Healthcare Technology Legal Issues: Overview of Information Security Agreement (ISA) and Top trends for 2015

Gregory M. Kratofil, Jr.
gkratofil@polsinelli.com

Polsinelli PC. In California, Polsinelli LLP

Information Security Agreements Purpose

- Vendors are creating, using, processing or storing Customer Data.
- Vendors are connecting to the information networks of Customers.
- Customers care about:
  - Minimizing risks of their network being infiltrated
  - Customer data being corrupted or accessed
  - Violation of federal or state security laws
  - Compromise ability to provide care

Information Security Agreements Model

- Security is important to us, but different solutions "require" different levels of security.
- We will identify some things we believe are good security. You tell us what you do or strike out what you don't do.
- Based on the solution, we may be OK with your level of security or we may have a vendor selection issue.

Information Security Agreement Vendor Scenario Chart

- Start with a list of questions that helps determine what schedules apply.
- Example:
  - Is the Vendor’s solution on our network?
  - Will they need admin or remote access?
  - Will they have access to sensitive data?
  - Does vendor provide PCI related products or services?

Information Security Agreements
Security Schedules

General Terms and Conditions	Definitions
Agent Security and Training	Audit Logs
Protection against Malicious Software	Network Security
Data Backup	Patch Creation and Certification
Contingency Plan	Physical and Environmental Security
Device Storage and Media Handling	Special Network Connectivity
Encryption and Transmission of Data	Remote Access to our System
Incident Response	Risk Management Requirements

Information Security Agreement
Example of Schedules

- Device and Storage Media Handling
  - Access to device shall require a password
  - Devices shall be encrypted with Strong Encryption (defined term)
- Audit Logs
  - Vendor shall ensure that Audit logs for the past 90 days are readily accessible
  - Vendor shall provide or make available Customer Audit log data which are 91 days or older within 14 days from request

Information Security Agreements
Vendor Pushback

- Lawyer says No; Business folks say we do.
- Return/Deletion of CI after termination
- Warranty/Remedies
- Indemnification
- Subcontractors/Especially outside the U.S.
- Audits/Certifications
- Venue and Conflicts of Law
- Make it Neutral. Why?
- Notify Customer if changes to functionality of contractors
- Remove provisions feel covered by Master Agreement

Trends for 2015
Healthcare Privacy and Security

- Big Data
- OCR Changes
- Business Associates
- Cloud and Overseas access to Medical Records

Trends for 2015
General Privacy and Security

- Mobile Privacy
- Payment Card Security
- IoT and Big Data
- Drones

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

Emerging Trends in Healthcare Technology and Cloud Computing in 2015

Jean Marie R. Pechette
Shareholder

Heart of America HIMSS

February 4, 2015

Agenda

- Increased Adoption of Cloud Computing in Healthcare Technology
- Cybersecurity Threats/Legal Risks
- Mitigation Strategies

Healthcare Industry moving towards Increased Use of Cloud-Based Services

- Adoption of digital platform: patient-centered and data driven
- "Meaningful Use" of Certified EHRs driven by financial incentives/penalties
- Healthcare reform/increase efficiencies/reduce costs
- Care coordination/coordination of benefits/patient engagement
- Medical devices/mobile apps/fitness devices/remote monitoring tools to manage chronic diseases—interoperable or interconnected with EHRs and PHRs
- Big Data/research and population health

Cloud Computing-from Enabler to Backbone of Healthcare Reform

- The National Institute of Standards and Technology (NIST) definition of "evolving paradigm" of cloud computing:

  "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*"

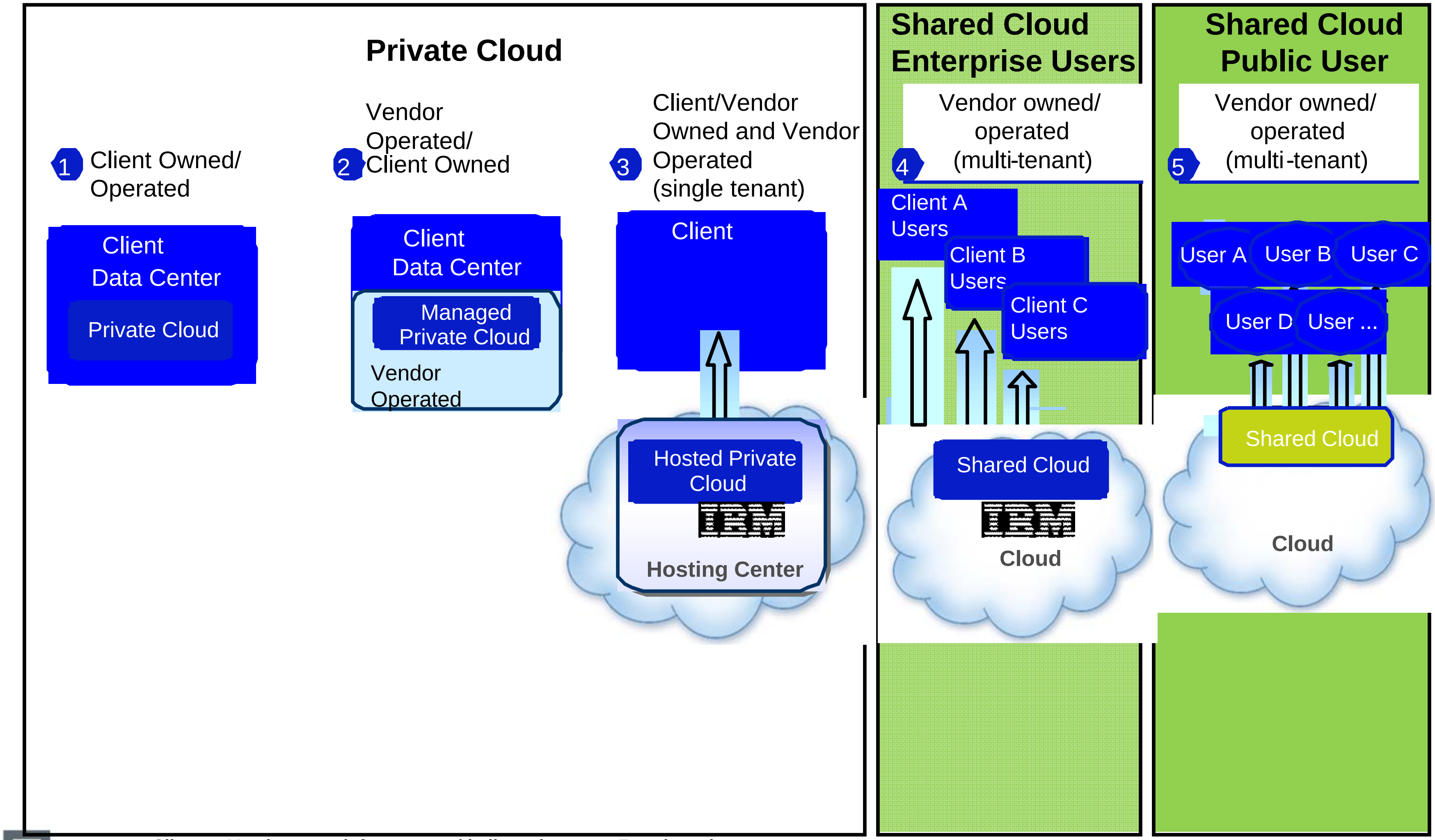
Essential Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Three Service Models

Software as a Service (SaaS)		Platform as a Service (PaaS)		Infrastructure as a Service (IaaS)	
Applications	Managed By Service Provider	Applications	Managed By Client	Applications	Managed By Client
Data		Data		Data	
Runtime		Runtime	Managed By Service Provider	Runtime	
Middleware		Middleware		Middleware	
OS		OS		OS	Managed By Service Provider
Virtualization		Virtualization		Virtualization	
Servers		Servers		Servers	
Storage		Storage		Storage	
Networking		Networking		Networking	

Deployment Models



Private Cloud

1 Client Owned/ Operated

Client Data Center

Private Cloud

2 Vendor Operated/ Client Owned

Client Data Center

Managed Private Cloud

Vendor Operated

3 Client/Vendor Owned and Vendor Operated (single tenant)

Client

Hosted Private Cloud

IBM

Hosting Center

Shared Cloud Enterprise Users

4 Vendor owned/ operated (multi-tenant)

Client A Users

Client B Users

Client C Users

Shared Cloud

IBM

Cloud

Shared Cloud Public User

5 Vendor owned/ operated (multi-tenant)

User A

User B

User C

User D

User ...

Shared Cloud

Cloud

Client or Vendor owns infrastructure/dedicated access. Fees based on model

Vendor owns infrastructure/Client has shared access/Fees based on usage metrics

Immutable Laws of Cloud Security

“These are things that will always be, things that will never change, and it is a state of being.”

- an understanding that if your data is hosted in the cloud, you no longer directly control its privacy and protection.
- when your data is burst into the cloud, you no longer directly control where the data resides or is processed.
- if your security controls are not contractually committed to, then you may not have any legal standing in terms of the control over your data or your assets.
- if you don't extend your current security policies and controls in the cloud computing platform, you're more than likely going to be compromised

Tari Schreider, HP chief architect of HP Technology Consulting and IT Assurance Practice.

“Security and the Cloud: The Great Reconciliation”, eCommerceTimes, 14 May 2012
http://www.ecommercetimes.com/story/Security-and-the-Cloud-The-Great-Reconciliation-75094.html

Healthcare Industry Most Vulnerable to Cybersecurity

- FBI (private industry notification)(PIN): “Cyber actors will likely increase cyber intrusions against health care systems—to include medical devices—due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market”. Compared to the financial and retail sectors, health care industry is even more vulnerable to cyber intrusions.
- More than 8 Million Americans have had their PHI compromised in hacking-related HIPAA breaches, according to OCR data.
- In the last 4 years, criminal data attacks on the healthcare industry have skyrocketed 100 percent.
- Impacted life-critical systems may jeopardize patient safety

Breach is Inevitable

- Companies “that have been hacked and those that will be…converging into 1 category—companies that have been hacked and will be hacked again”. (FBI Director Robert Mueller III-2012)

- When a breach occurs, judged by reasonableness of efforts to prevent and mitigate incidents

Key Laws and Standards

- HIPAA
- FTC Rule/Enforcement Actions
- State Privacy Laws
- Personal Data Notification & Protection Act (proposed)
- Frameworks/Standards/Self-regulation (e.g. NIST Framework, FTC Framework, FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks)

HIPAA Security Rule

- The Security Rule requires Covered Entities (and their Business Associates) to maintain reasonable and appropriate technical, physical and administrative safeguards to protect electronic PHI ("ePHI") and to:

  - ensure the **confidentiality, integrity, and availability** of all **ePHI** they **create, receive, maintain or transmit**;

  - **identify** and protect against reasonably anticipated threats to the security or integrity of the information;

  - protect against reasonably anticipated, impermissible uses or disclosures.

SECURITY RULE CHECKLIST

POLSINELLI

Administrative Safeguards

- Security management process(R)
  - Risk analysis (R)
  - Risk management (R)
  - Sanction policy (R)
- Assigned security responsibility (R)
- Workforce security (R)
  - Authorization/Supervision (A)
  - Workforce clearance (A)
  - Termination procedures (A)
- Information access management(R)
  - Isolate clearinghouse functions (R)
  - Access authorization (A)
  - Access establishment/modification (A)
- Security awareness and training (R)
  - Security reminders (A)
  - Protection from malicious software (A)
  - Log-in monitoring (A)
  - Password management (A)
- Security incident procedures (R)
- Contingency plan (R)
  - Data backup plan (R)
  - Disaster recovery plan (R)
  - Emergency mode operation plan (R)
  - Testing and revision procedures (A)
  - Applications and data criticality analysis (A)
- Evaluation (R)
- Business associate contracts (R)

Physical Safeguards

- Facility access controls (R)
  - Contingency operations (A)
  - Facility security plan (A)
  - Access control and validation (A)
  - Maintenance records (A)
- Workstation use (R)
- Workstation security (R)
- Device and media controls (R)
  - Disposal (R)
  - Media re-use (R)
  - Accountability (A)
  - Data backup and storage (A)

Technical Safeguards

- Access control (R)
  - Unique user Id (R)
  - Emergency access (R)
  - Automatic logoff (A)
  - Encryption and decryption (A)
- Audit controls (R)
- Integrity (R)
  - Authenticate ePHI (A)
- Person or entity authentication (R)
- Transmission security (R)
  - Integrity controls (A)
  - Encryption (A)

Expanded Reach of HIPAA

- Final Rule specified that the following are Business Associates (“BA”):
  - Personal health record vendor to one or more individuals on behalf of a Covered Entity (“CE”)
  - Health information organization (enabling health information exchange)
  - E-prescribing gateway
  - Other person that provides data transmission services with respect to PHI to a CE and that requires access on a routine basis to such PHI

“Expanded Reach of HIPAA” (continued)

- BA definition also includes an individual or entity that “*creates, receives, maintains, or transmits PHI for a function or activity*” on behalf of a CE or organized health care arrangement (OHCA), but other than as a part of the workforce of the CE or OHCA
- Thus, the HIPAA regulations more clearly regulate data center operators, cloud service vendors and other vendors that maintain or transmit Protected Health Information (“PHI”), even if they do not actively access the PHI
- “Conduit” exception is very narrow, and only excludes entities providing courier services and their electronic equivalents (ex. USPS, UPS).

Note: A data storage company that has access to PHI (whether digital or hard copy) is a BA, even if the entity does not view the information or only does so on a random or infrequent. Recently, at the AHLA Annual Meeting, Christina Heide, OCR’s Acting Deputy for Health Information, stated that SaaS vendors are business associates even if all data maintained is encrypted.

“Expanded Reach of HIPAA” (continued)

- Final Rule expanded the definition of BA to include Subcontractors
- A Subcontractor is an individual or entity to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of the BA
- The analysis used to determine whether a Subcontractor is acting on behalf of a BA is the same analysis used to determine whether a BA is acting on behalf of a CE
- The BA, not the CE, is required to enter into a Business Associate Agreement (BAA) with the BA’s Subcontractor

Breach Notification Standards

- Under the Breach Rule, a covered entity must notify an individual and OCR of a breach of unsecured PHI.
  - PHI is considered secure if it is rendered **unusable, unreadable or indecipherable** to unauthorized persons through the use of a technology or methodology specified by HHS in guidance issued under the HITECH Act.
  - Likewise, a BA must notify a CE of a breach of unsecured PHI.
- The Breach Rule defines a breach generally as the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

Definition of Breach

- A Breach is **presumed** unless CE or BA demonstrates that there is a "low probability" that the privacy of PHI has been compromised based on a risk assessment considering at least the following factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  - The unauthorized person who used the PHI or to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - The extent to which the risk to the PHI has been mitigated
- The CE or BA has the burden to prove that an unauthorized disclosure is not a Breach

FTC Breach Notification Rule

- Requires businesses not covered by HIPAA to notify customers of breach of unsecured, individually identifiable electronic health information.
- Applies to a vendor of personal health records (“PHR”), a PHR-related entity, or a third-party service provider for a vendor of PHRs or PHR-related entity
- If breach involves 500 people or more, must notify the FTC within 10 business days after discovering the breach.

FTC Enforcement against Already Regulated Entities

In the Matter of LabMD Inc.

- FTC brought enforcement action against LabMD (already regulated under HIPAA) in August 2013 alleging it failed to reasonably protect the security of consumer's personal data, including medical information. The complaint alleged that in 2 separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers and that data from nearly 500 patients had fallen into hands of identity thieves. LabMD argued FTC lacked authority and failed to promulgate data security standards depriving LabMD of fair notice and due process.

- **See also enforcement action against *Wyndham Worldwide Corp*** alleging computer network intrusions led to more than $10.6M in payment card fraud losses. FTC also argued that other statutes relevant to data security (like FCRA, GLB, and COPPA) do not limit the FTC's jurisdiction.

Mitigation Strategies

- Due Diligence
- Operational
- Contractual
- Cyber-Insurance

Applicable State Laws

- 49 states and territories have enacted their own laws affecting consumer privacy and data security, including:
- **California Confidentiality of Medical Information Act**
  - Requires confidentiality of ”medical information” which is any “individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition or treatment.”
- **Massachusetts Data Privacy Law**
  - Broad definition of personal information: “resident's first name/last name or first initial/last name in combination with any one or more of the following data elements that relate to such resident: (a) SS no. (b) driver's license no. or state-issued ID card no.; or (c) financial account no., or credit or debit card no., with or w/o required security code, access code, personal identification no. or password, that would permit access to a resident’s financial account.
- **Texas Medical Privacy Act**
  - “Covered entity”: “any person who engages in the practice of assembling, collecting, analyzing, using, evaluating, storing or transmitting PHI”.
- **Texas Identity Theft Enforcement and Protection Act**
  - Provides further standards for notification to customers in the event of data breach, as well as safe harbors guidelines, and purports to extend its protections beyond Texas state residents

Due Diligence

- Vendor’s proposed cloud architecture/track record/financial viability/DR/BCP
- Compliance with privacy/security laws/industry standards
- Location of data/multi-tenant with virtual segregation
- Encryption in transit and at rest
- Personnel (background checks)/identify offshore resources/access/transfer
- Use of downstream contractors
- Permitted de-identification if compliant with HIPAA
- Periodic risk assessments/intrusion detection/controls
- Track record with performance requirements
- Audit of certifications/BCP/DR/insurance coverage

Operational Strategies

- **“Minimum Necessary”**
  - Don’t collect more than what you need
  - Don’t retain longer than you need it
- **Privacy by Design**
- **Adopt/Adhere to Written Data Security Compliance Program/Flow down to contractors**
- **NIST Framework for Improving Critical Infrastructure Cybersecurity**
- **Technical controls: (e.g. encryption on all devices/unless can justify why not)**
- **Physical (e.g., data center security; no offshoring/geographically remote data centers)**
- **Administrative safeguards (HIPAA training/ regular risk assessments/ risk mitigation plans/audits)**
- **Breach Notification/Security Incident Response Plan**
- **Readiness for new cyber-threats (Chinese hackers, economic espionage)**
- **Cyber-insurance**

Contractual Strategies

- Compliance with data protection laws/HIPAA/BAAs
- Warranties/covenants adequately address heightened cybersecurity risks: physical, technical (e.g., encryption at rest and in transit, virus protection, patches), and administrative safeguards; written policies and procedures; background checks; training; no offshore access; breach notification protocols; disaster recovery/business continuity plans; regular risk assessments and audits, industry certifications
- **Cyber-insurance coverage**
- Termination rights and transition services
- Indemnification (including data breach, investigation, remediation, identity theft protection, government-imposed penalties)
- Carve-outs to limitations on liability/consequential damages
- Exit Strategy/return/purging/destruction of data

Trends and Take-Aways

- Cloud computing has evolved from enabler to backbone of healthcare IT delivery
- It’s all about the data—for coordination of care/benefits, patient-centered outcomes, research and population health
- With interconnectivity/interoperability/Internet of things and the Cloud/Breach is inevitable
- Entities judged not by the breach but by reasonableness of measures to detect, prevent and mitigate breach and potential harm
- Facing overlapping/multiple enforcement actions from various regulatory agencies and class actions
- Mitigate with due diligence; comprehensive security compliance programs; transparency in data collection/use; ongoing risk assessments; privacy by design; compliance with “recommended” Frameworks; readiness against new cyber-security threats; cyber-security insurance

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.