CCA & DC|IA proudly present:

Health + Government in the Cloud
Legal / Regulatory Framework + Developments

Presented by Kaiser Wahab, Wahab & Medenica LLC

CLOUD COMPUTING EAST 2014

Revolutionizing Business Processes in Government & Healthcare

MAY 15-16, 2014
Doubletree by Hilton
Downtown Washington, DC

Benefits of Cloud are Now Well Known

- What is cloud computing?: From the FL State Bar: “Cloud computing is analogous to connecting a home to a city water supply when previously that home drew its water from a private, individual well.”
  - Use of Pooled/Distributed Resources to Reduce Cost
    - Multiple consumers serviced using dynamically allocated physical and virtual resources
  - Dynamic Scalability
    - On-demand scalable, as needed service delivery
  - Multi Platform, Multi-Device Accessibility
  - Potentially Increased Redundancy
  - Pay as You Go / Consumption Billing
    - Pricing based on actual consumption of Cloud-based resources
    - Lower pricing given lower infrastructure and entry costs

What seems to Good to be True…Legal Pitfalls Abound

- JURISDICTIONAL/OWNERSHIP
  - What territory is the data stored; does that implicate foreign or undesired legal frameworks or laws?
  - Who owns the data and what happens to the data if the CSP relationship is terminated?
- REGULATORY
  - Government/Health data is “radioactive” typically subject to a variety of controls and penalties for breach or misuses
- OVERSIGHT, TRANSPARENCY & CONTROL
  - How to assure transparency in terms of security, breach, standards, protocol, etc.?
  - Who is responsible for damages and penalties incurred as a result of breach or data loss?
- COMPLIANCE AND IMPLEMENTATION
  - Does the Cloud Service Provider (CSP) have the protocols, controls, and standards compliance in place to adequately serve health and/or government interests? Does the CSP have to configure its offering specifically for those interests?
- PRICING/TERMINATION
  - Is the scalability of the CSP offering matched by runaway pricing? What happens in the event of termination and who has that power?

Breakdown of Applicable Law/Regulations

- FISMA (Federal Information Security Management Act of 2002)
  - Basic goal is to provides security control selection and assessment standardization
  - Latest Action: 04/17/2013 Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs
- HIPAA (Health Insurance Portability and Accountability Act of 1996)
  - HIPAA is a Federal law
  - HIPAA establishes uniform rules for protecting Health Information and privacy
  - State laws that can be stricter than HIPAA with greater protections of health information privacy than HIPAA are not necessarily preempted and may still apply, but still serves as a baseline and a good starting point
    - See for example NYS PHL Section 18
  - Augmented by HITECH ACT in 2009
  - Augmented by HIPAA OMNIBUS RULE in 2013 which expands compliance obligations to CSP's "Business Associates"
- There are many other data privacy and computing laws, standards, and regulations (e.g., PCI, ECPA, FOIA, Patriot Act) that could apply to the cloud, which are beyond the cope of this presentation

HIPAA in a Heartbeat

- Enacted in 1996
- Comprised of two major components:
  - Security Rule
  - Privacy Rule (compliance mandated in 2003)
- Applies to so called “Covered Entities”
  - Health plans, health care clearinghouses, and health care providers that transmit health information
  - Designed to assure that Covered Entities follow privacy and security procedures when dealing with PHI
- But also applies to the “Business Associates” of Covered Entities
  - Receive PHI (see slide on Protected Health Information) from a Covered Entity, or may create or obtain PHI from other parties for use on behalf of Covered Entity
  - A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity

HIPAA Privacy Rule

- Per HIPAA, the rule “applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form.”

- Designed to protect “individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral”.

HIPAA Security Rule

- Requires ***administrative*** AND ***technical*** safeguards to:
  - Ensure confidentiality, integrity, and availability of all PHI that is created, received, maintain or transmitted
  - Identify and protect against reasonably anticipated threats to the security or integrity of PHI
  - Protect against reasonably anticipated, impermissible uses or disclosures of PHI
  - Ensure compliance by personnel
  - Provide ongoing risk management

  - Example: an organization's strong password policy is an example of an administrative safeguard for electronically-stored customer information.

What is PHI (Protected Health Information)?
(A Non-Exhaustive Core List)

1. Names
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and [t]he initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

HITECH – Stricter Enforcement

- 2009 Enactment
  - HITECH Broken Down into Five Parts:
    - Data breach notification requirement – If there is a breach or misuse of PHI federal government and effected individual(s) must be notified; documentation of potential data breach scenarios must also be maintained (private sphere analogue: FTC Red Flag Rule)
    - Applies HIPAA privacy and security requirements to outside vendors and service providers
    - Allows privacy and security complaints to be brought by state as well as federal regulators
    - Provides new limits on use and disclosure of PHI
    - Gives individuals new rights over PHI
- Penalties
  - Civil and criminal
  - Maximum penalty $1.5 million and 10 years in prison

HIPAA recently updated with 2013 “Omnibus Rule”

- The new rule greatly expands the definition of who or what is considered a “Business Associate” to include a party that “creates, receives, maintains, or transmits” PHI
- All Business Associates must be compliant by 9/23/13
- Newly minted Business Associates must have a formal BA agreement in place that addresses:
  - Permitted PHI use/disclosure
  - Safeguard requirements
  - Disclosure of breach or non-permitted use
  - Agreement to extend HIPAA obligations to subcontractors and agents
- The general consensus is the CSP’s are now Business Associates under HIPAA, such that all the above requirements apply

Federal Information Security Management Act (FISMA) & E-Government Act of 2002

- Provides security control selection and assessment standardization:
  - Consistent information protection framework at the federal level
  - Provides standards and guidance for IT and data security risk management and protection
  - Mandates development of adequate controls to protect information and systems
  - Sets out federal oversight framework for security programs
- FISMA requires federal agencies to:
  - Engage in security planning
  - Have a personnel tree with specific personnel roles for security
  - Engage in periodic review of IT systems security controls
- FISMA comprised of three main sections
  - Annual security reporting
  - Independent Evaluation
  - Corrective action plan for remediation of security weaknesses

FISMA Requirements

- Federal agencies must implement an integrated, risk-based information security program conforming to high-level information security standards
- Agencies Must:
  - Assess the current level of risk associated with their information and information systems
  - Define controls to protect those systems
  - Implement policies and procedures to cost-effectively reduce risk
  - Periodically test and evaluate those controls
  - Train personnel on information security policies and procedures
  - Manage incidents

FISMA Mandates:

- Risk Mitigation activities
- Risk assessment activities
- Security awareness training
- Security systems, protocol, and control testing
- Security issues response procedures
- Continuity procedures
- Chief security officers responsibilities

Relationship between FISMA and National Institute of Standards and Technology (NIST)

- NIST provides detailed guidance on FISMA
- NIST guidance in a nutshell:
  - Information and information systems categorization standards
  - Minimum security requirements standards
  - Guidance on security controls
  - Guidance on security control testing and assessment
  - Guidance for certifying and accrediting information systems

NIST + FISMA Publications

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-18, Rev 1 (Security Planning)
- NIST Special Publication 800-30, Rev 1 (Risk Management)
- NIST Special Publication 800-37 (Certification & Accreditation)
- NIST Special Publication 800-53 Rev 3 (Recommended Security Controls)
- NIST Special Publication 800-53A Rev 1(Security Control Assessment)
- NIST Special Publication 800-60 (Security Category Mapping)

Various CSP Delivery Models

- Software as a Service ("SaaS") (EXAMPLES: Google Gmail, Facebook)
    - Scenario: User accesses provider application using cloud infrastructure.
- Platform as a Service ("Paas") (EXAMPLES: Microsoft Azure)
    - Scenario: Customer deploys applications and services over CSP's infrastructure.
- Infrastructure as a Service ("IaaS") (EXAMPLES: Amazon, IBM, Google)
  - Allows a user to access provision processing, storage, network
  and other fundamental computing resources.
- Private, Public, and Hybrid Clouds
    - Single, multiple tenants, etc.

Not all CSP’s Are Equal—Due Diligence and Negotiation Critical to Health and Gov’t Sectors

- Many cloud service providers provide standard “take it or leave it” service contracts
  - One-sided, extremely CSP centric terms
  - No accepted standards for contract terms, service levels, etc. for non-routine undertakings
  - Often have little accountability and disclaims warranties on an “as is” basis
  - Often limit and disclaim all liability for universe of damages (direct, indirect, consequential)
  - Makes security, data protection and backups customer responsibility
  - Provide CSP’s unilateral right to suspend service or terminate agreement
- This often means **<u>NO</u>** transparency on security –Absent transparency and communication, cloud clients may never know if compliance is being maintained during the ordinary course, or worse if data breaches or other security issues are being reported and dealt with per applicable regulations

So Choose Wisely, Kick Tires, and Negotiate Deals

- Due Diligence
  - Are cloud solutions the core service offering of the CSP?
  - Is the CSP financially stable?
  - Does the CSP offer indemnification?
  - Is the CSP outsourcing any functionality of its offering to third parties (is the third party contractually and otherwise bound to same standards as CSP?)
  - Does the physical security of its datacenters meet your legal, regulatory and business needs?
  - Are its business continuity and disaster recovery plans consistent with your business needs?
  - What is its level of technical expertise within its operations team?
  - What is the CSP's history offering the solution (how long, reputation, etc.), does it have a verifiable track record with health and/or government clients?
- Negotiation of Contract
  - Agencies and health providers should negotiate any CSP contracts rather than just signing off on the CSP "master service agreement (MSA)."
  - Get the attorneys involved: IT pros should not move ahead on cloud solutions without legal oversight.
  - IT can evaluate the technical dimensions of the CSP contract but should not be tasked with vetting legal and procurement issues for health and public-sector to minimize legal exposure.
  - The health or public entity needs to be willing and prepared to migrate and seek other CSP's in the event the contract is breached.
- Implementation

Cloud Service Contract Best Practices

- **Pricing.** Assure the contract doesn't carry hidden incidental charges for initial and/or upfront costs, maintenance and renewal costs. You may also try to negotiate cost increase caps.
- **Service-level Agreements.** There should be penalties for noncompliance with basic service level parameters (e.g., uptime guarantees that are not satisfied, may be coupled with a reduction in fees, or other penalties).
- **Governing Law/Venue**. Particularly with CSP’s, the contract should clearly lay out what law applies, preferably local jurisdiction of the agency, or health interest. Moreover, a venue clause should also be added to assure that the proceeding is in a local jurisdiction.
- **Infrastructure Security**. Parameters should be set out as to specific security protocol, hardware, etc.
- **Outsourced Services**. If the CSP resorts to third-party providers and vendors, the contract should make clear that the CSP bears primary responsibility for any breaches and that, moreover, the outsourced third-party is contractually obliged to adhere to applicable laws and regulations (e.g., HIPAA).
- **Functionality**. CSP contracts should mandate that any material changes in functionality must be approved.
- **Disaster Recovery**. The contract should address disaster recovery and continuity processes and safeguards.
- **Mergers and Acquisitions**. The contract should spell out what happens if the CSP gets purchased and under what circumstances the contract is assigned and under what terms.
- **Compliance with Laws**. Particularly in connection with government and health interests, the CSP agreement should carry terms obligating compliance with HIPAA and other applicable rules and regulations.
- **Modifications of Terms and Conditions**. CSP’s should be barred from being able to modify terms and conditions unilaterally and certainly not by merely posting new terms via their web site.
- **Contract Renewal and Termination**. Terminating CSP services should be a core concern. There should be provisions relating to the removal, destruction, and return of data on the case of termination. Renewal of the CSP contract should not be automatic.

Government Cloud Adoption Rising Pursuant to Standards Initiatives

- Fed and state governments not using same cloud as Instagram
- Fed and state governments are shaping private cloud environments to meet unique needs, increase reliability
- IDC says that by FY 2014 U.S. Federal government spending on private cloud will be $1.7 billion vs. just $118.3 million on public cloud.
- Per the U.S. Federal Cloud Computing Strategy paper put forth by the former White House CIO, the U.S. government undertook an aggressive cloud modernization policy to accelerate cloud adoption.
- As a result, agencies must support operations with robust government centric cloud services with equally robust mobile, social and analytics functionalities.
- Agencies are increasingly leveraging strict compliance / security security based on cloud standards and mandates such as FedRAMP

What is FedRAMP (Federal Risk and Authorization Management Program)?

- Akamai, Lockheed Martin, Microsoft, Amazon Web Services (AWS) and the U.S. Department of Agriculture -- Why are they in this presentation?
- They all leverage the Federal Risk and Authorization Management Program (FedRAMP)
  - Federal government-wide standards initiative
  - Provides standardized framework to security assessment, authorization, and continuous monitoring for cloud products and services
- Developed by NIST in 2012 upon consultation with a variety of partners
- FedRAMP is now driving powerful current in cloud service providers offerings towards government agencies
  - Example: IBM lost a $600 million CIA cloud bid because it did not conform to FedRAMP
- FedRAMP is designed to provide a standardized framework for security assessment, authorization, and continuous monitoring for cloud products/services

How Does FedRAMP Work?

- Per FedRAMP, CSP’s catering to Federal agencies must:
  - Employ the minimum control standards set forth in the FedRAMP requirements
  - Apply for FedRAMP authorization for their offering
  - Engage in authorized “Third-Party Assessment Organization” (3PAO) for an independent system assessment
  - Create and submit authorization packages
  - Provide continuous monitoring reports
- 3PAO’s, a layer of third-party oversight:
  - Perform initial and periodic assessments of CSP systems to assure ongoing compliance with program requirements
  - 3PAOs are also tasked with developing Security Assessment Plans and Security Assessment Reports,
  - Performing tests of cloud security controls
- Some of the core requirements of a CSP under the program include:
  - Electronic discovery and litigation holds capabilities
  - Identification systems, coupled with dual factor authentication for network access to privileged accounts
  - Capabilities to cure and manage high risk issues within 30 days,
  - Capabilities to cure and manage medium risk within 90 days
  - System safeguards to prevent unauthorized data transfer via shared resources
  - Encryption for data integrity and safety during transmission
- **FedRAMP CSP’s:** Amazon AWS GovCloud, Windows Azure public cloud solution, IBM SmartCloud for Government (SCG)

Regulatory as an Enabler Not Barrier

- FedRAMP accreditation presents overlap with other compliance initiatives such as HIPAA or PCI
- FedRAMP security controls address the classes of private data addressed by HIPAA and PCI that require safeguarding (e.g., patient PHI and credit card info)
- No ideal overlap between these regulations
- Each special sphere has its own laundry list of compliance items
  - Example: FedRAMP doesn't provide for Business Associates Agreements (BAAs) specified under HIPAA
- FedRamp core protections and risk management focus may at least reduce compliance burden for agencies caught between multiple regulations.
  - Example: Department of Health and Human Services implemented FedRAMP into an IT security Standard Operating Procedure

Federal Information Security Management Act (FISMA) 2013 Update PENDING

- The House of Reps unanimously approved a bill making the first significant reforms in 11 years to fed government information security by updating FISMA.
- The Federal Information Security Amendments Act, H.R. 1163 will require fed agencies to:
  - Continuously monitor IT systems against cyber threats
  - Implement regular threat assessments
  - Hold each department secretary and agency director for IT security
  - Appoint a chief information security officers to coordinate IT security, if none present.
- Some believe the amendment addresses a checkbox approach under FISMA, rather than continuously monitoring systems and strategically assessing and addressing cyber attack risks.

2014 HIPAA Compliance Challenges and Updates

- Increased enforcement and litigation activities due to stated Office for Civil Rights enforcement intent of HIPAA and HITECH Act
- Coincides with new operational footprint of mobile, EHR, online scheduling and other practice management tools that all use/disseminate PHI
- In light of Snowden, HIPAA related whistleblower activity might increase
- Affordable Care Act (ACA) may create compliance difficulties, in light of billing and other data centric activities