HIPAA in the Cloud
How to Effectively Collaborate with Cloud Providers

Agenda

• Evolution of the Cloud
• Comparison of Private vs. Public Clouds
• Other Regulatory Frameworks Similar to HIPAA
• Cloud Adoption in Healthcare - Benefits
• HIPAA in the Cloud - Obstacles
• Key Concerns for Working with Cloud Providers
• Health IT Cloud Forecast

Chad Kissinger – Founder | OnRamp

Chad Kissinger is the Founder of OnRamp, an industry leading high security and hybrid hosting provider that operates multiple enterprise class data centers located in Austin, Texas and Raleigh, North Carolina. As an SSAE 16 SOC II Audited, PCI Level 1 and HIPAA compliant company, OnRamp specializes in working with companies in the Healthcare, Financial, Education and other industries meet the rigorous compliance requirements associated with the storage and transmission of sensitive data.

A leader in the development of OnRamp’s HIPAA Compliant Hosting Solutions, Chad brings a wealth of experience, expertise and intimate knowledge for data privacy and security issues.
HIPAA in the Cloud

Evolution in the Cloud

In-House
- Colocation
- Private Cloud
- Public Cloud

Public Clouds
- Multi-tenant Environment
- Shared Equipment
- Typically Pay-as-you-go
- Less Control Over Hardware Performance - “Noisy Neighbors”
- No Physical Access to Equipment
- Hard or Impossible to Inspect/Audit

Private Clouds
- Single Tenant Environment
- Dedicated Equipment
- Customized Solutions
- Guaranteed Performance (Single Tenant)
- Easy to Inspect/Audit
- Suited for Secured Confidential Information & Core Systems

Evolution in the Cloud

Amazon Web Services
- Cloud Services
- Windows Azure

Evolution in the Cloud

Private Clouds
- Hybrid
- Colocation

Evolution in the Cloud

Private Clouds
- Hybrid
- Colocation
Public vs. Private Cloud - Key Concern
How do I achieve auditable compliance?

Evolution in the Cloud

CONFIDENTIALITY  AVAILABILITY  INTEGRITY

SENSITIVE DATA  SENSITIVE DATA

BANKING  E-COMMERCE  GOVERNMENT  HEALTHCARE

GLBA gives the authority to eight federal agencies to administer and enforce the Financial Privacy Rule and the Safeguards Rule which govern the collection and disclosure of personal financial information and requires financial institutions to implement and maintain safeguards to protect customer information.
The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements that prescribe operational and technical controls to protect cardholder data.

FISMA is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or manmade threats.

HIPAA gives the Department of Health and Human Services the authority to mandate the use of standards for the interchange of patient health information and to mandate the steps entities must take to provide for the security and privacy of patient health information.
83% of Healthcare Provider Organizations are using Cloud Services with SaaS-Based Applications being the most popular (66.9%) and 9.3% plan to adopt cloud services.

Top Reasons Healthcare Companies are Adopting the Cloud

Obstacles Regarding Cloud Adoption

2014 HIMSS Analytics Survey (Healthcare Information and Management Systems Society)
Disassociation with Infrastructure

In a physical IT environment, the key components of a compute infrastructure are easily identified and the safety of the data stored within the environment can easily be determined. In a cloud infrastructure, the location of these components, whether they are properly configured and whether they even exist is not always clear.

Compliant Collaboration: Collaboration between in-house employees and subcontractors is necessary to meet and maintain compliance.

Security / Compliance: Risk associated with storing electronic protected health information (ePHI) on platforms or within environments that do not have HIPAA compliant hosting processes, systems and procedures.
Compliant Encryption: Ensuring compliance with NIST standards for all compute, storage and transmission media used to handle PHI.

Media Sanitization: Ensuring compliance with NIST standards for appropriately rendering storage media unusable, unreadable, or indecipherable.

Security Incident Response: Cloud users and providers must prepare for security incidents and adequately detect, report, forensically examine, mitigate and contain and eradicate risk associated with the incidents.
Availability/Uptime: EPHI must be available to authorized users at all times, this facilitates the need for a disaster recovery or secondary site to maintain high availability in the cloud.

Evaluating Providers

Top Considerations When Selecting a Cloud Provider:

1. Physical & Technical Security
2. HIPAA & State Law
3. Patch Management
4. Incident Response
5. Service Level Agreements
6. Customer Support
7. Cloud Service Provider's History
8. Legal & Compliance

2014 HIMSS Analytics Survey (Healthcare Information Management Systems Society)

Approach to Evaluating Cloud Providers

- Employee Training
- Media Handling & Sanitization Policies
- Information System Development Lifecycle
- Cooperative Policies
- Coordinated Incident Response
Business Associates Agreements

- Should reflect division of responsibilities
- Should include (but usually do not) the Administrative, Technical and Physical measures the customer must still take to protect EPHI
- Realistic patient access, amendment and accounting of access request handling

Indemnification & Limitations of Liability

- Indemnifications were specifically excluded from the Omnibus rule despite many requests to address them. Vendors won't accept indemnifications normally.
- Limitations of Liability "contain" the amount of risk accepted and facilitate pricing of vendor products.

Privacy Injury Liability & Insurance

- Privacy Injury Liability - Breach notification, credit monitoring and other expenses concerning breach are usually handled by customer.
- Insurance – Breach notifications and other remediation are conducted by Covered Entity – insurance should cover these costs.
Thank you!