



Notification & Security Act: Lost PDA/Laptops Incident Response

CHITA Forum – Session XVII
March 21, 2006

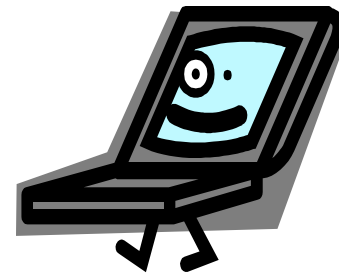
Once Upon a Time...

- There were two little laptops.
 - Their names were

SECURE

and

Breach



SECURE Laptop . . .

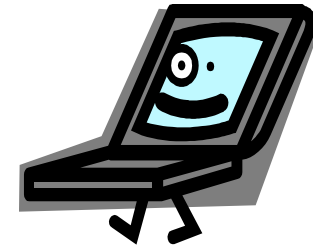
- **had a Mommy, her name was Owner, and Daddy, his name was Operator, who took very good care of him.**
 - **They made sure he kept up with his “vaccinations” so no viruses could harm him.**
 - **They taught him how to protect his “private parts” from bad people.**
 - **They kept him safe and secure from scary people who might want to kidnap a cute little laptop.**

SECURE was a happy little laptop...

- and made everyone around him happy & proud.
- His accomplishments were recognized and appreciated by Owner, Operator and their entire extended family.



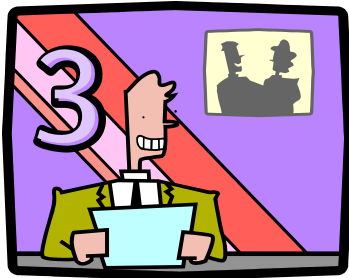
The second little laptop. . . .



■ **Breach** not so lucky

- He was a laptop orphan in a large IT “orphanage”**
- No one paid much attention to him.**
- He didn’t get his vaccinations against viruses.**
- He had worms.**
- No one told him how to protect himself.**
- He spent a lot of time chatting with strangers online and sharing all his secrets.**
- Soon he ran away with a stranger.**

Pretty soon the newspaper and TV headlines read.





Everyone likes a happy ending. . .

Today we are going to give you:

- “Parenting tips” on how to take good care of your laptops, and other media devices so you too can have a happy and secure laptop instead of a bad breach in the news.....
- and if despite good parenting you still end up with a bad breach, how you can handle it.....

Today's Topics

- Policies
- Notification
- Incident Response



Policies & Procedures

Bill Thieleman

Group Health Cooperative





Portable Device Policy

- Address specific portable devices and storage media
 - Laptop, PDAs, storage media
- Determine what devices are approved for business purposes
 - entity deployed
 - entity approved personally-owned devices
 - What portable devices supported



Portable Device policy

- Federal/state laws applicable to PD users
- Users must observe
 - technical, physical, administrative security safeguards
 - operational policies and user standards
- Reserve right to monitor use of PDs & storage media
- Reserve right to revoke privilege of PD use



Portable Device Policy

- Will PHI be allowed on certain devices?
 - Specify what devices, for what purposes.
 - And if so, with what security protections?
- Define user responsibilities re:
 - Confidentiality
 - Security
 - Integrity
 - Availability of PHI



Policy:

Address Technical Safeguards

- Specific to organization
 - Passwords
 - Encryption
 - Software
 - Log Off
 - Call Home technology
 - Storage of data on secure servers via portal



Policy:

Address Physical Safeguards

- Never leave unsecured and in plain sight
- Use cable locks when appropriate
- Lock PDs away where not seen or accessed
- Discuss transport in vehicles
- Discuss storage of PDs at home
- Engrave personally owned devices



Policy:

Address Administrative Safeguards

- **Storage of PHI**

- Security: password, encryption, store to servers
- Limit to work responsibilities

- **Accessibility of PHI to other providers/staff**

- **Password rules**

- **Internet use:** safe, prudent use; encrypted e-mail, alternative secure messaging

- **Reporting** theft/loss, tampering, unauthorized access



Policy:

Reference related policies & procedures

- Incident response procedure & assigned responsibilities
- User accountability
- Risk management of information & systems
- Incident reporting requirement for staff & mgrs



Policy:

Additional Security Strategies

- Targeted education for PD/Laptop users
- System required password changes
- Charge accountable dept for cost of response to device loss
- Address in C&S Agreement
- Controlled decommissioning of devices



Policy:

Procedural Content

- What types of devices included in policy
- Discuss risks and liabilities of PDs
- What entity support available for PDs
- Installing a PD on a workstation
- Security standards
- Responsibilities, e.g. Info Security, managers, users, Info Services
- Definitions: portable device, storage media



Notification

Richard Meeks
UW Medicine

UW Medicine
HIPAA
Program Office



Notification Requirements

- Legislative requirements to notify people when there has been a security breach of a system containing their personal information.
- SB 6043:
 - An act relating to breaches of security that compromise personal information
- Nearly 35 other states and debate for federal legislation.



Notification Law

- Effective July 23, 2005
- Codified at RCW Titles 19.255.010 (private entities) and 42.17.31922 (government agencies)
- Applies to government agencies and “any person or business that does business in the state” who also “owns or licenses computerized data that includes personal information



Examples of Incidents

- Hacking into server containing billing files with names & SSNs
- **Stolen computers with names & SSNs**
- Documents containing names & SSNs mailed or faxed to wrong people
- Business Associate has compromise



Notification Law (cont.)

- Requires them to “disclose any breach of the security, following discovery or notification of a breach in the security of the data to any resident of Washington state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”



Notification Law (cont.)

- Disclosure shall be in the most expedient time possible but can be delayed if:
 - A law enforcement agency determines that disclosure will impede a criminal investigation, or
 - To determine the scope of the breach and restore the reasonable integrity of the data system



Notice of Potentially Affected Individuals must be given either:

- In writing, or
- Electronically, if you comply with the requirements of the federal Electronic Signatures in Global and National Commerce Act; or

Notice of Potentially Affected Individuals must be given either:

(cont.)

- Substitute notice, if costs would exceed \$250K, or more than 500K people need to be notified, or the entity does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - Email notice when the entity has an email address for the subject person;
 - Conspicuous posting of the notice on the entity's web site page, if the agency maintains one; and
 - Notification to major statewide media.

Notice of Potentially Affected Individuals must be given either:

(cont.)

Or

- According to the organization's own notification procedures which are part of its information security policies, as long as they are consistent with the timing requirements of the law



Breach of the Security of a System

- Means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information. It does not include:
 - A “good faith” acquisition of the information by an employee or agent for the owner’s/licensor’s business purposes, or
 - A “technical breach... that does not seem reasonably likely to subject customers to a risk of criminal activity.”



Personal Information

- Is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements:
 - Social Security number,
 - Driver's license number,
 - Washington ID card number, or
 - Account number, credit or debit card number in combination with any security/access code or password which would "permit access" to the individual's "financial account"



Practical Impacts

- Encrypt Sensitive Data
- Recognize this new cost of doing business



Incident Response

Ellen Rubin
UW Medical Center

UNIVERSITY OF WASHINGTON
MEDICAL CENTER
UW Medicine

Applicable Law



- 45 CFR Part 164; Section 164.530 (d)
 - (1) *Standard: Complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.
 - (2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.
- 45 CFR Part 164; Section 164.308(a)(6)
 - (i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents.
 - (ii) *Implementation specification: Response and Reporting (Required).* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
- RCW Titles 19 (private entities) and 42 (government agencies)



Other Potentially Applicable Laws

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act of 2002 (SOX)
- Data Disposal Rule - Federal Trade Commission (FTC) - Fair Credit Reporting Act (FCRA), 6/1/2005

Security Incidents Policy Components

- Process to receive and report complaints & incidents
- Training for workforce - how to make a complaint or report an incident
- Documentation of complaint/incident
- Investigation of complaint/incident
- Resolution of complaint/incident



Examples of Incidents



- Stolen/Lost Devices:
 - from the Seattle Times over the last three months:
 - *“Records for 125 patients were stolen when two employees’ work laptops were stolen from their cars Friday...”*
 - *“On Dec. 31, a theft of a laptop from an health care employee’s car resulted in the loss of more than 358,000 records of current and former patients...”*
 - *“Laptop theft from a health care institution’s off-site offices results in loss of the information on 1600 patients over the holiday weekend...”*
 - *“The state Department of Social and Health Services reports computer thefts recently...”*
- Stolen/Lost Electronic Media
- Hacker

Incident Response & Investigations Policy Components



- Security Team Handling Procedures
 - Forensics
 - Recover information and return to business operations ASAP
 - Asset recovery procedures
- Escalation Procedures (Institutional Risk)
 - Law enforcement, police report, FBI
 - Communication plan / procedures
 - Board, President, Hospital Administration, employees
 - Determination of Institutional Risk
 - Attorney/Client Privilege

Roles & Responsibilities Security Team



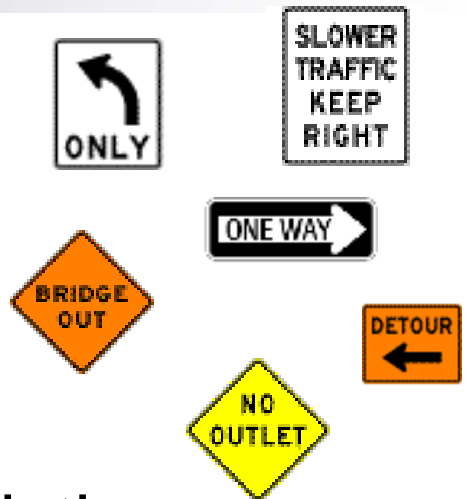
1. Define Security Incident Response Team members

- ISO
- Risk Management
- Compliance Officers
- IT Security
Director/Manager
- Medical Director
- Administrator
- Nursing
- Privacy Official
- Department Chair/Medical Director
- Department Administrator/Manager
- System Owner
- System Operator
- Public Relations
- Legal

2. Define who leads the Incident Response Team

Conduct Investigation

- Defined Decision Process
- Disclosure/Notification Procedures -victims
 - Include ID theft information
 - <http://www.atg.wa.gov/consumer/idprivacy/IDTheftWhatToDo.shtml>
 - Public Relations: have response ready.
- Consider notifying OCR of the incident.

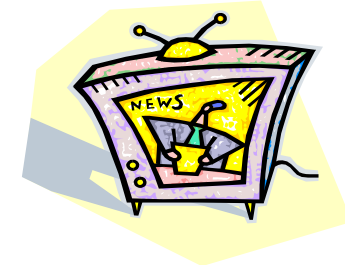


Response

- Timely
- Personal touch
- Professional
- Acknowledgment of wrongdoing if warranted and sanctions/retraining response
- Legal Review
- Closing the complaint



Media Issues



- Media: Press conferences, newspaper stories
 - Use their outlets to communicate with potential victims
- Public: Toll free phones, scripting, staffing for phones, web-site
- Communication Plan: Point of contact, employees, patients, business partners, public.



Media Issues cont.

- Costs?? Extra staffing, time to acquire addresses for notifications, postage
- Business Impact: Public/Patient inquiries, loss of trust, practice changes, new monitoring tools



Conduct Investigation – cont.

■ Follow-up:

- Controls implemented for vulnerabilities
- Documentation – summary, outcome, resolution
- Post-event monitoring
- Policy changes, education
- Lessons learned
- Fines, further legal action if warranted

Documentation

- Document investigation - incidents/breaches (Event Database)
 - Statement of problem
 - Actions taken
 - Resolution
 - Corrective / remedial actions
- Document Retention Requirements
 - HIPAA
 - State Law



Sanctions



A sanction policy and a process to apply appropriate sanctions against workforce members who fail to comply based upon policy and the relative severity of the violation.

- No Breach of Confidentiality/Information Security
- Unable to Determine Whether a Breach Occurred
- Policy Violation with Mitigating Circumstances
- Policy Violation without Reasonable Appearance of Inappropriate Access or Malicious Intent
- Policy Violation with Reasonable Appearance of Malicious Intent

Lessons Learned



- Well defined & documented policy and procedures
- Pre-established communication plan – Know who to inform, maintain relationships
- Workforce education: Users need to know who to call and what to do

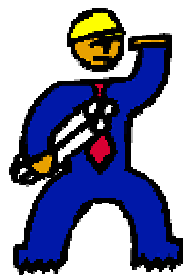


Lessons Learned - *Continued*

- Consistent operational security practices, e.g. logging, uniform configuration standards, managed devices, minimum device security requirements
- Data restore / recovery: Importance of testing those back-up tapes; know what worked and what didn't; storage safeguards

Lessons Learned - *Continued*

- Learn from past incidents: Evaluate your investigation/response process and update as often as needed.
- Follow up / implement change,
 - e.g. *Masking/removing SSN data from electronic forms and databases*



The Happy Ending

- **Through cooperative work with law enforcement and the media, our second little laptop, *Breach*, was found.**
- **After contact by the Feds, his IT orphanage underwent reorganization and he was adopted by an owner and operator of his own.**
- **His worms and viruses are gone.**
- **They gave him a new name: *Encrypted***
- **He and his organization lived happily ever after - (*as soon as the bad press died down.....*)**



Questions?