mHealth and BYOD

Susan Salpeter
Zurich Insurance
September 12, 2014

Agenda

- What is it, why use it, who uses it
- Risks/Concerns
  - Regulatory
  - Quality of device
  - Users
  - Data dump
  - Security
  - Impact on outcomes
- BYOD

Timeline of Healthcare Communication

ZURICH

- 20th century (but some are still here)
- Today (but not everyone)
- Future – sooner than we'd think

3

mHealth

ZURICH

- Use of mobile technology to boost access to health information, distribute health care services and provide diagnostic services, often to remote communities that may not otherwise have access to regular health care
- The provision of health-related services using mobile communication technology
- The World Health Organization - medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices

Why mHealth

ZURICH

- Ability to provide health care to underserved population – nationally and globally
  - Mother Baby 7 day mCheck – used in Mysore District, India to identify signs of infant and mother mortality risk
- Ability to provide coaching and monitoring services to patients
- 6 billion people have access to mobile phones – excellent way to reach people
- Global mHealth market expected to be worth between 30 and 60 billion by 2015

5

Global mHealth

ZURICH

- In developing countries:
  - Average doctor:patient ratio is 1:250,000
  - Over 80% of world-wide mobile phone subscriptions

6

Usage - Patients

- 2015 - 500 million smartphone users worldwide will be using a health care application
- 2018 - 50 percent of the more than 3.4 billion smartphone and tablet users will have downloaded mobile health applications
- > 40 000 medical applications available for download in U.S.

Percentage of Downloads By Category: iPhone & Android

- Weight loss – 39%
- Exercise – 21%
- Women's health – 8%
- Sleep and meditation – 6%
- Pregnancy – 6%
- Tools and instruments – 5%
- Other – 14%

2013 - Verasoni Worldwide
http://verasoni.com/mobile-health-applications-2012-study/

Usage – Providers (2013 HIMSS survey)

ZURICH

- Almost 83 % of the participating doctors had downloaded medical apps
- > 33% of MDs, 75% of RNs use medical apps on smartphones daily for work purposes
- 35% of hospitals offer patient apps (portals, tele-health, remote monitoring)
- Providers use technology to:
  - 69% view patient information
  - 65% access web-based repositories, services for health care information
  - Communication and telemedicine functions

– HIMSS report, 2014

– http://www.himssanalytics.org/research/AssetDetail.aspx?pubid=82144&tid=127

Booz&co – mHealth usage

ZURICH

- Clinicians –
  - 250% more likely to own a tablet than any other consumers
  - 66% use for medical purposes
  - More than half say expedite decision making
  - 40% say decrease administrative time
  - 39% of MDs communicate with patients via e-mail
  - 86% of clinicians use smart phone in practice areas
- Consumers
  - 78% of consumers interested in m-Health solutions
  - 13% of consumers have accessed, stored or transmitted personal health info or records in past year, 48% are interested in doing so.
  - 52% are comfortable with consulting with their MD through a video connection.

http://ihealthtran.com/wordpress/2014/01/infographic-m-health-physician-use-of-mobile-technology/

Types of Devices

- Monitors – in hospital
  - Airstrip OB
  - Wireless monitoring of patients in the hospital
- Monitors - at home
  - Home vital signs
  - EKG, left atrial pressure (include implantable devices)
- Diagnostic
  - Ultrasound
  - Blood glucose
  - Breathalyzer

Types of Devices

- Coaching –
  - Diabetes care
  - Diet/nutrition
  - Fitness
- Treatment
  - Telehealth using mobile devices
  - Wii fitness
- Aging in place solutions
  - Wearable biosensors
  - Motion sensors
  - "smart" pill bottles
- Future devices
  - Google lens
  - Rehabilitative motion sensors

Mobile Health in 2024

ZURICH

- Contact lens takes picture of retina to ID early symptoms of diabetic retinopathy
- Refrigerator monitors drinks consumed, vitamin consumption, calories/sugar consumption
- Artificial pancreas – monitors blood sugar and injects insulin as needed
- Clothes – smart fibers sense rash or skin condition appearing signaling possible onset of diseases

Mobile Health in 2024

ZURICH

- Thermometer patch – detect precise temperature changes, tracks blood flow
- Shoes and socks that track movements of feet and detect when not moving
- Diapers – monitor sleeping patterns and body temperature
- Toilet – measures frequency and amount of urine, analyze glucose levels, dehydration, infection
- Continuous data collection and instant reporting of fitness – incentivize good behavior

Does it work?

ZURICH

- Too soon to conclude - little research and small studies
  - Patient Portals – "Evidence that patient portals improve health outcomes, cost, or utilization is insufficient. " (Annals of Internal Medicine, 2013)
  - Texting diabetes patients - program sends health-behavior–related text messages to type 1 and type 2 diabetes patients. Sent reminders and reinforced self-care behaviors. Resulted in improved glycemic control and lowered costs (Health Affairs, 2014)

ZURICH

RISKS AND CONCERNS

Are these devices regulated?

ZURICH

- FDA guidance issued September, 2013
  - "Intends to exercise enforcement discretion…for the majority of mobile apps as they pose minimal risk to consumers"
  - Focus on a subset that present a greater risk to patients if don't work as intended.

17

FDA Regulation – which apps?

ZURICH

- Those intended to be used as an accessory to a regulated medical device
  - Allow provider to make a specific diagnosis by viewing a medical image
  - Transform a mobile platform into a regulated medical device (application that turns a smartphone into an ECG machine)
- Look at intended use – i.e., LED
  - Intended to illuminate objects generally – not a device
  - Promoted as light source to examine patients – a device
- Assessed using same standards and approach applied to medical devices

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

18

Does HIPAA apply to Mobile Medical Apps?

- It depends….
  - Any mobile medical app that permits physicians and patients to communicate about protected health information – covered
  - App used solely by an individual is not covered by HIPAA
  - If information transmitted to covered entity (physician, health plan, etc.) information falls under HIPAA

Risks – Controlling Apps

- What are your providers downloading/developing?
  - Quality of app
  - Quality of data/information within app
  - Non-standardized
  - Rapid generational changes in devices/platforms

Risks - Distractions

- Interruptions for non-work-related reasons
- Clinicians create their own interruptions during patient care
  - Nurse checking airfares during surgery
  - Neurosurgeon using a wireless headset to make personal calls during surgery
- Perfusionist study –
  - 50% texted during heart-lung bypass procedures
  - 15% accessed the Internet
  - 3% visited social networking sites during procedures

21

Risks - Distractions

- Resident physician using her smartphone to enter an order to stop anticoagulation therapy in the CPOE system.
- Before completing, resident received a personal text message.
- Responded to the personal message by text
- Never completed the order
- Anticoagulation therapy continued unnoticed for several days
- Patient developed conditions that necessitated emergency open-heart surgery

22

Risks – Display limitations

- Small display limits the utility of the device for interacting with many systems
- EHR or CPOE system designed for desktop or laptop computers may not display information well on smaller screen
- Image quality may suffer – resolution, room brightness

Risks - Texts

- 75% use smartphones to send job-related messages use text message
- TJC – unacceptable to text orders:
  - Can't identify person sending text
  - Original message can't be kept as validation of what was entered
  - Accuracy of texting OMG MSO4 = Magnesium or Morphine?
- DHHS:

  "Your organization may approve texting after performing a risk analysis or implementing a third--party messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved mobile devices."

Risks – Security and Privacy - Cameras

- Appropriate use of cameras
  - Confidentiality
  - Security in sending images
  - Quality of image – sender and receiver
  - Assurance that image is received

Risks – Malware/Viruses

- Is mobile more vulnerable than "fixed"?
  - Wireless technology – if unsecured network
  - Device development – app makers "traditional" approach more about innovation than about safety
- Infected devices can stop working or perform unpredictably
- Transmit incorrect data

Attack Surface: Healthcare and Public Health Sector

ZURICH

- DHS Report raised concerns regarding:
  - Introduction of spyware and other malware
  - Theft of patient information
  - Loss of test results or treatment records
- Sci-FI?
  - Implanted insulin pump can be remotely shut off or altered without the user's knowledge
- Some strategies
  - VA used Virtual LAN to create a separate network for the devices

http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf

DHS - Recommendations

ZURICH

- **Purchase** only devices with good security features that can be configured safely on networks.
- **Require** vendor support for ongoing firmware, patch, and antivirus updates.
- **Operate** - external-facing firewalls, network monitoring techniques, intrusion detection techniques and internal network segmentation (as practical)
- **Configure** - access control
- **Establish** strict policies for connecting any networked devices, particularly wireless devices, to health information networks

DHS - Recommendations

- **Establish** policies to maintain, review and audit network configurations as routine activities when the Medical IT network is changed
- **Use –** provide least privilege principle – only give access to what is specifically needed
- **Implement** - patch and software upgrade policies for medical IT networks that contain regulated medical devices
- **Secure** communications channels, particularly wireless ones, through the use of encryption and authentication at both ends of a communication channel
- **Establish and enforce** password policies to protect patient information

29

Identifiers

- Touchscreen phones know it's you from taps and swipes
- Android phone – pattern based
- Analyze veins in palms
- Voice recognition
- Iris Scan

30

Risks - Unusual

- Charge a mobile device using outlet for essential equipment
- Tripping hazards
- Overload WiFi Network
- Infection-causing pathogens on the surfaces of cell phones
- Electromagnetic Interference

Concerns – Too much data? ONC Report

"providers are concerned about possibly being overwhelmed with data from patients and the staff time required to process it. Patients, meanwhile, are concerned about whether their doctors will actually see the information they submit."

http://www.healthit.gov/sites/default/files/pghd_brief_final122013.pdf

Concerns – Too much data?

ZURICH

- Data from non-providers
  - Reporting of monitoring
  - E-mails
  - Patient health diaries/other information
- How often is it transmitted?
- Who is reviewing – and assessing the information
- Who is responding and acting on the information
- How is this being documented
- How is the information being integrated into health record

Where does it go?

ZURICH

- Lack of integration between mobile and EHR
- MD Survey
  - 25% said 75% of info in mobiles integrated into EHR
  - 27% said <25% of info integrated
  - 22% - none integrated
- Information from remote monitoring generating alerts in EMR and clinical systems
  - 44% get message via text
  - 41% get messages via e-mail

Reimbursement

- There is no proven model for reimbursement of mobile health apps
- Is physician compensated for reviewing alerts and patients' data?
- Is organization compensated for these activities?

SECURITY AND PRIVACY

5 steps to manage mobile devices used by health care providers

- **Decide** – will mobile devices be used to access, receive, transmit, or store patients' health information or used as part of your organization's internal networks or systems
- **Assess** how mobile devices affect the risks to the health information your organization holds
- **Identify** mobile device risk management strategy, including privacy and security safeguards
- **Develop, Document, and Implement** mobile device policies and procedures to safeguard health information
- **Train** on mobile device privacy and security awareness and training for providers and professionals

HealthIT.gov

37

Develop, document, and implement

- **Mobile Device Management**
  - Identify all the mobile devices being used
  - Track
  - Assign responsibility to check all mobile devices used for remote access, to determine if selected security/configuration settings are enabled
  - Develop schedule for review and audit of the mobile

HealthIT.gov

38

Develop, document, and implement What to consider

ZURICH

- **Restrictions on Mobile Device Use**
  - May want to restrict how providers and professionals can use mobile devices
    - Can they access internal networks or systems, such as an EHR
    - Restrictions on use when outside the organization?
    - Can they take their mobile devices home?
    - Should the organization allow texting or emailing of health information?

HealthIT.gov

39

Develop, document, and implement What to consider

ZURICH

- **Information Storage on Mobile Devices**
  - Are there restrictions on the type of information providers and professionals can store on mobile devices?
    - If so, where and for how long should the data be stored?
  - Are providers and professionals allowed to download mobile applications to mobile devices? If so, what type(s) of applications are approved?
- **Security/Configuration Settings for Mobile Devices**
  - Will you institute standard configuration and technical controls used to access internal networks or systems, such as an EHR?

HealthIT.gov

40

Develop, document, and implement What to consider

- **Misuse of Mobile Devices**
  - Written procedures for addressing misuse of mobile devices?
- **Recovery/Deactivation of Mobile Devices**
  - Procedures to wipe or disable a stolen or lost mobile device?
  - Procedure to recover mobile devices when employment or association with the organization ends?
- **Mobile Device Training**
  - Develop training for workforce on policies and procedures
  - How do you hold its workforce accountable for non-compliance?

HealthIT.gov

41

How Can You Protect and Secure Health Information When Using a Mobile Device? HealthIT.gov

- Use a password or other user authentication
- Install and enable encryption
- Install and activate remote wiping and/or remote disabling
- Disable and do not install or use file sharing applications
- Install and enable a firewall
- Install and enable security software

http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device

42

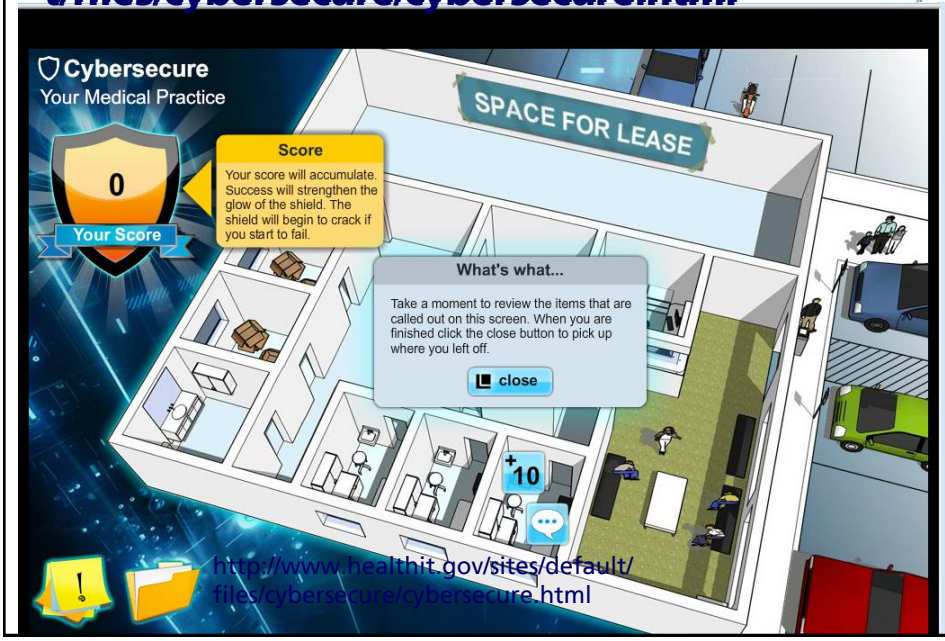
How Can You Protect and Secure Health Information When Using a Mobile Device? HealthIT.gov

- Keep your security software up to date
- Research mobile applications (apps) before downloading
- Maintain physical control
- Use adequate security to send or receive health information over public Wi-Fi networks
- Delete all stored health information before discarding or reusing the mobile device

http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device

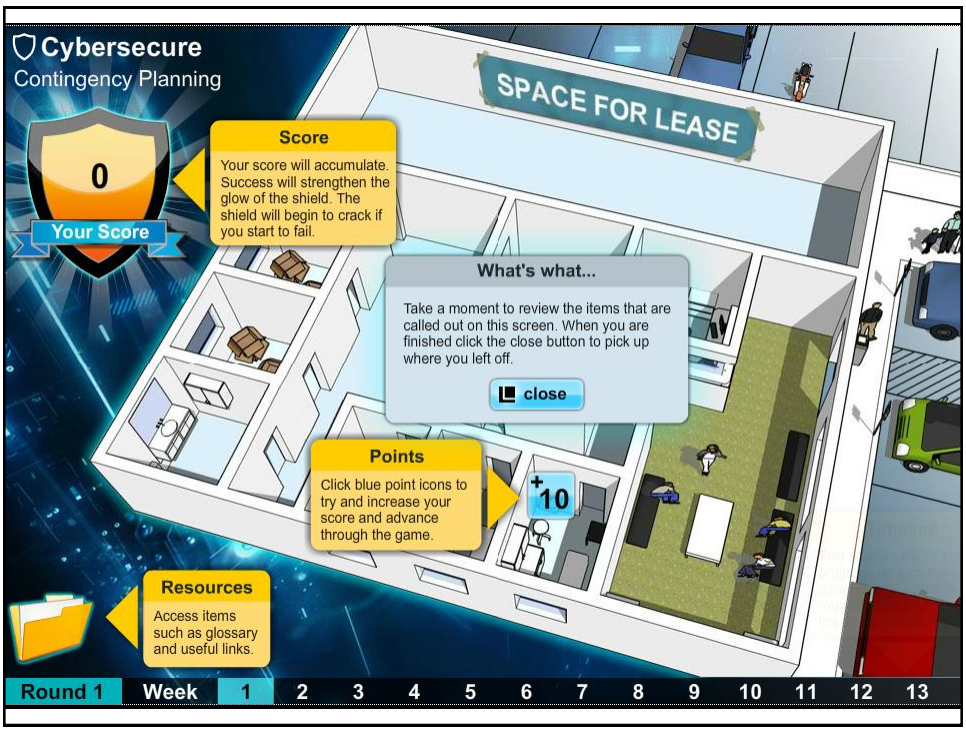
43

http://www.healthit.gov/sites/default/files/cybersecure/cybersecure.html



ZURICH

http://www.healthit.gov/sites/default/files/cybersecure/c...
http://www.healthit.gov/sites/default/files/cybersecure/cybersecure.html



BRING YOUR OWN DEVICE

BYOD

- Bring your own device or BYOD – allow staff to use their own smartphones or devices within the healthcare facility for work-related activities
  - Employer provides but lets staff use for personal work
  - Staff provides
  - Hybrid –
    - One group allowed to BYOD, one not
    - Limited options for what is supported

Why BYOD?

- Staff/user satisfaction – easy to transition between work and personal
- Rapid technology advances – don't want to wait for employer to provide the newest version of a device
- Increased mobility/working remotely
- Cost Savings

Should you implement?

- Should you allow people to use personal devices within the organization?
- Should they be able to connect to the organization's internal network or system either remotely or on site?
- Different implementation schemes
- Provide organization-supported devices (greater control)

BYOD – what can you access?

ZURICH

- Restrictions on which devices can be used
  - Providing access to only supported devices
  - Providing access to limited information/systems
- Containerization or "sandboxing"
  - Build an environment within an environment on protected devices
  - Create a secure container (or sandbox) for business data
  - Wall off that container from the rest of the device's operating system
    - prevents the export of data outside of the container
    - can encrypt data stored within the container

BYOD – what can you access?

ZURICH

- Thin-client configuration –
  - Patient data can't be stored locally on device
  - Device operates as a terminal
  - Authorized users log in and access information stored on a server
  - Lowers risk of loss of sensitive data

Documenting a BYOD Relationship

ZURICH

- Written contract to include:
- Types of information that may be stored, processed or transmitted
- Financial responsibility borne by users and the organization for the purchase, maintenance and replacement of devices
- Level of technical support (if any) the organization will provide
- security controls the organization will deploy on the user's device
- Any limitations in functionality that the user will experience
- User's agreement
  - To surrender the device to IT if required
  - Company may remotely lock or wipe the device in the event it is lost or stolen, or if the user leaves the organization
  - Remote wiping may remove personal information from the device

Mobile Device Management: Not What it Used to Be.. (CDW 2014)

BYOD – Other Considerations

ZURICH

- Phone upgrades – must be reported
- Phone no longer being used – old devices must be adequately secured and checked before being donated or disposed of.
- Support considerations:
  - Non-Windows platforms may not be compatible with standard healthcare apps already in use
- Develop ability to identify those who by-pass control
- Restrict cloud storage capability
- Consider partnering with vendor to provide mobile device management solutions

Disclaimer

The information in this publication and presentation was compiled by The Zurich Services Corporation from sources believed to be reliable. Further, all sample policies and procedures herein should serve as a guideline which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and presentation and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich Services Corporation reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication and presentation is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.

55

Additional Resources and Information Sources

- Fierce Healthcare IT - www.fiercehealthit.com
- Fierce Healthcare Mobile – ww.fiercemobilehealthcare. com
- CDW: http://webobjects.cdw.com/webobjects/media/pdf/108281-WP-Mobile-Device-Mgt.pdf?cm_ven=OnlineAds&cm_cat=Engagement&cm_pla=147710-Healthcare-Lenovo_ZZ&cm_ite=Healthcare_Flash_HIMSS
- Health and Human Services Resources - http://www.healthit.gov
  - http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device
  - Training Sites
    - http://www.healthit.gov/sites/default/files/cybersecure/cybersecure.htm
    - http://www.healthit.gov/sites/default/files/CyberSecure_103_FINAL/index.html

56

ZURICH

- HIMSS – www.himss.org
  - Mobile device survey – www.himss.org/mobile-health-survey
- HIMSS mHIMSS roadmap - http://www.himss.org/mobilehealthit/roadmap

- http://allthingsd.com/20130703/house-call-five-smartphone-accessories-that-help-monitor-your-health