HIPAA in the Cloud
How to Effectively Collaborate with Cloud Providers
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 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 of data privacy and security issues.
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
HIPAA in the Cloud

In-House → Colocation → Private Cloud → Public Cloud
## HIPAA in the Cloud

<table>
<thead>
<tr>
<th>Public Clouds</th>
<th>Private Clouds</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Multi-tenant Environment</td>
<td>- Single Tenant Environment</td>
</tr>
<tr>
<td>- Shared Equipment</td>
<td>- Dedicated Equipment</td>
</tr>
<tr>
<td>- Typically Pay-as-you-go</td>
<td>- Customized Solutions</td>
</tr>
<tr>
<td>- Less Control Over Hardware Performance - “Noisy Neighbors”</td>
<td>- Guaranteed Performance</td>
</tr>
<tr>
<td>- No Physical Access to Equipment</td>
<td>(Single Tenant)</td>
</tr>
<tr>
<td>- Hard or Impossible to Inspect/Audit</td>
<td>- Easy to Inspect/Audit</td>
</tr>
<tr>
<td></td>
<td>- Suited for Secured Confidential Information &amp; Core Systems</td>
</tr>
</tbody>
</table>
HIPAA in the Cloud
HIPAA in the Cloud

Public vs. Private Cloud - Key Concern

How do I achieve auditable compliance?
HIPAA in the Cloud

CONFIDENTIALITY

SENSITIVE DATA

AVAILABILITY

GOVERNMENT

E-COMMERCE

HEALTHCARE

SENSITIVE DATA

INTEGRITY

HIPAA

BANKING

GLBA

Gramm-Leach-Bliley Act

PCI

Payment Card Industry

FISMA

Federal Information Security Management Act

HIPAA

Health Insurance Portability and Accountability Act
HIPAA in the Cloud

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.
HIPAA in the Cloud

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements that prescribe operational and technical controls to protect cardholder data.
HIPAA in the Cloud

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

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.
HIPAA in the Cloud

HIPAA in the Cloud - Adoption & Use

83% of Healthcare Provider Organizations are using Cloud Services w/ SaaS-Based Applications being the most popular (66.9%) and 9.3% plan to adopt cloud services.
HIPAA in the Cloud

ADOPTION & USE

TOP REASONS FOR ADOPTING

- MAINTENANCE COSTS
- SPEED OF DEPLOYMENT
- STAFFING CHALLENGES

83% USE CLOUD SERVICES

- CLINICAL APPS + DATA
- HIE
- HR APPS + DATA
- BACK UP + DISASTER RECOVERY

onramp
HIPAA in the Cloud

**OBSTACLES**

**PERFORMANCE ISSUES**
- 33% reported slow response
- 23% reported downtime or unavailability

**CHALLENGES**

- Operations visibility: 21%
- Customer service: 20%
- Costs and fees: 19%
- Availability and uptime: 16%
- Migration of services or data: 15%
- Contractual issues: 6%
- Other: 6%
- No challenges: 38%
HIPAA in the Cloud

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.
HIPAA in the Cloud

Considerations - **Compliant Collaboration**

Collaboration between in-house employees and subcontractors is necessary to meet and maintain compliance.
HIPAA in the Cloud

Considerations - 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.
HIPAA in the Cloud

Considerations - Compliant Encryption

Ensuring compliance with NIST standards for all compute, storage and transmission media used to handle ePHI.
HIPAA in the Cloud

Considerations - Media Sanitization

Ensuring compliance with NIST standards for appropriately rendering storage media unusable, unreadable, or indecipherable.
HIPAA in the Cloud

Considerations - 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.
HIPAA in the Cloud

Considerations – Availability / Uptime

E PHI must be “appropriately” available to authorized users. This often requires a Disaster Recovery (DR) or secondary site to maintain availability in the case of a cloud outage.
HIPAA in the Cloud

Evaluating Providers

TOP CONSIDERATIONS WHEN SELECTING A CLOUD PROVIDER

WILLINGNESS TO ENTER INTO A BUSINESS ASSOCIATE AGREEMENT

PHYSICAL + TECHNICAL SECURITY
HIPAA in the Cloud

Evaluating Providers

- Employee Training
- Media Handling & Sanitization Policies
- Information System Development Lifecycle
- Cooperative Policies
- Coordinated Incident Response
HIPAA in the Cloud

Subcontractor Negotiations

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
HIPAA in the Cloud

Subcontractor Negotiations

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
HIPAA in the Cloud

Subcontractor Negotiations

Privacy Injury Liability & Insurance

• Privacy Injury Liability - Breach notification, credit monitoring and other expenses related to a breach are usually handled by customer.
• Insurance – Breach notifications and other remediation are conducted by Covered Entity – their insurance should cover these costs.
How OnRamp is addressing HIPAA in the Cloud

- Colocation Space
- Private Cloud Environment
- Backups
- SAN Storage
- Internet
HIPAA in the Cloud

**Forecast**

**Partly Sunny**

Neearly all adopters will expand cloud services

**Areas of Expansion**

- Hosting of archived data
- Back up + disaster recovery
- Hosting of operational apps + data

Only 6% will not adopt cloud services in the future
HIPAA in the Cloud

Q&A
HIPAA in the Cloud

Thank you!