



---

## Now You See It, Now You Don't: Data Breaches

Marti Arvin  
*Chief Compliance Officer, UCLA*

Cheryl Washington  
*Chief Information Security and Privacy Officer, Office of the President*

Deborah Yano-Fong  
*Chief Privacy Officer, UCSF*

---

---

---

---

---

---

---

---



---

## Overview of Presentation

- Preparing for a Breach
  - National Risks
  - New Risks
  - Risk Mitigation Strategies
- Responding to a Breach
  - UC Incident Response Plan
  - Internal Check lists
    - Communication plan
    - Investigation procedures
    - Internal/External Notifications
    - Corrective Action Plans
- Post-Incident Review



---

---

---

---

---

---

---

---



---

## Preparing For a Breach

- Identify the Risks
  - National Risks
  - Security and Privacy Risk Assessments for Your Organization

---

---

---

---

---

---

---

---

## OCR Statistics – January 2013

Top Reasons for HITECH Breaches by BAs As of Dec. 17, 2012	
# of Breaches	Reason for Breach
36	Theft
30	Unauthorized Access/Disclosure
19	Loss
8	Hacking/ IT Incident
3	Unknown

Source: Health Information Privacy/Security Alert Analysis of HHS Office for Civil Rights Data

---

---

---

---

---

---

---

---

## Mitigate the Risks

- Major focus to decrease the risk of stolen/lost mobile devices/laptops is **encryption**
- Major focus to deter unauthorized access is auditing/monitoring and education of the workforce
- However, we have new challenges on the horizon...

---

---

---

---

---

---

---

---

## New Risks

- New ways to share PHI
  - Accountable Care Organizations/Accountable Care Collaborations
  - Transitional Care Management Arrangements
  - Hosting another organization's Electronic Medical Record
  - Transmitting PHI to a third party EHR, not your BA.
  - National un-mandated diagnostic registries
  - Cloud Computing



---

---

---

---

---

---

---

---

## How to Mitigate These New Arrangements?

- New ways and reasons to exchange electronic data in health care for treatment, quality, administrative, and research purposes.
- First priority, determine the purpose for the exchange and the specific data elements required to meet this purpose.



---

---

---

---

---

---

---

---

## Assessing the Exchange Arrangement

- Once the purpose and data elements are determined, then a standard process includes...
  - Determine how the information will be exchanged. Will it be "pushed" or "pulled"?
  - Is the data being transmitted securely? Stored securely?
  - A documented Security Risk Assessment
  - Obtain a Business Associate Agreement \* (\*UC BAA document)



---

---

---

---

---

---

---

---

## New Arrangements

- Develop contracts/agreements to clearly define roles and responsibilities
- Define protocol for responding to a breach, which includes expectations and liability
- The challenge is to sort out when each party will be responsible and for what component.



---

---

---

---

---

---

---

---

## What If?

**Scenario 1:**

A Medical Group is providing EHR services to a group of individual community practitioners:

- In this capacity, they are not a covered entity,
- They are the BA of the community physicians.

An academic medical center is requested to send the referring community physicians their patient information via the Medical Group's EHR system.



---

---

---

---

---

---

---

---

## Questions for Scenario 1

1. Does the Academic Medical Center need to have a BAA with the EHR company (the Medical Group)?
2. Does the answer change if the EHR is a third party vendor and not a Medical Group?
3. If there is a breach of the Academic Medical Center's ePHI from the Medical Group's EHR, who is responsible for the notifications?

---

---

---

---

---

---

---

---

## Scenario 2

XRay Radiation Dose Registry:

Your doctors want to start a national registry to collect radiation dose levels from across the country.

- Not currently mandated, but definite value to patients and health workers.
- ePHI required for this registry.
- Identifiable reports will be provided to each organization
- Aggregate benchmark data as well
- No current plans to report high levels of radiation, if identified.

---

---

---

---

---

---

---

---

## Questions for Scenario 2

1. Is consent/authorization from the patient required to send this data to the registry?
2. Since the exchange is between covered entities, is a BAA required/reverse BAA?
3. If safety issues are identified related to high levels of radiation exposure, what are the legal responsibilities of the entity housing the radiation dose registry?
4. Who is responsible for notification if the database is breached?



---

---

---

---

---

---

---

---

## Tips for Managing your Vendor Relationships

- Collaborate with your Legal Counsel, Health Plan Strategies/Contracting and Clinical Departments about the arrangement
- Collaborate with your information security and privacy experts for Security Risk Assessments related to the arrangement
- Standardized UC BAA
- Resource: CalOHII's "Model Modular Participant's Agreement"  
<http://www.ohii.ca.gov/calohi/PrivacySecurity/ToolsToHelpYou/mmpa.aspx>

---

---

---

---

---

---

---

---

## Responding to a breach



*The Incident Response Life Cycle includes several phases*

- How do you get a handle on what needs to happen first?
  - Checklists can help
- Who will be responsible for what?
- How do you stay on top of the investigation?

---

---

---

---

---

---

---

---

## What needs to happen first?

- Be familiar with the UC Security Incident Response Plan.
- Prepare notification template letters for individuals and regulatory agencies.
  - These will vary based on the statute or regulation you dealing with in the incident
  - The details of the incident itself will need to be added but the majority of what will be needed can be templated.
  - Remember even if the letter is only going to the patient there is a chance it will end up on the press
- Get agreements with external experts in breach response.

---

---

---

---

---

---

---

---

## Internal Checklist

- Have a checklist prepared which includes
  - Who to contact internally
  - How the issue will be triaged
  - Who will be responsible for what (this may depend on how issue is triaged)
  - Who you may need to contact externally and in what circumstances
  - UC Breach decision tree



---

---

---

---

---

---

---

---

## Internal Checklist

1. Communication plan:
  - senior management,
  - board members,
  - legal,
  - risk management,
  - IT,
  - media relations and
  - others

---

---

---

---

---

---

---

---



## Internal Checklist

---

2. Initial action plan:

- determine who does what activities based on expertise
- manage internal and external inquiries (communication)
  - Media relations is critical here

---

---

---

---

---

---

---

---



## Internal Checklist

---

3. Investigation and risk assessment activities:

- what information was lost, disclosed, intercepted, or altered
- what occurred, how and why, and potential liability

---

---

---

---

---

---

---

---



## Internal Checklist

---

4. External notification:

- enforcement agencies and patients
- timelines to be considered based on what and when you know
- determine how to send the notifications based on what you learn
- Consider a separate checklist for this

---

---

---

---

---

---

---

---



## Breach Notification Checklist

- Individual notification
  - State law in CA and other states
- DPH notification
  - Required versus courtesy
- Notice to the Secretary
- Notice to the Attorney General
- Media Notification
  - Required versus courtesy
- Internal workforce

---

---

---

---

---

---

---

---



## Internal Checklist

5. Response plan to inquiries after notification:

- Who will initially respond to the patient?
  - External company
- When will it be triaged to your organization?
  - Who will be the point person?
  - Do you need a script?
- Remember patients may contact someone they work with directly so prepare the workforce to direct them to the right place
- litigation (determine who the contact will be)

---

---

---

---

---

---

---

---



## Internal Checklist

6. Corrective action plans:

- remediate damages
  - Do you need/want to offer credit monitoring
- audit and monitor
  - What follow-up items need to be done

---

---

---

---

---

---

---

---

## Post Incident Review Cycle

```
graph TD; A[Preparation] --> B[Incident & Response]; B --> C[Containment, Eradication & Recovery]; C --> D[Post-Incident Activity]; D --> A;
```

- One of the most important phases of the incident life cycle is also most often overlooked.
- The *post incident review* creates an opportunity to learn lessons from the incident response.

---

---

---

---

---

---

---

---

## Post Incident Review

- The incident response plan should mature over time to reflect new threats, improved technology, and lessons learned.
- Universities can leverage the post incident review process to learn valuable lessons, improve the campus' security posture, and update the incident response plan and policies.
- Over time data collected from the lessons learned session can be used to:
  - Justify additional funding for the incident response team
  - Identify and study trends that may indicate security weaknesses and threats
  - Provide input to the risk assessment process and lead to the selection and modification of controls
  - Measure the success of incident response team

---

---

---

---

---

---

---

---

## Benefits of a Post Incident Review

- Hosting a "lessons learned" session can be extremely helpful in improving security measures and the incident handling process itself.
- Potential outcomes of the post-incident review session include:
  - Opportunity to assess the effectiveness of the university's response plan.
  - Opportunity to evaluate existing security and privacy protection controls or identify the need for additional controls.
  - Opportunity to update the university's general security and privacy awareness and training materials

---

---

---

---

---

---

---

---



## Post Incident Review Session

- Host the meeting within several days following “containment, eradication, and recover” phase.
- Document major points and action items.
- Assess the escalation process.
- Determine if reporting lines were clear, organizational teams worked effectively, and communications channels were sufficient and effective.
- If the university is required to produce a correction action plan (CAP), review the CAP and make sure someone is responsible for its management and execution.
- Document aspects of the response that went well.

---

---

---

---

---

---

---

---



## Sample Questions to Discuss During the Review Session

- What happened?
  - What actions can you take to prevent similar incidents in the future?
  - Is there a need for continuous monitoring?
- How quickly was the incident identified?
- How well did the university manage the incident?
- How well did staff and management perform?
  - Was every team member prepared to manage the incident? If not, what steps can we take to better prepare the staff?
- Were the documented procedures followed?
- How effective are your security policies?

---

---

---

---

---

---

---

---



## More Sample Questions

- Are the internal and external communication plans effective?
- Did information flow in a timely manner? If not, what information was needed sooner?
- How could information sharing be improved?
- Overall, what would staff and management do differently?
- If the incident involved a third party, did the vendor agreement clearly spell out the responsibilities of each party?
  - Do we need to hold the vendor to higher security standards?
- What additional resources (e.g., people or tools) are needed to detect, analyze, and mitigate future incidents?

---

---

---

---

---

---

---

---

## Post Incident Review Report

- Create a report
- The post-incident report will become part of the university's knowledgebase for security and privacy related incidents.
- The response team can reference this knowledgebase for assistance in handling similar incidents in the future.

---

---

---

---

---

---

---

---

## QUESTIONS



---

---

---

---

---

---

---

---

## Contact Information

- Marti Arvin
  - Chief Compliance Officer, UCLA
- Cheryl Washington
  - Chief Information Security and Privacy Officer, Office of the President
  - [Cheryl.washington@ucop.edu](mailto:Cheryl.washington@ucop.edu)
  - 510-987-9189
- Deborah Yano-Fong
  - Chief Privacy Officer, UCSF

---

---

---

---

---

---

---

---