Security & Privacy in mHealth

Khaled El Emam, CHEO RI & uOttawa

Breach Statistics

- 52% of data losses in healthcare were the result of loss or theft of mobile devices
  (Ponemon Institute, 2011)
- 38% of all large data breaches (>500 records) were caused by theft or loss of mobile devices (laptops and portable electronic devices)
  (Health and Human Services, for 2010)
- 31% of all large data breaches (>500 records) were caused by theft or loss of mobile devices (laptops and portable electronic devices)
  (Health and Human Services, for 2009)
- 29% of breaches in the medical/healthcare sector involved mobile devices and affected 51.8% of all records (~2m)
  (Identity Theft Resource Center, 2011)

Breach Costs (in US$)

- The range of costs for a data breach in the healthcare sector per record have been estimated to be $200-$300 (multiple studies – all US)
- These cover all costs, include reporting, legal costs, and penalties
- The most credible estimate of the % of healthcare providers that had a reportable breach in the last year is 19% (based on HIMSS survey)

Risk Exposure - I

- Risk Exposure is defined as:
  Loss x Probability of Event
- Risk exposure can be used evaluate and compare risks from alternate policies
- Approximately 1/3 of breaches involve mobile devices
- The overall probability of mobile device involvement given that a breach has occurred is ~6.3%
- Now we can compute the risk exposure from a mobile device breach

Risk Exposure - II

- The risk exposure from a loss of 100,000 records is $1.254m and the risk exposure from a breach involving 1000 records is $12,540
- Investments in protecting the data on mobile devices that eliminate that risk exposure can be justified up to that value – and this will depend on the size of the institution and the data sets that it handles

Risk Exposure - III

- Some risk mitigation strategies have fixed costs, which put smaller institutions at a disadvantage (e.g., writing standard operating procedures and training)
- This makes a strong case for smaller institutions to pool their resources when implementing risk mitigation strategies

Risk Mitigation - I

- Provide remote access to PHI from mobile devices – avoid storage of PHI on the device itself if possible
- Secure communications to access remote data
- Automatic locking of devices (and enforced)
- Only store/transport de-identified data on the device itself
- Remotely delete data from lost or stolen devices

Risk Mitigation - I I

- Whole disk encryption of all mobile devices (file or folder encryption has some risks associated with it)
- Remove or securely wipe all data from devices before disposal
- Enable audit trails that will track access to PHI from mobile devices
- Training/education of users about good privacy and security practices (and refresher training on a regular basis)

Risk Mitigation - III

- Audit devices to ensure compliance (especially if users have the option of disabling certain protections)
- Have formal agreements with users regarding the use of mobile devices to access patient data
- Ensure that any loss or theft is reported immediately, and have a process in place to manage breaches (step 1: limit the damage)

Wrinkles

- Use of personal devices:
  - Users do not want to carry multiple devices with them for personal and professional uses
  - Freedom of Information requests for information on devices that hold the user's personal data
  - Users want to download apps to their personal devices
  - Users may share passwords on personal devices

More Wrinkles

- Devices or apps used by patients to provide data (e.g., in the context of PROs in clinical research)
- Modes of communication vary by age of patient
- Trusting cloud service providers that may hold data

Things That You May Not Know

- Backdoors (known or computable root passwords, bypass mechanisms used for testing, forensic tools, hacks)
- Apps that deliberately (malware) or inadvertently leak information
- Electronic eavesdropping (keylogging, enabling mic and camera)
- Tracking (e.g., WiFi tracking)

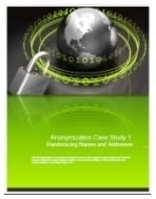
What we are doing about it

- For data collection, secure multi-party computation protocols allow the performance of mathematical operations on encrypted data:
  - data encrypted at the point of collection
  - Cloud apps can provide statistics, benchmarking and feedback without having to trust the cloud provider
  - for example, a secure survey platform

kelemam@uottawa.ca

www.ehealthinformation.ca

www.ehealthinformation.ca/knowledgebase




Electronic Health Information Laboratory