Security Issues in Healthcare Wireless Applications

Claudia Tessier RHIA

President, mHealth Initiative

Author: *Management and Security of Health Information on Mobile Devices*, AHIMA 2010

HIPAA Summit
February 4, 2010

Copyright mHealth Initiative 2010

Mobile Phone Adoption

- **Worldwide mobile subscriber base >4 billion at end of 2009**
- *Compare that to:*
  - Landline phones: 1.2 billion
  - TV sets in use: 1.4 billion
  - Registered automobiles: 850 million
  - People using PCs: 950 million
  - Access to internet: 1.3 billion

Mobile Phones in Healthcare

- **Thousands of devices** including
  - Apple iPhone, Droid, Blackberry Curve and
  - Storm, HTC Touch HD and HTC Pro, Palm, Samsung, Sony Ericson, and more
- Estimated **5000 mHealth apps** over range of devices
  - Over 3700 clinical
  - Over 1000 consumer
  - **But** not all apps available on all phones

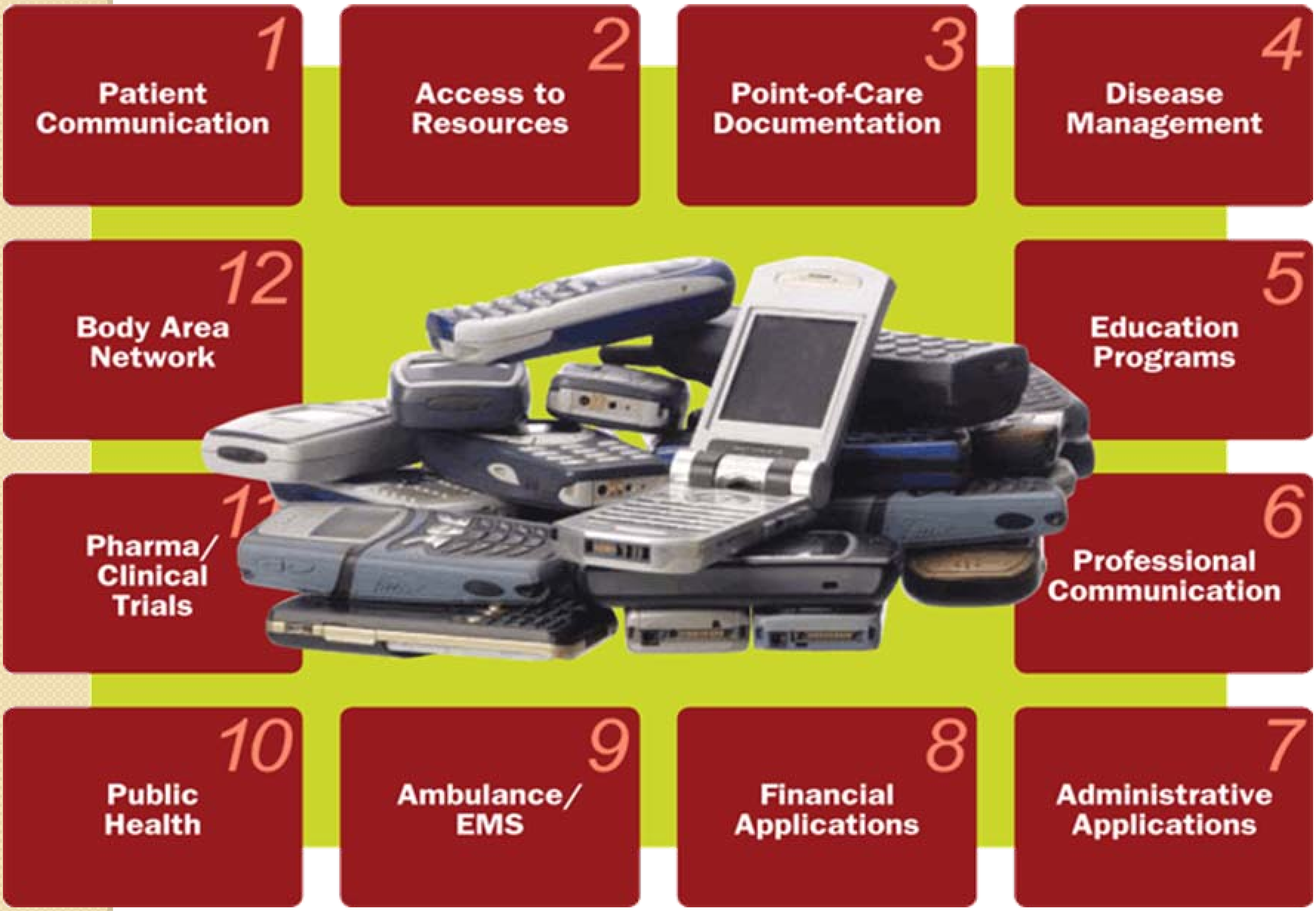
How does mHealth differ from eHealth?

- eHealth focuses on technologies
- mHealth focuses on behavioral and structural change enabled by **new communication methods**

The Vision for mHealth

- Consumers and Patients use mDevices to
  - Research and manage health issues
  - Communicate with wellness and care providers
    - From administrative to reporting and questioning
    - From tracking to monitoring and more
  - Communicate with disease-specific groups
  - Communicate with payers

mHealth 12 Application Clusters



1 Patient Communication

2 Access to Resources

3 Point-of-Care Documentation

4 Disease Management

5 Education Programs

6 Professional Communication

7 Administrative Applications

8 Financial Applications

9 Ambulance/ EMS

10 Public Health

11 Pharma/ Clinical Trials

12 Body Area Network

What this means for healthcare

- mHealth will have a dramatic effect
  - Care process to move from Doctor’s office to “health space”
    - Participants: patients, wellness providers and care providers
    - **Leading to participatory health**
- From occasional visit to continuing communication
- Scientific body of medicine
  - From books to apps

MOBILE SYSTEMS ARE ENABLERS

mHealth Benefits

- Savings ($ billions)
  - Proven in communication-based disease management
  - Savings through communication
  - Less need for visits (reimbursement reform needed)
- Better quality of care
- Benefits to clinicians

The mHealth Revolution and Health Information Management

- Clinicians’ and patients’ mHealth adoption is ahead of executives and department heads
- Potential benefits outweigh the risks and “hassles” of mHealth integration
- Adoption of mDevices and apps requires
  - Institutional strategy
  - Policies and procedures
  - Cooperation and communication among C-level execs, clinicians health information managers, IT and IS professionals, legal counsel, bioengineering…

Organizational Strategies for Implementing mHealth

- Top management must be alert to
  - New developments in mHealth and participatory health
  - Need for new systems that allow continuous communication between patients and providers
  - What is needed to create such systems
  - How administrative and clinical workflow will be affected

Organizational Strategies for Implementing mHealth

- Educate all stakeholders
  - New system requirements
  - Impact on workflow, administrative and clinical
  - Evolving roles in competitive healthcare market of the future
- Extent and type of current use of mDevices in organization
  - Identification of “no cell phone” areas
  - Potential for extending open areas for use by clinicians, staff, patients, and visitors

Organizational Strategies of Implementing mHealth

- Step-by-step implementation plan to facilitate participatory health and new communication systems
- Compliance with federal and state laws and regulations and with institutional policies and procedures re PHI.

Designing a Wireless Architecture for Healthcare Institutions

- Healthcare apps must be
  - Clinical grade, robust
- System: “always on” reliability and performance – 24-hour monitor
- **Protect against security threats**
- **Automated compliance reporting for HIPAA**
- Evaluate and compare in-house vs contracted services

Outdated technologies and merging legacy systems

- mDevice capabilities exploding
- mDevices are quickly outdated
- Integration into legacy EMR systems is a problem
  - Most EMR systems proprietary
  - Some EMR systems have options for mDevice integration
  - Will mean transitioning from messaging standards to Internet XML

Clinical grade mHealth Requirements

- 24/7 availability
- **Integrated security**
  - Dependability, information privacy, integrity and regulatory compliance
  - Only authenticated logged access by authorized persons
  - Networkwide layers defense model
- Quality of service (QofS) and guaranteed service level agreements – consistent, trusted, solution risk-taking, measured traffic

Clinical Grade mHealth Requirements – cont’d

- Pervasive coverage: facility and beyond
- Seamless mobility –accommodate any mDevice
- Transaction integrity
- Nonrepudiation
- Ability to evolve
- Ease of use
- Workflow integration

mDevice Communications

- Volume and types of communications via mDevice
    - Voice is least difficult but will diminish in volume to be replaced by **eCommunications**
        - Texting
        - Instant messaging
        - Fax via cell
        - Social media – Facebook
        - Twitter
        - PHRs on mDevices

mCommunication Issues

- Encryption
  - All messages or only those with clinical content
- Clinic-provided email accounts (instant message or blogs)?
    - Offer to patients on facility’s server?
    - Inside or outside the firewall?
- Outcomes evaluation
  - Evaluate efficacy and usefulness
  - Cost-benefit analysis, patient satisfaction, provider satisfaction, clinical outcomes

Texting

- Initially avoided in healthcare and continues to be in some environments
- Most widely used for administrative communications which don't require security of PHI – appt reminders, messages to call for lab results, mass mailings., etc.
- Becoming more accepted for some PHI messages
  - Patient wants/expects it
  - Facilitates communication and compliance, especially for disease management

Texting issues

- Security
  - But patients may expect/want it
  - Opt-in or opt-out?
- Clarity and completeness
  - 160 character limit
  - Abbreviations/acronyms/short forms may be confusing or misleading
- Keyboarding frustrations
  - Keyboard size, touch-screen keyboards, numeric keyboards (original telephone keypad)

Policy Considerations re texting, email, instant messaging, etc.

- Triage
  - Who triages the communications and what is response time?
- Administrative issues
  - How to integrate messages into patients' records?
  - By whom?

Policy Considerations re texting, email, instant messaging, etc.

- Categorization and direction
  - By provider, each with own account?
  - By category (e.g. billing, clinical, scheduling)
  - Both?
- Access to providers
  - Will the provider’s electronic address be released to all patients or selectively?

Policy Considerations re texting, email, instant messaging, etc.

- Archiving and backup
  - Whose server – the provider's, the institution's, or both?
  - Schedule archiving, clearing, indexing for storage and retrieval
- Forbidden topics
  - Allow topics such as HIV and behavioral conditions to be addressed
    - Easy answer: NO!!!
    - But what if patient requests, consents, demands?

Policy Considerations re texting, email, instant messaging, etc.

- Selective confidentiality
  - Can patients opt to exclude certain e- or m-communication content from their records.
  - Is a secure repository required for such exclusions?
  - Ares such exclusions allowed?

PHRs on mDevices and Health Information Management

- Adoption of PHRs is expanding
- Integration of PHRs into mDevice applications is growing
- Traditional records (paper and electronic) must integrate mDevice-based PHRs and their related applications, including ODLs

What are ODLs?

- Observations of daily living
- Information that is collected and reported by the patient – sleep, diet, exercise, mood, adherence to meds, etc.
- ODLs allow both the patient and the provider to identify and respond to trends, incidents, factors that might not otherwise be recognized if patient info is collected only at time of infrequent encounters

Confidentiality, Security, Data Protection Concerns re PHRs on mDevices

- Encryption required
- Must identify anyone accessing the data
- Safe and secure host system
- Policies to guide overall system

Confidentiality, Security, Data Protection Concerns re PHRs

- Questions
  - Where does the data reside?
    - With primary healthcare provider?
    - Independent company
    - PHR provider (e.g., Microsoft HealthVault or Google Health)
    - With patient?
  - Who decides?
  - Who owns the data?

Authentication Concerns re PHRs

- Physicians (some) don’t trust PHR information if not authenticated by another physician.
- Don’t want data “tampered with” by the patient
- PHRs need sections where patients can enter data and comments
- PHRs also need safeguarded sections where authenticated provider information is displayed

Camera function on mDevices

- Easy picture-taking, swift transmission, easy storage and organizations
- Patients: wounds, rashes, injuries, etc.
- Clinicians: receive photos and other clinical images (x-rays, EKG readings) on cell phones for initial assessment.
- **Threats to confidentiality**
- Restrictions required, enforcement difficult
- Education, guidelines needed
- Sanctions if misused

Selecting mDevices

- Many types: smartphones, designer phones, multimedia phones, touch screens, PDAs, tablets, more…
- One size does not fit all
  - Users want to pick their own
  - Institution wants consistency and compatibility
- How to fit multiple types/styles with range of capabilities into institution’s operations?
- And assure security with all of them?

Risk management of mDevice security

- Increased connectivity + large number of devices and applications
= increased risk
- Value of content and value of devices both at risk

Risk management issues of mDevice security

- Malware
  - Restrict certain applications from installation
  - Restrict port usage to approved ports (e.g. patient portal to PHR)
  - Enable only authorized input/output capabilities
- Blurred distinction between enterprise devices and consumer devices
- Competing platforms
  - No OS is dominant
  - Must manage multiple networks as well as multiple devices as well as multiple applications

Protection against Data Loss

- Secure passwords and timeouts
- Automatic locking of devices after specified period of time
- Encryption of data at rest and in transit
- Remotely wipe device if stolen or lost
- Synchronization with institution restricted to compliant devices only

Data Safeguarding Solutions

- 24/7 security monitoring
  - Vulnerability and breach detection and prevention
- HIPAA, ARRA, state and other regulations as well as institutional policies and procedures
- Extend already existing PHI security measures to mDevices:
  - Viruses, malware, hackers, RFID, applications, Bluetooth, unapproved downloading and storage of PHI, and unsecured networks

Safeguarding Data

- Device tracking and loss prevention
  - GPS location systems
    - Must advise users (if you know where my device is, you know where I am)
    - Document with formal agreement
  - Device tracking for equipment, supplies, paper medical records, and patient tracking (Alzheimer's patients, for example
- Clearing the memory in event mDevice is lost or stolen

Breaches involving PHI

- Policies and procedures to address breaches by covered entity as well as its business associates – extend to mDevices and mApps
- Wireless communications add a layer to these responsibilities not yet fully adjusted to in terms of EMRs
- Must identify and address
  - Systems that store data
  - Response team
  - Federal and state requirements
  - Contracts with third parties
  - Data breach insurance coverage

Health Information Management and mDevices requires

- Expanding emphasis on recordkeeping to managing communications to/from patients
- Increased communication and cooperation among C-level execs, IT and IS, legal counsel, biomedical engineers, and clinicians
- More involvement of and with patients – to educate, to meet expectations, to provide better administrative as well as clinical services – while protecting PHI

For more information….

Management and Security of Health Information on Mobile Devices –
to be published this month by AHIMA (American Health Information Management Association)

AND…

Plan now for mHealth Initiative's next

mHealth Networking Conference

September 8-9, 2010

San Diego, CA

www.mobih.org

Thank you!

- Claudia Tessier RHIA
- President, mHealth Initiative
- 617-816-7513
- claudia@mobih.org
- www.mobih.org