
Understanding the Business Risk of Cloud Computing

Some Clouds may contain tornados!

Clyde Hewitt, MS, CISSP, CHS, PCI-QSA, ISO 27001 Lead Auditor
Managing Consultant, Security Advisory Services

Security Trends: The CIO / CSO Challenge

Questions every healthcare CIO / CSO should ask:

- Where is my data and have I protected it at rest and in motion?
- Are there more legal, regulatory, or contractual requirements I need to be concerned with?
- How do we know that we are addressing our highest risks?
- Does our current suite of security controls provide adequate protections today?
- Would moving our data & applications into the Cloud solve the problem?
- How would we know if we have gaps that need immediate attention?

A Changing Compliance Landscape within the Cloud

The evolution to Cloud does not change the compliance landscape

- Legal and regulatory compliance, including eDiscovery, breach notification, and encryption
- Access control and data leakage
- Third-party terms and conditions
- Audit requirements
- Business continuity management, including backup, recovery, and archiving
- Security information and event management

A Changing Compliance Landscape within the Cloud

Legal and regulatory compliance

- Moving data to a Business Associate does not eliminate the compliance requirements
 - HITECH removed the liability protections from having a valid BAA and no knowledge of non-conformance
 - Gaining visibility into compliance requires due diligence
- Public Clouds must still be fully conforming to the HIPAA & HITECH
 - Additional effort must be exerted to get an enforceable BAA
 - Accounting for disclosures will require subrogation of requirements
 - Supporting n-tier sub-contractors must also be held accountable

A Changing Compliance Landscape within the Cloud

Information Lifecycle Management (ILM)

- ILM in the Cloud requires special care to ensure that data retention schedules are followed
- Designated destruction dates could become problematic if data is replicated and stored off-spindle
- Litigation holds, required by eDiscovery, can present additional challenges as data is moved outside applications
- Getting a clean forensic environment can be more challenging when attempting to log activities

A Changing Compliance Landscape within the Cloud

Encryption Requirements

- Patient Accounts Receivable data may contain credit card numbers which require encryption
- Backups and disaster recovery plans need to be adjusted to meet these more stringent requirements

A Changing Compliance Landscape within the Cloud

Encryption Requirements

- Patient Accounts Receivable data may contain credit card numbers which require encryption
- Backups and disaster recovery plans need to be adjusted to meet these more stringent requirements

Access Control & Data Leakage within the Cloud

Hospitals have tight controls on who can access ePHI

- The challenge is to bridge the gap to public Cloud vendors
- Specialty training and client-specific background checks may be difficult to enforce in a shared services environment

Data leakage is harder to control when different organizations share an environment

- Spindles & database backup tapes may include shared data, if not expressly prohibited & monitored
- A litigation hold and discovery for another customer's legal action could result in the disclosure of your data

3rd Party Terms & Conditions within the Cloud

HITECH requires all Business Associates to be fully compliant with the HIPAA Security Rule

- Cloud providers' supporting vendors must also conform
- A large distributed Cloud environment supporting one hospital could result in a hospital having hundreds of sub-tier Business Associates

Data leakage is harder to control when different organizations operate in a shared Cloud environment

- Spindles & database backup tapes may include shared data, if not expressly prohibited & monitored
- A litigation hold and discovery for another customer's legal action could result in the disclosure of your data

Auditing within the Cloud

Hospitals will be required to “account for disclosures” within the treatment payment, and healthcare operations (TPO) environment once HITECH is fully implemented

- Will the public Cloud vendors be ready to monitor all internal access to ePHI?
- What mechanisms are needed to track access in a shared model?

Business Continuity within the Cloud

As hospitals move clinical applications into the public Cloud, Business Continuity requirements change

- Adding more critical components to the equation
 - Reliance on more critical communication links
 - Loss of relevant experience pool
- Are SLAs written to acknowledge the shared environment, e.g., what is “our systems” fail, then would the Cloud provider be capable of recovering within the RTO/RPO criteria?
 - If multiple systems fail, are the RTO/RPO limits still valid (e.g., do we still get the same priority?)
 - Testing the BCP/DR plan for a major outage in a shared environment may not be possible

Security Incident Management within the Cloud

HITECH's security incident response must be completed within 60 days from when it should have been discovered

- Adequate controls to detect incidents must be built into the Cloud
- Following a breach, the first step of an incident response process is to determine if there is a “*significant risk of financial, reputational, or other harm to the individual.*”
- Depending on how the BAA is crafted, the Cloud provider may want to make a determination before reporting an incident to the covered entity
- This effectively reduces the covered entity's response time and may result in non-compliance

Summary

Hospitals are under intense pressure to reduce costs and increase the responsiveness to increasing information availability demands

- As hospitals research options for moving their data and processes to the Cloud, consider the challenges addressing the business, legal, and regulatory risks