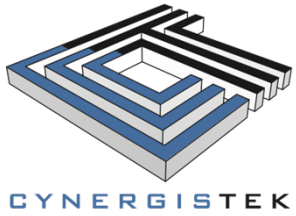
Creating Stable Security & Compliance Relationships

David Holtzman
JD, CIPP/G
VP, Compliance
CynergisTek, Inc.

James Wieland
JD
Principal
Ober|Kaler



OBER | KALER
Attorneys at Law

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.

Session Objectives

Who is a Business Associate

Privacy & Security Rule Standards

Developing a Compliance Plan

Resources and Tools

Who is a Business Associate?

Who is a Business Associate?

- Agents, contractors, and others hired to do the work of, or to work for, the CE, 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

BA Must Safeguard PHI

- Applies to Protected Health Information
  - Created
  - Received
  - Maintained
  - Transmitted
- On behalf of, or received from:
  - Covered entity
  - OHCA
  - Another 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

What is Satisfactory Assurance?

- The Privacy and Security Rules require "satisfactory assurance"
  - Assurance usually takes the form of a Business Associate Agreement
  - Must contain elements specified in the Rule
  - BA only use or disclose PHI as permitted by agreement
  - Safeguard PHI from unauthorized disclosure

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

Can Vendors Avoid HIPAA?

- The absence of a BA Agreement does NOT mean that a BA can avoid HIPAA compliance
  - A BA is determined by HIPAA's definitions and the activities of the BA (or sub), and direct compliance and enforcement by OCR cannot be avoided by simply not having a HIPAA-compliant BA Agreement in place between the CE and the BA, or the BA and its subcontractor

- Just because you are not a BA, HIPAA is still relevant
  - If you do not need access to a covered entity's PHI to perform a "service or function" on "behalf of" such covered entity, then you are most likely not a BA, but you might also not have the authority to access or use such PHI

What are the Requirements?

Responsibilities for Covered Entities

- Ensure that each vendor who meets the criteria as a BA receives and executes a BA agreement.
  - Any vendor who *"creates, receives, maintains, or transmits ePHI on their behalf"* must receive a BAA. CEs are not responsible for Subcontractors, but should be aware of them.
- Any CE who becomes aware of a situation involving non-compliance by a BA must remedy the situation.
  - CEs have the option of terminating the relationship or providing specific direction from remedy.
  - If remedy is sought, CE gives BA guidance to remedy situation within a certain time period.
  - If remedy is not met CE must terminate relationship or incurs risk

HITECH Added New Elements to BAAs

- BA must **comply with HIPAA Security Rule**
- **Minimum necessary applies** to use & disclosures of PHI
- BA must **report breaches** of unsecured PHI to CE
- **Subcontractors agree in writing** to same restrictions
- If BA is going to carry out **CEs obligations** (i.e., providing access to individuals), then BAA must state BA is obligated to perform as required by Rule

BA Privacy Rule Compliance

- Limiting uses and disclosures
  - What is permitted or required by Privacy Rule
  - What is allowed under the BA agreement
    - Compliance with Minimum Necessary Standards
- Breach notification to CE
- Provide copy of ePHI to the CE or the individual as specified in BA agreement
- Disclose PHI to OCR in an investigation
- Provide accounting of disclosures

BA Security Rule Compliance

- Ensure ePHI is used, stored, transmitted or received with:
  - **Confidentiality**
    - only the right people see it
  - **Integrity**
    - the information is what it is supposed to be – no unauthorized alteration or destruction
  - **Availability**
    - the right people can see the ePHI when needed

BA Considerations and Issues

- “I am not a BA” or “We don’t need a BAA”
- Defining permitted “BA Services and Functions”
- An agent, or not
- Security assessments (show me)
- Breach notification timeframes
- Encryption required
- Use of de-identified data
- Foreign (non-U.S.) sub-agents
- Cyberinsurance
- Indemnification (breaches; penalties; lawsuits)
- State law

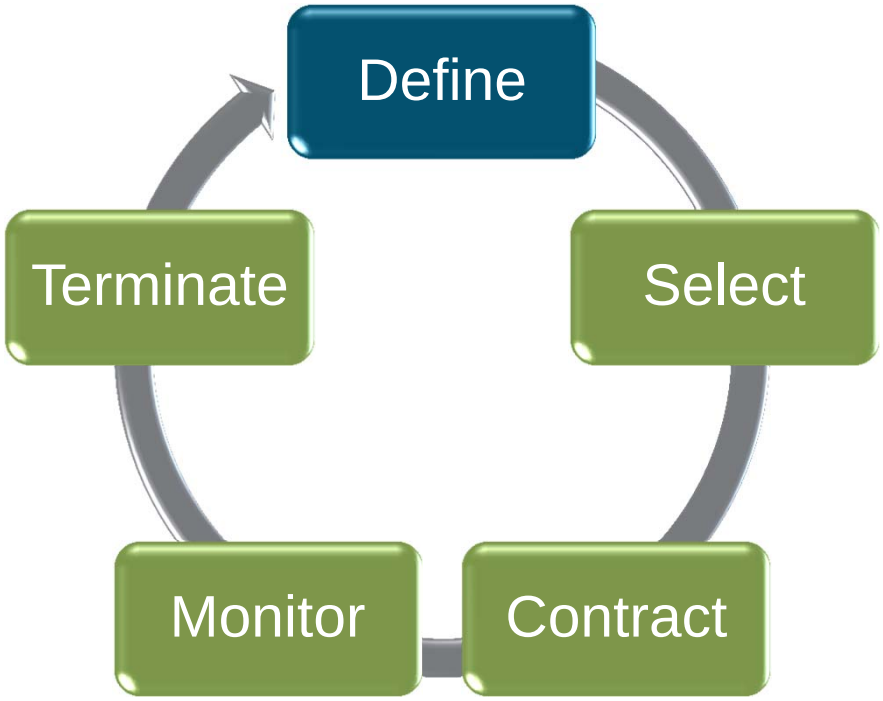
Develop a Vendor Management Program

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

Lifecycle of a Vendor Relationship

- Requirements Definition
- Solicitation/RFP Processes
- Contract & Agreements
- Performance Monitoring
- Termination
- Security Incident Management & Breach Notification
- Documentation



Administrative Oversight

- Requirements definition
  - Classification
  - Security
  - Minimum Necessary
- Solicitation/RFP processes
  - Solicitation/RFP development
  - Pre-contract evaluation
- Contract & Agreements
  - Security requirements
  - BA Agreement development

Operational Oversight of Vendors

- Performance Monitoring
  - Updating documentation as required
  - Back up/recovery
  - Physical security
  - External requests
  - Business changes
- Incident Response
  - Notification of CE
  - Risk analysis
  - Clean up/remediation
  - Notification of others
- Terminations
  - Disposition of information
  - Workforce turnover

Developing a BA Compliance Program

Privacy Policies

- Limiting uses and disclosures of PHI
  - What is permitted or required by Privacy Rule
  - What is allowed under the BA agreement
- Processes to assure use & disclosures respect the Minimum Necessary standard
- Provide an individual access or copies of PHI as specified in BA agreement
- Disclose PHI to OCR when requested
- Produce accounting of disclosures
- Breach notification to CE

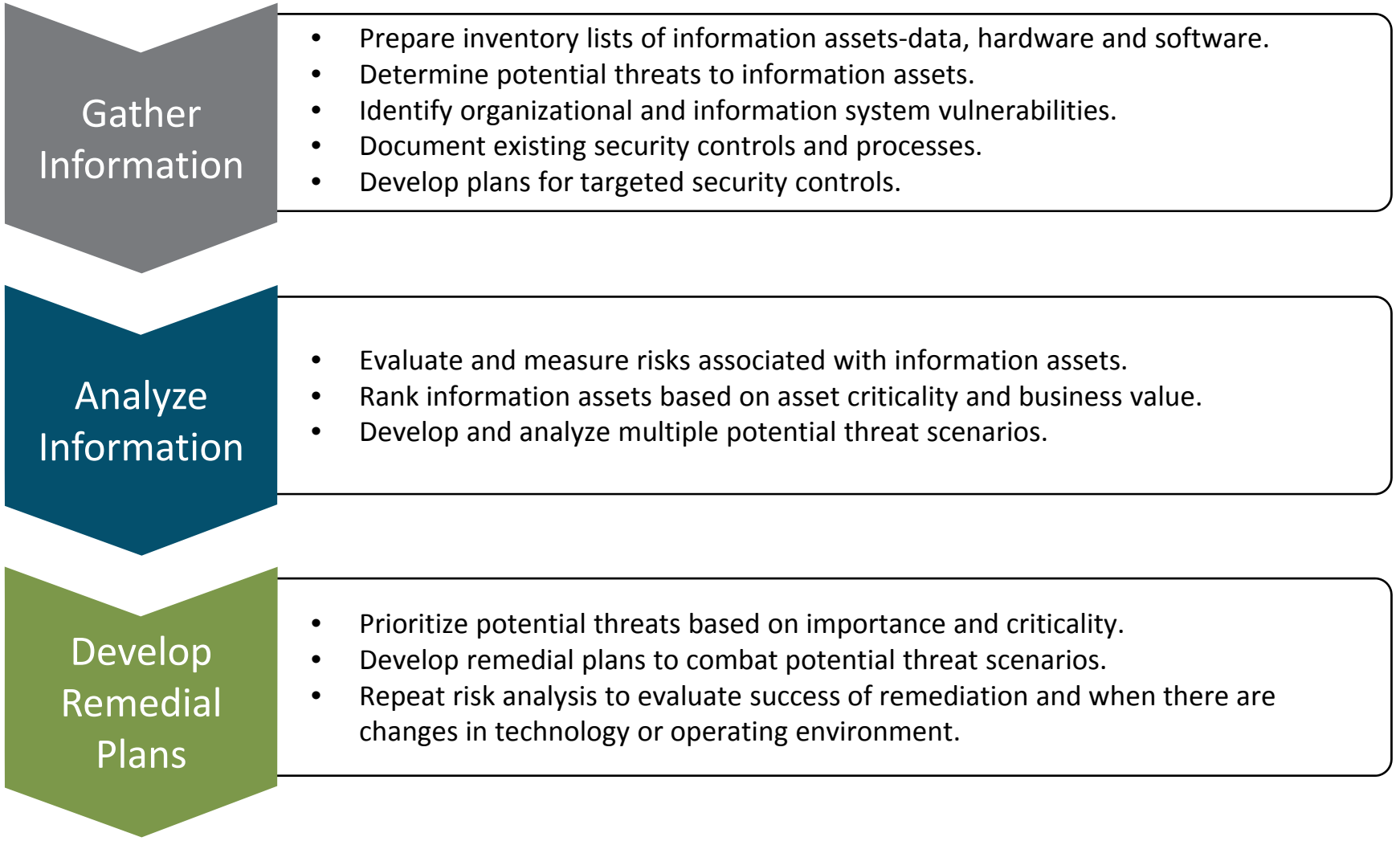
Information Security Risk Assessment

- An assessment of threats and vulnerabilities to information systems that handle e-PHI.
- This provides the starting point for determining what is ‘**appropriate**’ and ‘**reasonable**’.
- Organizations determine their own technology and administrative choices to mitigate their risks.
- The risk analysis process should be ongoing and repeated as needed when the organization experiences changes in technology or operating environment.

What is Risk Analysis

- The process of:
  - Analyzing threats and vulnerabilities in a specified environment,
  - Determining the impact or magnitude, and
  - Identifying areas needing safeguards or controls

Performing a Risk Analysis



Document Results of Risk Analysis

- Goal is to document the findings from the risk analysis into an official document and briefing
- Presented as a systematic and analytical approach to assessing risk with three objectives:
  - Gain understanding of risks in the environment
  - Identify resources to reduce or correct threats to e-PHI
  - Demonstrate compliance with HIPAA Security requirements
- Document retention requirement in HIPAA Rules is 6 years

Train the Workforce

- Provide training in the following areas:
  - Basic HIPAA Security & Privacy requirements
  - Specific organizational policies for safeguards of PHI
  - Appropriate knowledge around privacy uses and disclosures
  - Any specific position related responsibilities
  - Make training relevant and continuous, and *DOCUMENT completion*
- Include orientation, refresher and periodic reminders
- Initial training within a reasonable period of time after starting role granting access to PHI

Resources and Tools

Resources and Tools

- **OCR HIPAA Privacy & Security**
  - http://hhs.gov/ocr/privacy
- **HIPAA Security Rule Risk Assessment**
  - HHS Risk Assessment Tool for Small Providers
    - http://www.healthit.gov/providers-professionals/security-risk-assessment
  - NIST HIPAA Security Risk Assessment Tool
    - http://www.scap.nist.gov/HIPAA
- **Sample HIPAA Privacy and Security Policies**
  - California State Health Information Program Manual
    - http://www.ohi.ca.gov/calohi/ohii-shipm-manual.htm
  - HIPAA Collaborative of Wisconsin (HIPAA-COW)
    - http://hipaacow.org

Questions?

Jim Wieland, Esq.

jbwieland@ober.com

David Holtzman

david.holtzman@cynergistek.com

@HITprivacy