issues that may temporarily impact the business
      - eliminates meaningful remedies

Service Availability

- Example:
  - Provider will make the Services Available continuously, as measured over the course of each calendar month period, an average of 99.99% of the time, excluding unavailability as a result of Exceptions, as defined below (the **"Availability Percentage"**). **"Available"** means the Services shall be available for access and use by Customer. For purposes of calculating the Availability Percentage, the following are **"Exceptions"** to the service level requirement, and the Services shall not be considered unavailable, if any inaccessibility is due to: (i) Customer's acts or omissions; (ii) Customer's Internet connectivity; and (iii) Provider's regularly scheduled downtime (which shall occur weekly, Sundays, from 2 am – 4 am Central Time).

Service Availability

- Example:

o.	Title	Performance Credit Allocation Percentage	Description	Service Level	
1. Mainframe Computing Operations					
.1	Service Availability	10%	The Availability of the Service as described in Exhibit E.4.a (Service Specifications) in each calendar month.	**Measurement Window**	Calendar Month
				Expected Service Level	99.98% or greater Availability or greater in each calendar month.
				Minimum Service Level	99.96% or greater Availability or greater in each calendar month.
				Calculation	Availability of Service in each calendar month.

Service Availability

- Definitions for prior example:

1.1 "Availability" shall mean the Actual Uptime expressed as a percentage of the Scheduled Uptime less Excused Downtime for such Service (i.e., Availability % = ((Actual Uptime/(Scheduled Uptime – Excused Downtime)) x 100)).

1.2 "Excused Downtime" shall mean the aggregate amount of time in the month during Scheduled Uptime during which the applicable Service is not Available For Use by Authorized Users due to scheduled outages Approved in advance. For the avoidance of doubt, Excused Downtime shall not include time spent by Provider seeking the assistance of Third Party Vendors or internal resources for Service Requests, Incidents, or Problems associated with Service Requests, Incident, or Problem Resolution.

1.3 "Scheduled Uptime" shall mean the period of time during which Services are to be available to all Authorized Users for normal business use, expressed in hours and minutes.

1.4 "Actual Uptime" shall mean, for each measurement period, with respect to any particular Service Level measured in terms of Availability, the aggregate amount of time within the Scheduled Uptime for such Service Level that the particular Service being measured by such Service Level is Available For Use.

Service Levels: Response Time

- Unavailability as a result of failure to respond or slow response
  - Include a specific service level target for response time
- Example:

  The average download time for each page of the Services, including all content contained therein, shall be within the lesser of (a) 0.5 seconds of the weekly Keynote Business 40 Internet Performance Index ("KB40") or (b) two (2) seconds. In the event the KB40 is discontinued, a successor index (such as average download times for all other customers of Provider) may be mutually agreed upon by the parties.

Service Levels: Simultaneous Visitors

- Does the customer expect the services to support multiple simultaneous visitors?
- Consider a service level specifying a requirement consistent with the customer's requirements

Service Levels: Data

- Data return
  - If services involve
    - a critical business function, or
    - sensitive customer information
  - Measures the time period between the customer's request for data and the provider's return of such data in accordance with the timeframe requirements of the agreement
  - Assurance that customer will receive its data if the provider stops providing services
- Explicitly specify customer's ownership of information stored by the provider
- Require that provider
  - deliver periodic copies of all customer data to customer, and
  - perform regular data backups to an off-site storage facility

Service Levels: Response/Resolution Time

- Example:

1.1 Response Time. "Response Time" shall be calculated for each Incident occurring in a calendar month as the total minutes commencing from the time when Provider becomes aware of a P1, P2, P3, or P4 Incident, whether by automated alarm or otherwise, until Provider Responds to each such Incident. Provider shall track and report monthly to Customer each P1, P2, P3 and P4 Incident and the time required to Respond to each such Incident. The Response Time Service Level is set forth on the Service Level Matrix.

1.2 Resolution Time. "Resolution Time" shall be calculated for each Incident occurring in a calendar month as the total minutes commencing from the time when Provider becomes aware of a P1, P2, P3, or P4 Incident, whether by automated alarm or otherwise, until Provider Resolves each such Incident as determined by Customer. Provider shall track and report monthly to Customer each P1, P2, P3 and P4 Incident and the time required to Resolve each such Incident. The Resolution Time Service Level is set forth on the Service Level Matrix.

2.	**Response Time**		
	P1 Incidents		
	Expected Service Level	Less than 15 minutes of becoming aware of an Incident	None
	Service Level Failure	15 minutes after becoming aware of an Incident	$500 for each additional 15 minute increment

Service Levels: Response/Resolution Time

- Example:

3.1	Severity 1 Resolution	20%	The number of Severity 1 Incidents Resolved by Provider within a 4 hour Incident Resolution Time in each calendar month.	**Measurement Window**	Calendar Month
				Expected Service Level	Less than 1 miss in each calendar month.
				Minimum Service Level	1 miss in each calendar month.
				Calculation	The actual number of Severity 1 Incidents that have an Incident Resolution Time greater than 4 hours in each calendar month.
				Additional Description	Incident records as recorded by Provider are used to determine the number of Incidents resolved on time. Incidents created at an inappropriately elevated Severity Level will be closed and excluded from the calculation as long as the record is closed and re-entered at the appropriate Severity Level within 1 hour of the applicable Incident Response Time.

Service Levels: Remedies

- Performance Credits
  - Credits towards the next period's service
  - If end of contract, timely payment of credit to customer
- Right to Terminate
  - For repeated failures
  - No penalty
  - No waiting period
  - Repeated failures of the same service level
  - Repeated failures of different service levels

Service Levels: Remedies (Example)

- If the Services are not Available 99.9% of the time but are Available more than 95% of the time, then in addition to any other remedies available under this Agreement or applicable law, Customer shall be entitled to a credit in the amount of $_____ each month this service level is not satisfied. If the Services are not Available more than 95% of the time, then in addition to any other remedies available under this Agreement or applicable law, Customer shall be entitled to a credit in the amount of $_____ each month this service level is not satisfied. Additionally, in the event the Services are not Available 99.9% for (a) four (4) months consecutively or (b) any four (4) months during a consecutive six (6) month period, then, in addition to all other remedies available to Customer, Customer shall be entitled to terminate this Agreement upon written notice to Provider with no further liability, expense, or obligation to Provider.

Data Issues in SaaS Contracts

- The security of a customer's data in a cloud computing environment has been recognized as one of the largest areas of concern for a customer
  - The customer is ultimately responsible for complying with privacy and security regulations, and data security breaches are costly
- To confirm it is able to continue using its data, the customer should:
  - Require regular backups
  - Require appropriate data conversion
  - Require provider to maintain confidentiality of data
  - Place appropriate limitations on the provider's ability to use the data and customer information

Data Issues in SaaS Contracts

- Due diligence is critical
  - Where is the data going to be located?
  - Who will have access to the data?
  - Will offshore be permitted?
    - Which law governs?
  - Who is operating the data center – the provider or a third party?
    - Provider should accept all responsibility for the third party host
    - Provider should be liable with the third party host for any breach
    - Consider entering a separate confidentiality agreement with the third party host
    - Require advance notice if any change of the host
- Some providers refuse to show you their security policies but will permit onsite access to them
  - For certain transactions you should go and review them

Data Issues in SaaS Contracts

- Ensure provider is obligated to notify you if it is required to disclose your data
  - Written notice sufficiently in advance
  - Reasonable efforts not to release data pending the outcome of any measures taken by your company to oppose the required disclosure

Data Issues in SaaS Contracts (Example)

1. **Security.**

1.1 In General. Vendor will maintain and enforce safety and physical security procedures with respect to its access, use, and possession of Company' Confidential Information, including Personal Data, that are (a) compliant with the requirements of Exhibit B and, to the extent not inconsistent, at least equal to industry standards for such types of locations, and (b) which provide reasonably appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access of such information. Without limiting the generality of the foregoing, Vendor will take all reasonable measures to secure and defend its location and equipment against "hackers" and others who may seek, without authorization, to modify or access Vendor systems or the information found therein. Vendor will periodically test its systems for potential areas where security could be breached. Vendor will immediately report to Company' any breaches of security or unauthorized access to Company' Confidential Information, including Personal Data, that Vendor detects or becomes aware of. Vendor will use diligent efforts to remedy such breach of security or unauthorized access in a timely manner and deliver to Company a root cause assessment and future incident mitigation plan with regard to any breach of security or unauthorized access affecting the Confidential Information, including Personal Data.

1.2 Unauthorized Access. In the course of furnishing the Services, Vendor shall not access, and shall not permit its personnel or entities within its control to access, Company' Systems without Company' express written authorization. Such written authorization may subsequently be revoked by Company at any time in its sole discretion. Further, any access shall be consistent with, and in no case exceed the scope of, any such authorization given by Company. All Company authorized connectivity or attempted connectivity to Company' Systems shall be only through Company' security gateways and/or firewalls, and in conformity with applicable Company security policies.

1.3 Vendor Systems. Vendor shall be solely responsible for all systems Vendor uses to access Company Systems. Vendor shall ensure that its systems include up-to-date anti-viral software to prevent viruses from reaching Company Systems through Vendor's systems. Vendor shall prevent unauthorized access to Company Systems through the Vendor systems. Further, Vendor shall ensure Vendor personnel do not use any virtual private network or other device ("**VPN**") to simultaneously connect machines on Company Systems to any machines on any Vendor or third party systems, without (i) using only a remote access method approved in writing and in advance by Company; (ii) providing Company with the full name of each individual who uses any such VPN and the phone number at which the individual may be reached while using the VPN; and (iii) ensuring that any computer used by Vendor personnel to remotely access Company Systems will not simultaneously access the Internet or any other third party network while logged on to Company Systems.

Addressing Security Breaches in SaaS Contracts

Cooley LLP

- In the event of a security breach:
  - Customer has sole control over the timing, content, and method of notification to its customers and third parties (if it is required)
  - If the provider is responsible for the breach:
    - Reimbursement for expenses associated with providing notifications and complying with applicable laws

Addressing Security Breaches in SaaS Contra
(Example in Service Level Agreement)

1. **Security Breaches**. In the event of an attack or threatened or suspected breach of security against the Services and/or Server, Provider will take whatever reasonable steps that are necessary to halt such action, including taking the Services down. Down time due to external attacks shall not count against Availability requirement set forth above. Provider will immediately contact the person designated by Company to discuss what measure to take. However, if time is critical, action may be required before the contact can be reached. Provider's actions will include, as appropriate:

- Confirm the threat;
- Deny access from the source of the attack;
- Investigate the extent of the damage, if any;
- Back-up the affected systems and those suspected to be affected;
- Strengthen defenses everywhere, not just the suspected path that the attacker used;
- Contact the ISP where the threat or attack originated and/or law enforcement to work with Provider's security team;
- Produce an Incident Report within 24 hours detailing Provider's findings; and
- Re-instate the denial of access after a set time period, but continue to monitor traffic from that source until risk of further attacks is deemed to be minimized.

Data – Ownership and Use Rights

- Ownership
  - Customer's ownership rights in its data should be clear
    - Avoid disputes as to ownership of the data upon termination or expiration of the contract, or if the provider stops providing the services for some other reason
  - Confidentiality provisions are critical
    - Place appropriate limitations on the provider's use of customer information (i.e., provider has no right to use such information except in connection with its performance under the cloud computing agreement)

Data – Ownership and Use Rights

- Aggregation and commercialization of data
  - Becoming a common practice
  - Use of de-identified and aggregated data for commercial purposes
- Understand this practice and determine whether it will be permitted
- Include contract provisions with respect to this practice and representations with respect to which practices and uses are permitted
  - The customer may conclude that the provider should not have any right to use the customer's data beyond what is necessary to provide the services

Data – Redundancy

- In a SaaS environment, the provider is the "custodian" of the customer's data
- Most SaaS contract will include provisions regarding:
  - Provider's back up responsibilities with respect to the customer's data
  - Specifics with respect to the frequency of the back-up (daily, monthly) and the types of back-ups (full, partial) required
  - Requirements with respect to delivery of data to customer or customer's permitted access

Data – Redundancy (Example)

1. **Backups**. Provider shall provide for both the regular back-up of standard file systems relating to the Server and Services, and the timely restoral of such data on request by Company due to a site failure. In particular, Provider shall:

- Perform weekly full back-ups;
- Perform daily incremental back-ups;
- Send back-up media to secured, off-site storage facilities with a thirty (30) day rotation of media;
- Retain one back-up tape per month for one year;
- Fulfill restoral requests as directed by Company due to site failures. Restoral will be performed within the interval of two (2) to four (4) hours dependent on the urgency of the request, and the agreed upon location of the desired backup media; and
- If the hosting server or location is expected to be down for more than twenty-four (24) hours, immediately transfer appropriate back-up data and re-establish all hosting operations in an appropriately functioning secondary server or location.

Payment

- Utility billing
  - Payment is based on the amount of resources used, similar to how a person is charged for water, gas, electricity
- Subscription billing
  - Payment is based on a period of time, similar to how a person is charged for a newspaper or magazine subscription (e.g., per month)
- Ability to add and remove resources with a corresponding upward or downward adjustment in the services fees
- Lock in recurring fees for a period of time
  - After expiration of lock, fees increase using an escalator based on CPI or another index

Publicity

- Customer's reputation and good will are substantial and important assets
  - Most notably via customer's name and other trademarks
- Consider a provision relating to any announcements and publicity in connection with the transaction
  - Prohibit the provider from making any media releases or other public announcements relating to the agreement, or otherwise using the customer's name and trademarks without prior written consent

Termination

- The customer should be able to terminate the agreement at any time upon notice and without termination charges
  - A short notice (e.g., 10 business days) is reasonable in some cases
  - The software is being provided as a service and should be treated as such
  - The provider may request a minimum commitment from the customer to recoup the provider's "investment" in securing the customer as a customer
    - If this is acceptable, limit it considerably
      - Required evidence of the provider's up front costs to justify such a requirement

Indemnification

- Third party claims relating to the provider's breach of its confidentiality and security obligations, and claims relating to infringement of third party intellectual property rights
  - Ensure damages and expenses that are paid pursuant to indemnification are carved out of any cap on liability and any exclusion of certain damages
  - For unintentional data breaches the provider may require a cap on its potential exposure; may be reasonable depending on the type of customer data in question

Indemnification (Example)

1. **Indemnification.** At Vendor's expense as provided herein, Vendor agrees to defend, indemnify, and hold harmless Company and its directors, officers, agents, employees, members, subsidiaries and successors in interest from and against any claim, action, proceeding, liability, loss, damage, cost, or expense, including, without limitation, attorneys' fees, experts' fees and court costs, arising out of any claim by a third party (a) related to (i) Vendor's breach of this Agreement; (ii) any action or inaction of Vendor that causes any injury to any person or persons or damage to tangible or intangible property; and (iii) Vendor's failure to comply with applicable laws and regulations; and (b) that Company' authorized use of the Services (the "**Indemnified Items**") infringe that third party's patent, copyright, trade secret or other intellectual property rights (collectively, "**Claim(s)**"), including the payment of all amounts that a court or arbitrator finally awards or that Vendor agrees to in settlement of any Claim(s) as well as any and all reasonable expenses or charges as they are incurred by Company or any other party indemnified under this Section in cooperating in the defense of any Claim(s). Company shall: (i) give Vendor prompt written notice of such Claim; and (ii) allow Vendor to control, and fully cooperate with Vendor (at Vendor's sole expense) in, the defense and all related negotiations. Vendor shall not enter into any stipulated judgment or settlement that purports to bind Company without Company' express written authorization, which shall not be unreasonably withheld or delayed. Notwithstanding the foregoing, Vendor shall have no indemnity obligation for infringement claims arising from (i) use of the Indemnified Items in excess of the rights granted hereunder; (ii) use of the Indemnified Items in combination with software and/or hardware that is not approved or provided by Vendor; or (iii) Company' failure to implement an update or enhancement to the Indemnified Items, provided Vendor provides the update or enhancement at no additional charge to Company and provides Company with written notice that implementing the update or enhancement would avoid the infringement. If the Indemnified Items, or any portion of them, become or are likely to become the subject of an infringement claim, then, in addition to defending the claim and paying any damages and attorneys' fees as required above, Vendor shall, at its option and in its sole discretion, either (a) immediately replace or modify the Indemnified Items, without loss of material functionality or performance, to make them non-infringing or (b) immediately procure for Company the right to continue using the Indemnified Items pursuant to this Agreement. Any costs associated with implementing either of the above alternatives will be borne by Vendor. If Vendor fails to provide one of the foregoing remedies within forty-five (45) days of notice of the claim, Vendor shall refund to Company all one-time sums paid by Company for the infringing Indemnified Items, prorated over two years from the Effective Date, plus the prorated portion of all pre-paid unused recurring fees.

Indemnification

- Vendor may seek customer indemnities for:
  - IP claims based on data or other content submitted by users and/or hosted by vendor
  - Claims that Customer's storage, processing, display of content violates any law (e.g., privacy) or third party right

Limitation of Liability

- Scrutinize limitation of liability provisions carefully
  - A reasonable limitation of liability provision balances the provider's concern about unlimited damages with the customer's right to have reasonable recourse in the event of a data breach or other incident
- Seek the following protections:
    - Mutual protection
    - Appropriate carve-outs (e.g., confidentiality, data security, indemnity)
    - A reasonable liability cap for direct damages

Limitation of Liability

- Provider's standard limitation of liability clauses usually
  - Are not mutual
  - Limit provider's liability to fees paid for a portion of the agreement (e.g., in the last 12 months; for the portion of services at issue)
  - Exclude indirect damages (e.g., incidental, consequential, punitive, etc.)

Warranties

- The following warranties are common in these types of agreements:
  - Conformance to specifications
  - Performance of services
  - Appropriate training
  - Compliance with laws
  - No sharing / disclosure of data
  - Services will not infringe
  - No viruses / destructive programs
  - No pending or threatened litigation
  - Sufficient authority to enter into agreement

Exclusivity

- Exclusivity can frequently lead to advantageous pricing and commercial terms
- But, the customer must ensure it has the proper protections in the agreement:
  - Excellent service levels
  - Appropriate exceptions to exclusivity
  - Right to transition in anticipation of termination
- Avoid being bound to a provider that can't perform

Post-Execution Ongoing Provider Agreement

- Regular program of evaluating the provider's performance
  - Provider required to supply the requisite information to access the services
  - Reporting and governance program
  - Notify requirements with respect to changes affecting provider (financial, business)

Negotiation

- Leverage is critical
  - With SaaS contracts, obtaining the terms and protections the customer wants will depend on where you are on the spectrum
    - High risk
    - Medium risk
    - Low risk
  - If the customer doesn't have leverage
    - Providers will likely resist the protections discussed and significant (or any) modification to its form agreements
- Risk mitigation is key
  - For example, if the customer can't get the service level it wants, it should focus on the remedies associated with service level failure

QUESTIONS?

Matt Karlyn
Partner
mkarlyn@cooley.com
(617) 937-2355

Phil Mitchell
Special Counsel
phil.mitchell@cooley.com
(212) 479-6581

Leah Roffman
Associate
lroffman@cooley.com
(212) 479-6578