Recovering from a Breach: Strategies for Reporting and Responding to OCR

Presented by:
David Holtzman
Vice President for Compliance

CynergisTek, Inc.

Founded in 2004

CynergisTek has been providing services to our clients since 2004, but many of our clients have been with one or both of the founders since well before the company was founded.

Consulting Services

CynergisTek provides consulting services and solutions around information security, privacy, IT architecture, and audit with specific focus on regulatory compliance in healthcare.

Synergistic

The name “CynergisTek” came from the synergy realized by combining the expertise of the two co-founders – building scalable, mature information security programs and architecting enterprise technical solutions.

Securing the Mission of Care

CynergisTek Services are specifically geared to address the needs of the healthcare community including providers, payers, and their business associates who provide services into those entities.

Today's Presenter

- 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
- Over 12 years of experience 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

David Holtzman
CynergisTek, Inc.

Agenda

Agenda

- Considerations of Timing of Notice
- OCR Breach Reporting Portal
- Prepare for the Omnibus Request
- Priorities for Preparation

Considerations of Timing of Breach Notification

HIPAA Notification & the BA Trap

- Without unreasonable delay to individuals affected
- In no case later than 60 days following discovery
- Notification to OCR when individual notice is sent
- Breach “at or by a business associate”
  - Covered entity is ultimately responsible for ensuring individuals are notified
  - Covered entity may delegate responsibility of providing individual notices to the business associate

State Notification Triggers HIPAA Notice

	Florida	California
Information Protected	Expansive definition of personal information	Medical Information Electronic Personal Information
Who is Covered	Any commercial or government entity that acquires or maintains personal information	Licensed healthcare facilities Any commercial or government entity that acquires or maintains personal information
Test	Unauthorized disclosure that could cause harm	Unauthorized acquisition of personal or medical information
Notification and Reporting Requirement	Florida consumers within 30 days. >500 notify AG >1,000 credit bureaus	California consumers within 15 days. Healthcare facilities notify CDPH 15 days. AG computerized information affecting >500.

Approaches to Reporting on OCR Breach Portal

Covered Entity or Business Associate?

*** Please select one of the following:**

- ○ Are you a Covered Entity filing on behalf of your organization?
- ◉ Are you a Business Associate filing on behalf of a Covered Entity?
- ○ Are you a Covered Entity filing on behalf of a Business Associate?

Breach Start and Discovery Dates

Breach Dates: Please provide the start and end date (if applicable) for the dates the breach occured in.

* Breach Start Date:

* Breach End Date:

Discovery Dates: Please provide the start and end date (if applicable) for the dates the breach was discovered.

* Discovery Start Date:

* Discovery End Date:

Type of PHI Involved in Breach

*** Type of Protected Health Information Involved in Breach:**

- [x] Clinical
- [x] Demographic
- [x] Financial
- [x] Other

*** Clinical**

- [ ] Diagnosis/Conditions
- [ ] Lab Results
- [ ] Medications
- [ ] Other Treatment Information

*** Demographic**

- [ ] Address/ZIP
- [ ] Date of Birth
- [ ] Drivers License
- [ ] Name
- [ ] SSN
- [ ] Other Identifier

*** Financial**

- [ ] Claims Information
- [ ] Credit Card/Bank Acct #
- [ ] Other Financial Information

*** Type of Protected Health Information Involved in Breach (Other):**

4000 / 4000

What Safeguards in Place?

*** Safeguards in Place Prior to Breach:**

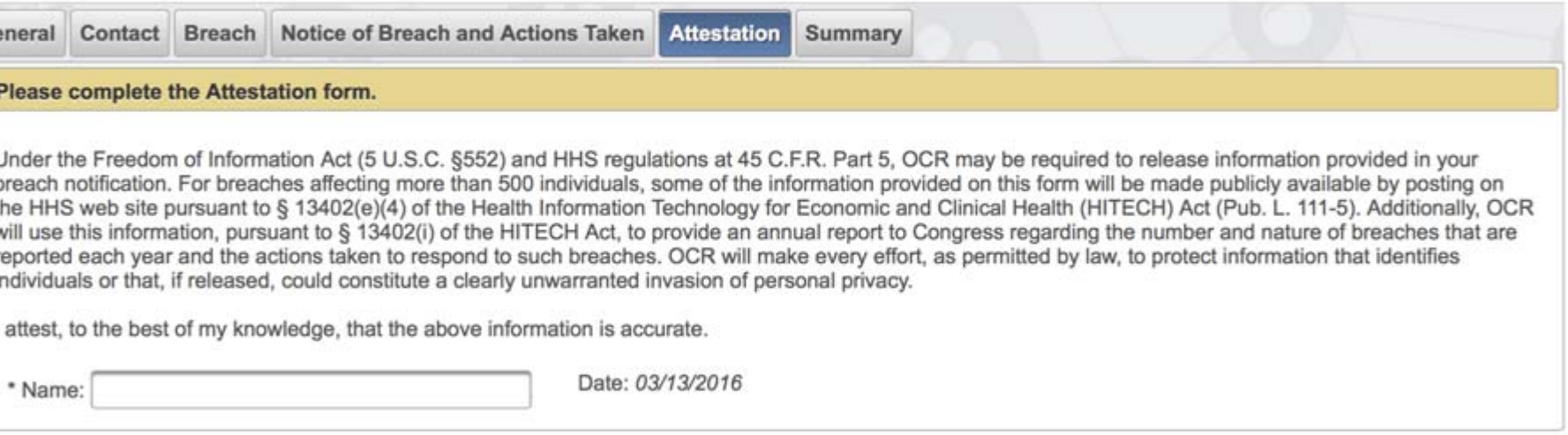
- [ ] None
- [ ] Privacy Rule Safeguards (Training, Policies and Procedures, etc.)
- [ ] Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)
- [ ] Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)
- [ ] Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

What Breach Actions Have Been Taken?

*** Actions Taken in Response to Breach:**

- [ ] Adopted encryption technologies
- [ ] Changed password/strengthened password requirements
- [ ] Created a new/updated Security Rule Risk Management Plan
- [ ] Implemented new technical safeguards
- [ ] Implemented periodic technical and nontechnical evaluations
- [ ] Improved physical security
- [ ] Performed a new/updated Security Rule Risk Analysis
- [ ] Provided business associate with additional training on HIPAA requirements
- [ ] Provided individuals with free credit monitoring
- [ ] Revised business associate contracts
- [ ] Revised policies and procedures
- [ ] Sanctioned workforce members involved (including termination)
- [ ] Took steps to mitigate harm
- [ ] Trained or retrained workforce members
- [ ] Other

Attesting to Accuracy of Information



Prepare for the Investigation

The “Omnibus Request”

- OCR Breach Investigation Document Request Letter
  - 15 – 20 separate interrogatories for documentation to meet a specific standard or specification
  - Documentation of incident and response
  - LoProCo breach risk assessment
  - Notification letters to patient and media (if needed)
  - Last HIPAA Security Rule enterprise-wide risk assessment
  - Steps taken to address gaps in last risk assessment
  - Policies, procedures and safeguards to demonstrate administrative, physical & technical safeguards are in place

Key Issues in OCR's Enforcement Cases

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

OCR Corrective Action Plans

- Most resolution agreements cite to Security Rule
  - Enterprise wide risk analysis is foundation
  - Expectation that encryption is used on all portable and mobile devices & media
  - Encryption of network servers when reasonable and appropriate
  - Managing/controls of device & media
  - Contingency planning

Priorities For Preparation

Get Prepared: Practice Response

- Does each breach response member know his/her responsibilities?
- Do you have documentation to support that there is not unreasonable delay in notification?
- Have you considered what state breach issues will be triggered?
- Do you have your response to the breach portal practiced and planned?
- Are you prepared for OCR's Omnibus Request?

Questions?

Questions?

David Holtzman

david.holtzman@cynergistek.com

512.405.8550 x7020

@HITprivacy