How Safe Is Your Mobile Information?

Issues and Safeguards for Mobile Devices

Dan Morrissey, **CHSP**
Catholic Health Initiatives
Fourteenth National HIPAA Summit
March 30, 2007

Agenda

- Mobile Information in the Real World
- Threats and Risks to Mobile Information
- Safeguards for Mobile Devices

Mobile Information in the Real World

What is happening out there today?

- **Proliferation of mobile devices and data**
- **Laptops, PDAs, Smart Phones, USB Memory Devices, Storage Cards, Blackberries, Converged Devices, Clinical Devices**

Headlines and Web Postings

- **130,000 former and current patients have been notified that a laptop with personal information was stolen…(2/7/07)**
- **A doctor's laptop was stolen from the Medical Center containing medical information of 22,000 patients. (2/14/07)**
- **Two laptop computers stolen from locked vehicle in the Hospital parking lot hold personally identifiable medical information and SSN of 2,500 patients. (2/16/07)**
- **A laptop with 7,800 uninsured patients' names, birth dates and Social Security numbers was stolen from the hospital… (2/29/07)**
- **Stolen laptop contains medical information on 21,600 health plan beneficiaries.**
- **Stolen laptop had medical claims data on 230,000 people**

Impact on Organizations

- Compromise of Corporate and/or Personal Confidential Information
- Public Image and Market Share
- Financial and Legal
- Compliance

Compliance

- HIPAA
- GLBA, and other Federal Regulations
- New State Regulations
- JCAHO Reviews and Accreditation

Real World Examples

- **Large Multi-State Health System**
  - Stolen Laptops and Backup Tapes
  - 365,000 Home Services Medical Records
  - Arrange and finance on-going credit monitoring
  - Pay for damaged credit ratings
  - Class Action lawsuit filed by former patient
  - Current and former patients and employees outraged
  - Cost Estimate: **$43,800,000**

Real World Examples

- **Federal Government Health System**
  - Laptop Stolen from data analyst's home
  - 26.5 Million records: ePHI and SSNs
  - Desktop Computer missing from subcontractor
  - 38,000 Records: Medical Claims, SSNs
  - Providing one year credit monitoring
  - Encrypting all laptops, revamped security training, enhanced authentication requirements

Real World Examples

- **National Healthcare Payer**
  - Laptop stolen from employee's car
  - 59,000 Members' personal information
  - Arrange and fund on-going credit monitoring
  - Now require all information on laptops be encrypted
  - Implemented new restrictions on use of USB devices
  - Conducted audit of all computers for compliance
  - Cost Estimate: **$8,142,000**

Future of Mobile Information

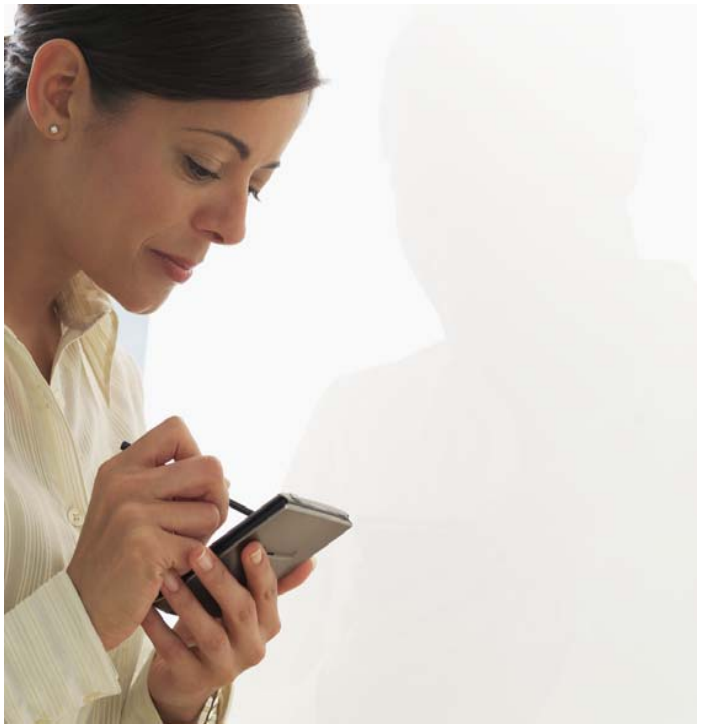
- Growing usage and reliance on mobile devices for network access, applications, e-mail, and internet.
- Greatly increased device data storage and capabilities, including audio and video recording, while physical size is decreasing.

Future of Mobile Information

- Advanced clinical mobile devices will become more common.
- Mobile devices can be adequately protected using a combination of technology, training, and effective polices and procedures.

Photo courtesy of GE Healthcare

Ownership, Support, and Controls



- Employee owned devices
- Software installation and configuration
- Technical support
- What happens when employee leaves?

Threats and Risks To Mobile Information

Threats and Risks to Mobile Information

- **Threats** - mobile devices being lost or stolen, or turned into “bricks”
- **Risks** - Unauthorized access, distribution, and use of confidential information
- **Risks** – potential patient care and safety issues resulting from inability to access medical records when required
- **Risks** - damage to proprietary networks

Threats and Risks to Mobile Information

- Technical
- Human
- Internet
- Physical - *especially because of size, portability, and physical availability*

Results of Threats Realized

- Unauthorized access and theft of proprietary information are the 2nd and 3rd most significant causes of information losses and accounted for over $62B in losses for 2005.
- Cost per lost account record: $138 (min) includes direct and indirect costs, and lost business cost (lost business is 90% from existing customers).

Results of Threats Realized

- **Confidential Information Compromised**
  - Personal or corporate / organizational
  - Identity theft is a growing national concern
  - Now driven by criminal activities for illegal gain
  - Consumer / Patient / Corporation at risk
  - Legal actions by individuals and groups

Results of Threats Realized

- If lost or stolen and access is not available when needed. (This can be critical in patient care and a potential patient safety issue.)
- Malicious activity can result in direct attack on the device or a denial of service attack. (Both results can also be critical in patient care and a potential patient safety issue.)

Results of Threats Realized

- Entry point to network that by-passes security perimeter protection can result in:
  - Unauthorized access to network
    - Compromise of confidential information
    - Malicious software or actions can create serious damage to network systems
  - Interception of communications (especially wireless)

Safeguards for Mobile Devices

Safeguards for Mobile Devices

- **Physical Protection**
  - Device lock
  - Theft prevention lock
  - Failed authentication automatic data wipe (after n attempts)
  - Do not leave devices unattended in plain view anywhere (car, office, airport, etc.)

Safeguards for Mobile Devices

- **Authentication to Device and Network**
  - Passwords
    - Strong – difficult to guess or crack
    - Changed frequently
    - Kept secret, not written
  - Biometrics
  - Smart Card
  - Policies enforcement via managed authentication system

Safeguards for Mobile Devices

- **Encryption**
  - Data at rest
    - Disk encryption, whole or part as required
    - Data base, configuration, software
    - Centralized encryption key backup and recovery
  - Data in transit
    - VPN
    - IPSec, SSL, S-HTTP
    - Secure FTP

Safeguards for Mobile Devices

- **Device Configuration**
  - Turn off certain capabilities not required for use
  - Implement all relevant security features available
  - Disable discoverable and connectable options (e.g. Bluetooth)
  - Do not store confidential information on devices unless necessary

Safeguards for Mobile Devices

- **Protection of the Device and Network**
  - Anti-virus at entry points: email, internet
  - Device Firewall
  - Integrity management systems can provide remote control of mobile devices to:
    - Detect unauthorized activities such as changes to system files (caused by virus or other malware)
    - Quarantine device and notify user and administrator
    - Clear data from device if lost or stolen

Safeguards for Mobile Devices

Enterprise Security Architecture

- Network
- Anti-virus
- Communications
- Monitoring – IDS / IDP
- Logging and Auditing

Recovery and Remediation

In the event of a security breach…

- Security Incident Response Procedures
  - Determine, assess, and mitigate damage
  - Ensure that legal is involved from start to end
  - Inform affected individuals and provide relief
  - Up front Public Relations
  - Implement relevant technical measures
  - Additional / improved education and training
  - Audit remediation results on regular basis

Recovery and Remediation

In the event of a security breach…

- Ensure that event cannot occur again (if possible)
- Review, revise, and re-establish effective security measures
- Obtain and secure relevant evidence for prosecution and /or disciplinary action
- Document the incident, the outcome, and new preventative measures implemented

Cost of Protection vs. Cost of Breach

- **Recovery / Resolution**
  - $120 (min) per year per account direct cost for one year of credit monitoring service
  - Civil / Class Action Lawsuit
  - Negative Publicity
  - Lost Revenue
  - Compare to less than $20 per account to implement adequate security controls

Successful Mobile Data Security

- Establish, implement, enforce and audit effective Security Policies and Procedures for mobile devices:
  - Administrative
  - Technical
  - Physical
  - Training
  - Accountability and Sanctions

Final Considerations

- Stay out of the news and off the web!
- Effects of a breach will reach far beyond the specifics of the incident.
- Potential long term consequences.
- Competitive Health Care environment, especially in the community.

Questions and Discussion

Thank You!

For additional information contact

Dan Morrissey

danmorrissey@catholichealth.net