Privacy for Healthcare Data in the Cloud - Challenges and Best Practices

Dr. Sarbari Gupta

sarbari@electrosoft-inc.com

703-437-9451 ext 12

Cloud Standards Customer Council (CSCC) Cloud Privacy Summit

The Hyatt Regency Hotel, Reston, Virginia

March 26, 2015

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Agenda

- Use of Cloud in Healthcare Industry
- Cloud Uncertainties and Responsibilities
- Drivers for Privacy of Healthcare Data
- Challenges
- Best Practices
- Other Promising Avenues

Use of Cloud in Healthcare Industry (I)

- Cloud Usage*
  - *Currently Use: 82.7%; Plan to Use: 9.3%*
  - *Private Cloud: 37%; Hybrid Cloud: 36%; Public Cloud: 23%*

- Cloud Use Cases
  - *Clinical Application Hosting - SaaS[#]*
  - *Business Applications (e.g. Email) - SaaS*
  - *Data Storage (Primary, Backup) - IaaS[#]*
  - *Server Virtualization - IaaS*
  - *Health Information Exchange Services - SaaS*

* Based on 2014 HIMSS Analytics Cloud Survey – June 2014
# SaaS – Software as a Service; IaaS – Infrastructure as a Service

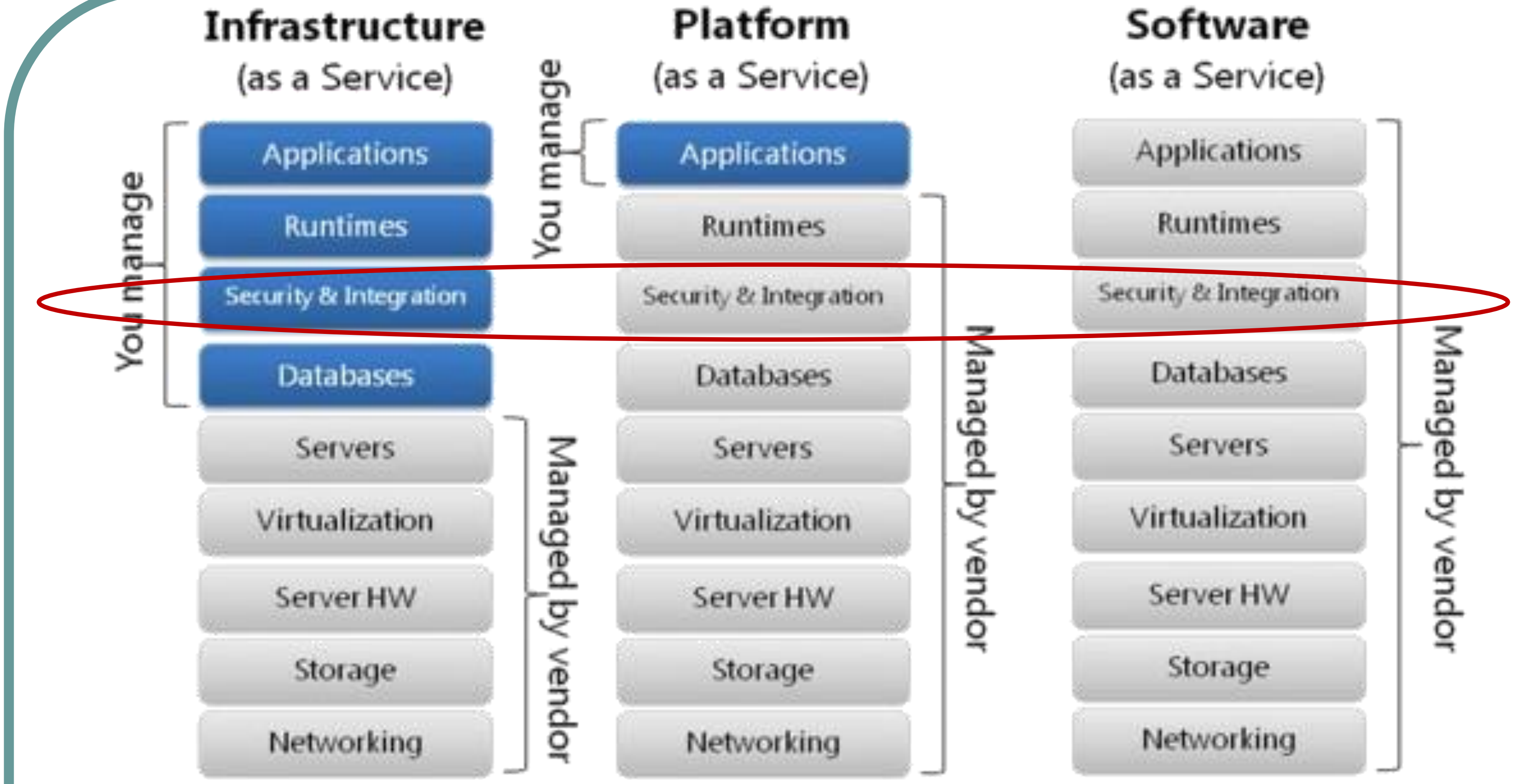
Use of Cloud in Healthcare Industry (II)

- Cloud Value/Benefits
  - *Cost Savings*
  - *Faster Deployment*
  - *Improved Robustness and Availability*
  - *Compliance and Security*
- Drawbacks/Concerns
  - *Poor Visibility into Operations*
  - *Security and Privacy*
  - *Performance and Availability not up to SLA*
  - *Cloud Migration Difficulties*

Cloud Based Systems – Uncertainties

- Where is my Data?
  - *Where does my data reside?*
  - *Is my data co-resident with other users' data?*
  - *Where do backup copies reside?*
- Where is it being Processed?
  - *Where is my process running?*
  - *Am I sharing the processor with other users/organizations?*
- Who has Access?
  - *What are the relevant roles/responsibilities?*
  - *How are users authenticated?*
  - *How are privileges granted/managed?*
- How is my Data Protected?
  - *How is my data protected at rest?*
  - *How is my data protected in transit?*
- Administration and Service Provisioning
  - *Who administers the cloud infrastructure?*
  - *What other players support service provisioning?*
  - *Do they have access to my data?*

Cloud Service Models & Data Protection



Infrastructure (as a Service)

You manage: Applications, Runtimes, Security & Integration, Databases

Managed by vendor: Servers, Virtualization, Server HW, Storage, Networking

Platform (as a Service)

You manage: Applications

Managed by vendor: Runtimes, Security & Integration, Databases, Servers, Virtualization, Server HW, Storage, Networking

Software (as a Service)

Managed by vendor: Applications, Runtimes, Security & Integration, Databases, Servers, Virtualization, Server HW, Storage, Networking

- **SAAS** allows users to run online applications. Off-the-shelf applications are accessed over the Internet. The vendors own the applications and the users pay a fixed subscription fees.
- **PAAS** allows users to create their own cloud applications. Basically, provides an environment and set of tools to allow the creation of new web applications.
- **IAAS** allows users to run any applications they want to on cloud hardware of their choice. Existing applications can be run on the vendor's cloud hardware, potentially replacing a company's data center infrastructure.

Courtesy of CIO Research Council (CRC)

Drivers for Privacy of Healthcare Data

- Broadly Applicable:
  - *HIPAA Privacy Rule*
  - *HIPAA Security Rule*
  - *OCR HIPAA Audit Program*
  - *ONC Heath IT Certification Program*
  - *CMS Meaningful Use Incentive Program*
- Applicable to Federal Organizations:
  - *FedRAMP*
  - *E-Government Act of 2002 (FISMA)*
  - *Privacy Act of 1974*

HIPAA Privacy Rule

- Establishes national standards to protect individuals' personal health information
- Applies to health plans, health care clearinghouses, and health care providers that conduct transactions electronically
- Requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization
- Gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- Sets requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.

HIPAA Security Rule

- Establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity
- Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information

HHS Office of Civil Rights (OCR) HIPAA Audit Program

- OCR conducts audit of selected Covered Entities
  - *Pursuant to HITECH Act audit mandate*
- Uses a comprehensive HIPAA Audit Protocol
  - *Scope includes policies, processes and controls*
- Audit protocol comprises three modules:
  - *Privacy, Security and Breach Notification*

Office for Civil Rights

ONC Health IT Certification Program

- Ensures health IT products/systems conform to standards & certification criteria adopted by the Secretary of HHS
- Assures providers and patients that the Health IT products/systems they use are secure and interoperable
- Publishes Approved Products on Certified Health IT Products List (CHPL)
- ONC Certification Criteria for Security/Privacy
  - *Authentication, access control and authorization*
  - *Auditable events and tamper-resistance*
  - *Audit reports*
  - *Amendments*
  - *Automatic log-off*
  - *Emergency access*
  - *End-user device encryption*
  - *Integrity*
  - *Accounting of disclosures (optional)*
- No additional requirements for cloud-based Health IT

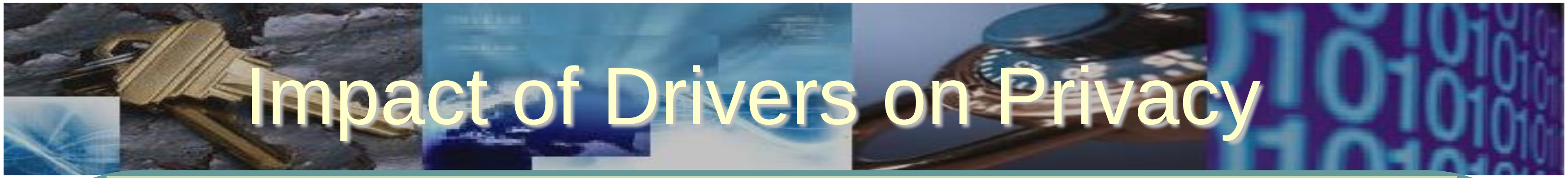
ONC Certified HIT SM

CMS Meaningful Use Incentive Program

- Provides incentive payments to eligible professionals (EP), eligible hospitals (EH), and critical access hospitals (CAHs)
- Promotes adoption, implementation, upgrade or demonstration of meaningful use of certified EHR technology
- EP/EH/CAH obtains incentive payments for:
  - *Selection and implementation of EHR products from ONC Certified Health IT Products List (CHPL)*
  - *Attestation of meaningful use of EHR*

FedRAMP and Privacy

- Federal Risk and Authorization Management Program
  - *Standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services*
  - *Applicable to Federal Government organizations*
- FedRAMP Baseline Security Controls
  - *Currently based on NIST SP 800-53 Rev 3*
  - *Alignment with SP 800-53 Rev 4 in progress*
- Privacy Controls
  - *Currently none*
  - *Indirectly addressed through technical controls*
- Privacy Threshold Analysis (PTA) & Privacy Impact Assessment (PIA)
  - *PTA/PIA limited value for health data in IaaS usage model*



Impact of Drivers on Privacy

- HIPAA Privacy Rule mostly administrative in nature
- HIPAA Security Rule costly/complex to implement
- OCR Audits touch a very small subset of Covered Entities
- ONC Certification Program tests “capability” of EHR to deliver security and privacy
  - *Actual implementation determines security/privacy posture*
- CMS Meaningful Use of certified EHR enforced through self-attestation
- No equivalent to FedRAMP for private industry clouds

Challenges

- Legislation and enforcement of privacy protection of healthcare data relatively weak
  - *Standards/requirements and enforcement methods evolving*
- Healthcare data handled by myriad players with strong vested interests and immense lobbying power
  - *Representation of patient's privacy rights much weaker in comparison*
- Use of cloud further complicates privacy
  - *Vastly increases the uncertainty of healthcare data location and movement*
  - *Access to cloud data from multiple (and possibly mobile) devices spreads data widely*

Privacy of healthcare data in the cloud is a myth at best!

Best Practices (I)

- **Covered Entities**
  - *Select and implement certified EHR*
  - *Implement policy/practices for privacy*
    - Define Privacy Practices
    - Implement Privacy through technical controls
    - Conduct Privacy Self Assessments
    - Establish Business Associate Agreements (BAA) to include privacy requirements
  - *Conduct regular risk assessments and strengthen security posture*
  - *Implement breach detection and timely notification*

Best Practices (II)

- Patients
  - *Know your rights under HIPAA*
  - *Ask for access to your health records*
  - *Amend (correct) your health information*
  - *Receive notice of Provider's privacy practices*
  - *Provide consent to share personal information*
  - *Obtain report on sharing of your health information*
  - *File complaints to enforce privacy rights*

Other Promising Avenues

- Ubiquitous smart mobile devices may serve as foundation for strong (2-factor) authentication to cloud based systems
- Security automation standards (SCAP) may provide mechanism for improved real-time visibility of cloud security posture & status
- HL7 work in support of privacy offers more granular and patient-centric model for privacy
  - *Security labeling*
  - *Data segmentation*
  - *Consent directive*
  - *Fast Healthcare Interoperability Resources (FHIR)*