Cloud Computing & Health Care Organizations: Critical Privacy & Security Issues - December 16, 2015

James B. Wieland, Principal, Ober|Kaler
David Holtzman, VP of Compliance, CynergisTek

OBER | KALER
Attorneys at Law

CYNERGISTEK

Welcome

- The slides for today's webinar are available at the right side of your screen in the Handouts pane.

- Type your questions into the Questions pane. We'll answer as many as we can at the end of the program.

- After the program, you'll receive an email with a link to a survey. Please take a moment to fill that out and give us your feedback.

Agenda

- Who We Are
- Cloud Statistics for Health Care
- HIPAA and the Cloud
- Requirements
- Vendor Management
- Data Loss Prevention
- Questions

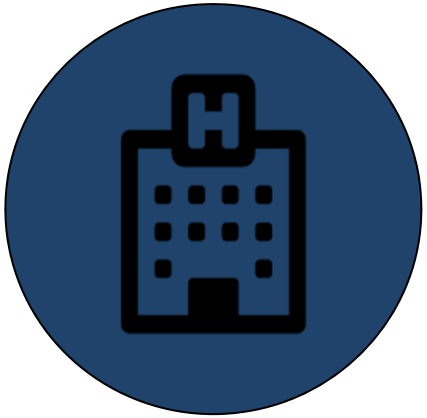
Who We Are: David Holtzman

- Vice President of Compliance Services, CynergisTek, Inc.
- Subject matter expert in health information privacy policy and compliance issues involving the HIPAA Privacy, Security, and Breach Notification Rules
- Experienced in developing, implementing, and evaluating health information privacy and security compliance programs
- Former senior advisor for health information technology and the HIPAA Security Rule, Office for Civil Rights

Who We Are: Jim Wieland

- Shareholder in Ober|Kaler and chair of the firm's Health Care Information Privacy, Security and Technology practice.
- Advises clients on all aspects of federal and state privacy laws, including breach notification.
- Assists clients in negotiating all types of technology contracts in the health care sector.
- Works extensively with data use agreements, including state and federal forms of DUA.
- Chair of the HIMSS Legal Advisory Task Force.

Cloud Statistics for the Health Care Industry



2014 HIMSS Analytics

- 83% of IT health care organizations are currently using cloud services
- The most common cloud-based applications:
  - Hosting of clinical applications and data
  - Health information exchange (HIE)
  - Backups & data recovery
- 23.4% of IT health care organizations chose public clouds for deploying their cloud applications

Cloud Services and Risk

- According to Forbes and Skyhigh Networks, approximately 90% of cloud services are high or medium risk
    - http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP-Cloud-Adoption-Report-Q2-2015-Healthcare.pdf
- Measured attributes include:
    - Data encryption
    - ISO 27001 Certification
    - Multifactor authentication
- On average, 6.8 TB of data are sent to cloud services each month by health care organizations based on measurements from Q2 2015

HIPAA & the Cloud Computing Vendor

Cloud Vendors are Business Associates

- Agents, contractors, and others hired to do the work of, or to work for, the HIPAA Covered Entity, and such work requires the use or disclosure of protected health information (PHI)
- Definition specifically calls out
  - Health Information Organization (or HIE)
  - E-Prescribing Gateway
  - Data transmission services with routine access
  - PHR providers working on behalf of covered entity
  - Subcontractors to a business associate

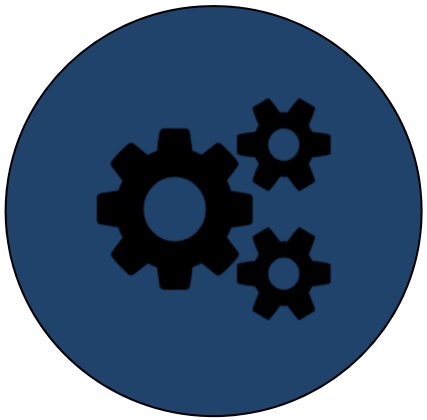
Business Associate or Conduit?

- Provides transmission services of PHI in any form
  - Including temporary storage of PHI incidental to transmission service
  - Examples: postal service, couriers and telephone companies
- Service provider that provides storage of PHI is a BA even if agreement with the CE or BA does not contemplate
  - Any access to PHI
  - Access only on a random or incidental basis
  - Persistence of custody; not the degree of access

BA of a BA: Downstream Contractors

- Each entity directly responsible for requirements of the Security Rule & certain provisions of Privacy Rule
- Liability even if the parties fail to enter into a written BA agreement
- In the event of a breach of unsecured PHI chain of reporting would follow the chain of contracting in reverse

Vendor Management to Ensure Data Safeguards

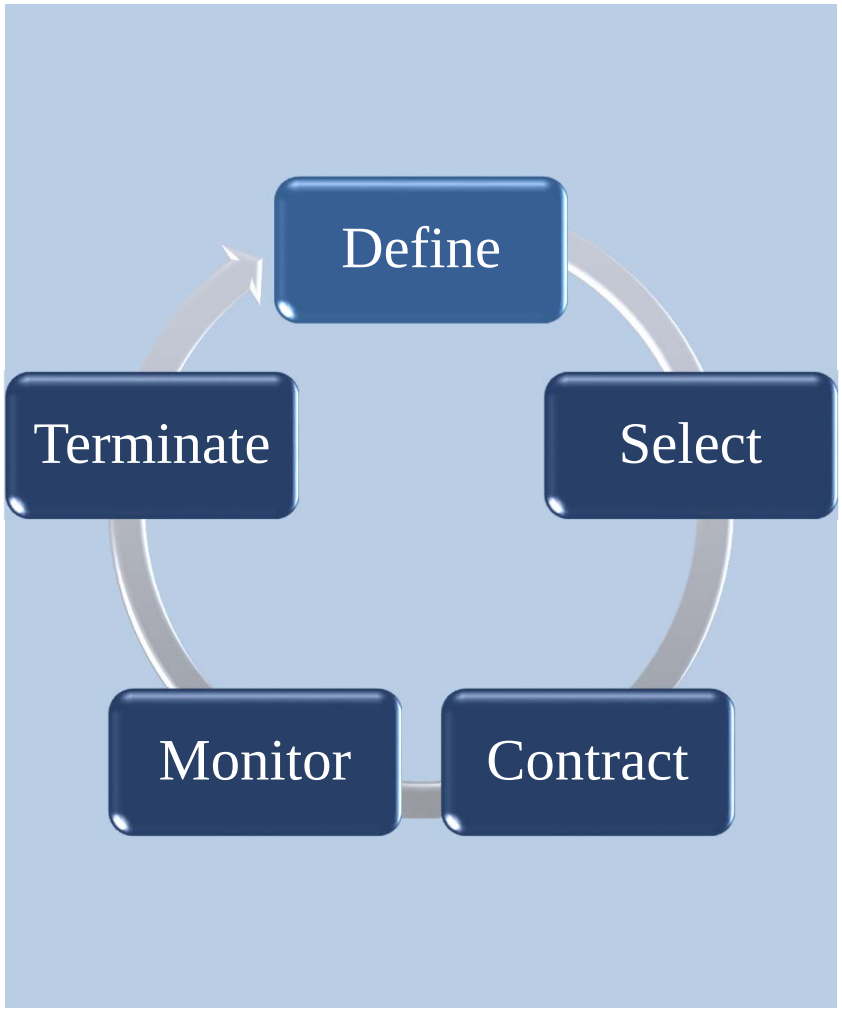


Look at Vendor Relationships

- Implement a process to **evaluate who is a BA, and who is *not* a BA** (i.e., conduit); and sub-BAs
- Keep BAA forms compliant with HITECH language
  - Include language required by the Privacy Rule
  - Consider using the **OCR BAA Template**
  - Add language to protect yourself from an agent issue
- Manage your BA Agreements
  - Keep a BAA tickler
  - Assign who is responsible for managing BAAs

Vendor Security Life Cycle

- Requirements Definition
- Pre-Contract Due Diligence
- Contract Security Specifications
- Performance Monitoring
- Breach Notification
- Contract Termination
- Documentation



Defining Requirements

- Examine Scope of Effort
- Determine What Level of Minimum Necessary
- Identify Security Requirements
- Develop SLAs for Security
- Incorporate into RFI, RFP and/or SOW
- Classify Vendor

Due Diligence: Pre-Contract

- Tailor requests to scope of contract
- Security standard followed
- Include security questionnaire
- Request documentation
- Review third party assessments
- Proof of Training
- Conduct site visit
- Security Incident history

Contract Security Specifications

- Define expectations, material changes, subcontractors
- Minimum Necessary
- Transmission, storage & processing
- Incident response
- Indemnification/Cyberinsurance
- Audit/monitoring
- Reporting requirements
- Contingency operations

Maintenance

- For contracts lasting more than 6 months
- Periodic audits of key processes
- Testing of contingency plans/operations
- Renewal of third party assessments

Breach Notification

- Timeliness of notifications
- Assistance in investigation/risk assessment
- Indemnification for certain costs
- Notifications to public

Contract Termination

- Termination for cause vs. end of contract
- Disposition of data if in receipt
- User/system access
- Reminder of Minimal Necessary
- Other continued responsibilities

Cloud Standards and Integration

Models of Cloud Services

- Public Cloud
  - Service provider makes computing resources such as apps & storage to multiple organizations available over the Internet
- Private Cloud
  - Vendor provides computing resources like Public Cloud in a proprietary architecture, dedicated to a single organization
- Hybrid Cloud
  - Mix of on-premises private cloud and public cloud with orchestration between the platforms
  - Allows workload to move between private and public clouds as computing needs and costs change

Cloud Security

- Shared Responsibility Model
  - ➢ Amazon Web Services (AWS)
    - Vendor protects data centers and servers on which data is stored
    - Application security and data is customer responsibility
      - Customers can purchase additional security services
        - ❑ Data encryption
        - ❑ User authentication
        - ❑ Access logs/audit/monitoring

Data Loss Prevention

Key Benefits

- Identifies storage locations of PHI or other sensitive data
- Identifies data being sent to the Internet/Cloud
- Restricts cleartext transmissions of data
- Allows for policy driven management of data storage
- Minimizes the likelihood of breaches
- Identifies user training gaps or issues

Implementation Considerations

- Important aspects:
  - Data fingerprinting
  - Email integration
  - Web content filter/proxy integration
  - Endpoint protections
- Consider implications of utilizing SSL intercept
- Requires resources for appropriate management

Questions?

Type your questions into
the Questions pane.

We'll answer as many as we can.

More Questions? Contact Us.

James B. Wieland

Principal
Ober|Kaler
jbwieland@ober.com

David Holtzman

Vice President of Compliance Services,
CynergisTek, Inc.
david.holtzman@cynergistek.com
@HITprivacy

OBER | KALER
Attorneys at Law

CYNERGISTEK