SECURITY AND PRIVACY: MOBILE MEDICAL APPLICATIONS

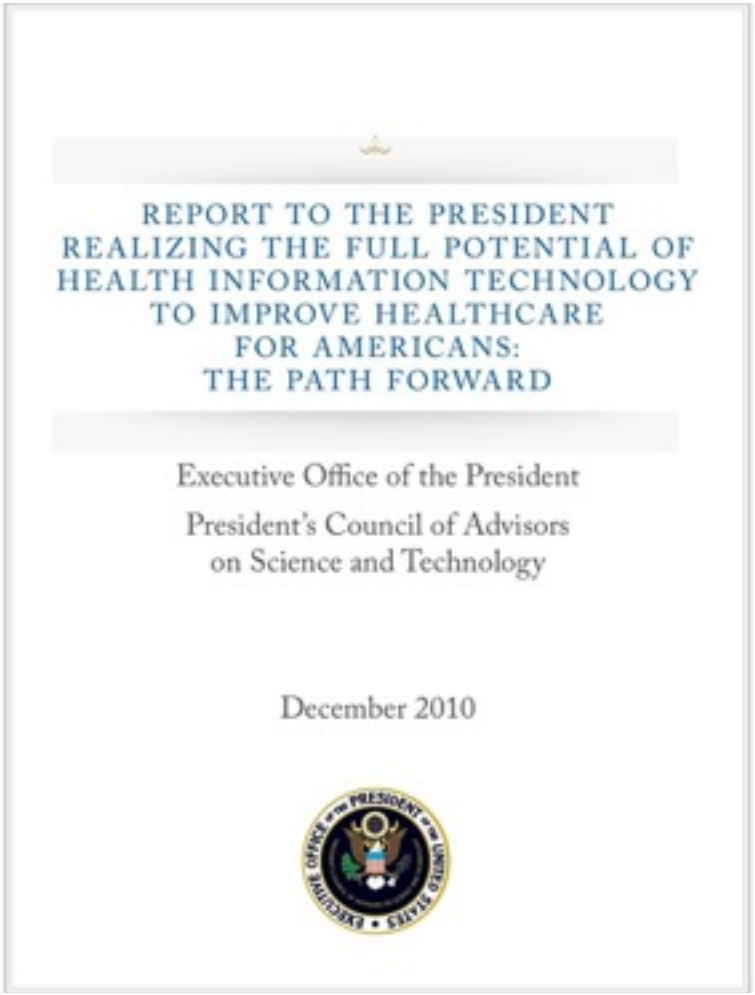
David Kotz, Dartmouth College

National Drug Abuse Treatment Clinical Trials Network Health Care Data Science Task Force Webinar

January 26, 2016

Healthcare IT essential to the U.S.

- Healthcare is a major part of our economy (18% GDP)
- I.T. has the potential to improve quality and reduce cost of healthcare
- Mobile & cloud technology is being deployed for health and wellness
- Security and privacy are essential to attain the quality and trust of patients and clinicians alike
- Fundamental research challenges remain!


REPORT TO THE PRESIDENT
REALIZING THE FULL POTENTIAL OF
HEALTH INFORMATION TECHNOLOGY
TO IMPROVE HEALTHCARE
FOR AMERICANS:
THE PATH FORWARD

Executive Office of the President
President's Council of Advisors
on Science and Technology

December 2010

Five trends in Healthcare IT
– and their implications for security & privacy

- Shifting locus of care
  - Healthcare delivered through small clinics, elder-care centers, or the home
  - Patients and clinical staff move among hospital, clinic, and residence
  - Distributed and remote monitoring, supported by cloud services

Five trends in Healthcare IT – and their implications for security & privacy

- Shifting locus of care
- Accountable care and patient engagement
  - Accountable Care Organizations (ACOs)
  - ACOs need to collect metrics about health of their patient population
  - ACOs motivate patients to engage and remain healthy

Five trends in Healthcare IT
– and their implications for security & privacy

- Shifting locus of care
- Accountable care and patient engagement
- Continuous patient monitoring outside the clinical setting
  - For post-discharge monitoring of patients returning home
  - For monitoring and managing chronic conditions
  - For encouraging healthy behavior and assisting with behavioral health

Five trends in Healthcare IT – and their implications for security & privacy

- Shifting locus of care
- Accountable care and patient engagement
- Continuous patient monitoring outside the clinical setting
- Advent of mobile devices and cloud services in health-related applications
  - Smartphones and wearables measure physiology, activity, and environment
  - Cloud services support small and distributed healthcare organizations

Five trends in Healthcare IT – and their implications for security & privacy

- Shifting locus of care
- Accountable care and patient engagement
- Continuous patient monitoring outside the clinical setting
- Advent of mobile devices and cloud services in health-related applications
- Emerging threats and changing regulatory environment
  - Expanding use of EHRs increase risk of large-scale privacy breaches
  - Increasing occurrence of Medical Identity Theft
  - Mobile devices and cloud services increasingly under attack
  - FDA will regulate some mHealth devices/apps as medical devices

mHealth

The use of mobile computing and communications technology in the delivery of healthcare or collection of health information.

mHealth in the clinic

Inpatient monitoring

Remote patient monitoring

Personal wellness applications

Fitbit Surge

sleep trackers

Raiing fertility tracker

mHealth in the developing world

mHealth platforms: Smart phones

mHealth devices are emerging

sensor clothing

smartsensing.fr

smart inhaler

ECG patch

pillbox

Shared sensors, environmental sensors

Withings wireless body scale

Caliber III
(temperature and humidity)

Wireless Heart Rate Monitor
(ProForm AccuRate)

Blood Pressure Monitor
(Omron M10)

mHealth – what's different?

- **Security**
  - **Immediate**, personal impact
    - mHealth devices directly affect your health, or health decisions
- **Privacy**
  - **Sensitivity** of data:
    - mHealth data is inherently personal, literally about you
  - **Volume** of data:
    - mHealth collects far more medical data, over extended periods
  - **Diversity** of data:
    - mHealth collects a broader range of information, including lifestyle, activities, and context
  - **Uses** of data:
    - mHealth enables a broad range of apps, outside the doctor-patient relationship

Poor practices in mHealth apps:

"Mobile healthcare application privacy policies are hard to find, and those in place are not providing transparency on privacy practices and more than half aren't focused software, according to a new study."

FierceMobile Healthcare

NEWS TOPICS ANALYSIS FEATURES

Topics: Software / Apps

Mobile app privacy practices scarce, lack transparency

August 24, 2014 | By Judy Mottl

SHARE

Email

34

Tweet

3

Share

0

Like

1

+1

Mobile healthcare application privacy policies are hard to find, and those in place are not providing transparency on privacy practices and more than half aren't focused software, according to a new study.

The research, published in the Journal of the American Medical Informatics Association, states that of the 600 most common apps, just 183 boasted a privacy policy. Of those policies, about two thirds, or 66.1 percent, did not address the software and sharing practices.

"Only a few privacy policies actually pertained to the app. The remaining privacy policies refer to Web pages unrelated to the app, state general privacy practices or even reference privacy practices of an entity entirely unrelated to the app," study author Ali Sunyaev, an assistant professor in the department of information systems at the University of Cologne, Germany, wrote in an email to *FierceMobileHealthcare*.

Security concerns in Android apps

- Studied 160 mHealth apps
- 64% of apps sending data over the Internet, do it in plaintext
- 82% of apps use third-party storage and hosting services such as Amazon's cloud services.

- Paper appeared at AMIA'14
  - *Dongjing He, et al., UIUC*

AMIA Symposium, Washington DC, November 2014

Security Concerns in Android mHealth Apps

Dongjing He, Muhammad Naveed, Carl A. Gunter, Klara Nahrstedt
Dept. of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL

Abstract

Mobile Health (mHealth) applications lie outside of regulatory protection such as HIPAA, which requires a baseline of privacy and security protections appropriate to sensitive medical data. However, mHealth apps, particularly those in the app stores for iOS and Android, are increasingly handling sensitive data for both professionals and patients. This paper presents a series of three studies of the mHealth apps in Google Play that show that mHealth apps make widespread use of unsecured Internet communications and third party servers. Both of these practices would be considered problematic under HIPAA, suggesting that increased use of mHealth apps could lead to less secure treatment of health data unless mHealth vendors make improvements in the way they communicate and store data.

1. Introduction

The mHealth trend is evident: as of March 2013, Research2Guidance reported that there were about 97,000 mHealth apps across 62 app stores[1]. According to a report from MarketsandMarkets, the global mHealth market is predicted to grow from $6.21 billion in revenue in 2013 to $23.49 billion by 2018 at a compound annual growth rate (CAGR) of 30.5 percent over the five-year-period from 2013 to 2018. The mobile fitness and wellness market is expected to grow at a CAGR of 36.7 percent from 2013 to 2018[2]. This rising mHealth market threatens changes in the way significant amounts of health data will be managed, with a paradigm shift from mainframe systems located in the facilities of healthcare providers to apps on mobiles and storage in shared cloud services. This trend is paralleled by a new openness in which devices that were once only available in hospitals become widely available to individuals while flexible mHealth applications tempt clinicians away from the hospital-based systems they used in the past. This popular market will disruptively challenge traditional approaches by being cheap and accessible.

Security and privacy of health data could be significantly affected by this trend. Freed from the bonds of HIPAA, mHealth apps are free to handle data using lower assurances than those typically applied to HIPAA entities. However, the data they handle is often as sensitive as the data handled by HIPAA entities. Typical Google Play apps such as Self-help Anxiety Management, iCardio, Epocrates CME, and Clinical Advisor provide assistance with mental health concerns, activity monitoring, and information services that reveal user interests in particular symptoms or diseases. It is important to develop guidelines for the security and privacy of mHealth apps that suit a dynamic market while assuring that the growth of mHealth does not lead to a cavalier vendor attitude toward personal data. New security and privacy risks particular to mobile computing and communications technology abound in mHealth apps[3, 4]. The aspects of mHealth make it different from other health information systems: First, mHealth apps allow a much larger amount of data being collected from the patient, as mobile devices can collect data over extended periods of time. Second, a much broader range of health-related data is being collected, as many mHealth apps collect patient activities and lifestyle, not only physiological data, but also include physical activity, location tracking, eating habits and diet details, social interactions and so on. Third, the nature of communications technology and mobile computing exposes many new attack surfaces to the outside world.

The goal of this paper is to carry out a three-stage study of the security and privacy status of free mHealth apps offered on Google Play. In the first study, the top 160 free mHealth apps in Google Play are classified and examined to formulate a list of attack surfaces that need attention in this area. These are shown in Table 1. Then a random sample of 27 apps is selected from the top 1080 apps and analyzed with respect to these seven attack surfaces. Significant issues are found in three attack surfaces: *Internet*, *Logging*, and *Third Party Services*. Since our concern about *Logging* will be addressed to a significant degree by deployment of a new version of Android, we focus our attention on the other two: *Internet* and *Third Party Services*. A random sample of additional 22 apps is taken involving Internet communications. Examination confirms that many of these 22 apps display significant risks to security and privacy on these two attack surfaces. Our primary conclusions are that the mHealth apps in Google Play commonly send sensitive data in clear text and store it on third party servers whose confidentiality rules may not be as strong as they need to be for the type of data being stored.

Trustworthy Health & Wellness

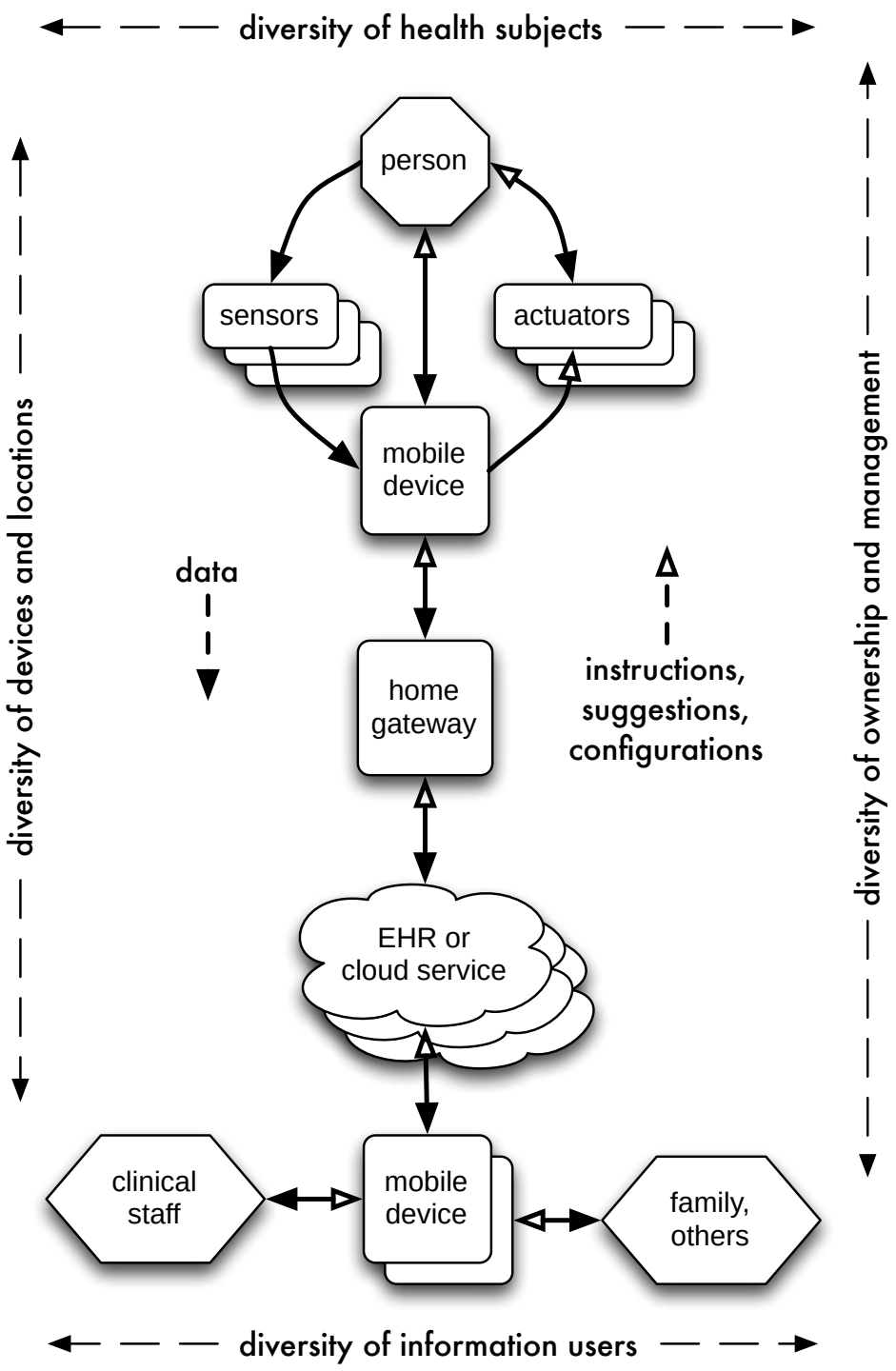
Funded by a Frontier-scale award from the NSF SaTC (Secure and Trustworthy Cyberspace) program, 2013–18.

Interdisciplinary research team

- Principal Investigators
  - **Kevin Fu** (UM) – medical device security
  - **Carl Gunter** (UIUC) – computer security in healthcare
  - **David Kotz** (Dartmouth) – mHealth security and privacy
  - **Avi Rubin** (JHU) – cybersecurity, cryptography, e-voting, healthcare
- Computer Science
  - **Roy Campbell** (UIUC) – security, cloud computing, and ubiquitous computing
  - **Peter Honeyman** (UM) – storage, security, and distributed systems
  - **Carl Landwehr** (GWU) – cybersecurity
  - **Klara Nahrstedt** (UIUC) – security, cloud computing, and multimedia
  - **Jenna Wiens** (UM) – machine learning in medicine
- Economics of healthcare IT
  - **Eric Johnson** (Vanderbilt) – economics of cybersecurity in healthcare IT
- Healthcare IT
  - **Darren Lacey** (JHU) – Chief Information Security Officer at JHU Medicine
- Behavioral health
  - **Lisa Marsch** (Dartmouth) – Director of the Center for Technology and Behavioral Health
- Health policy and population health
  - **Jonathan Weiner** (JHU) – Director of the Center for Population Health IT

TH&W

- Mobile & cloud technology is being deployed for health and wellness
- Security and privacy are essential to attain the trust of patients and clinicians alike
- THaW addresses issues of authentication, privacy, data integrity, device management, and accountability



THaW Projects underway

- Incentive Mechanism Design for mHealth Participatory Sensing
- Mobile Health Data Collection and Analysis
- Small Health Networks
- Secure Cloud Based EHR
- Inferring a Networked Device's Activity from its LED Blinks
- Clinician Friendly Authentication
- Wearable Device Outreach Activity
- Evaluating ECG use in Cryptography
- Beacons in Hospitals
- Kerberos Bracelet Identification (KBID)
- Detection of Close Encounters
- Wearable User-presence Authentication to Web Applications
- Securely Connecting Wearable to Ambient Displays with User Intent
- Assessing User Data Exposure to Advertising Libraries on Android
- Meaningful Security
- Optimal distribution (prioritization) of scarce security personnel
- Information Security and User Behavior in the Health Sector
- Patient Reaction to Healthcare Data Breaches
- Auditable Medical Devices

Beacon+

Bluetooth Low Energy (BLE) Beacons for
Asset and Personnel Tracking,
Location-Based Restrictions,
and Real-Time Navigation

Tom Tantillo, Michael Rushanan, Paul Martin, Avi Rubin

Location tracking in a hospital

- Challenges:
  - **Inventory**: maintain accurate up-to-date picture of equipment, inventory, personnel – “moving parts”
  - **Sensitive data**: every computer gives users access to entire database
  - **Navigation**: visitors need to find their way, and staff are burdened with questions
- Solution: **Beacon+**

  Bluetooth beacons

example: estimote.com

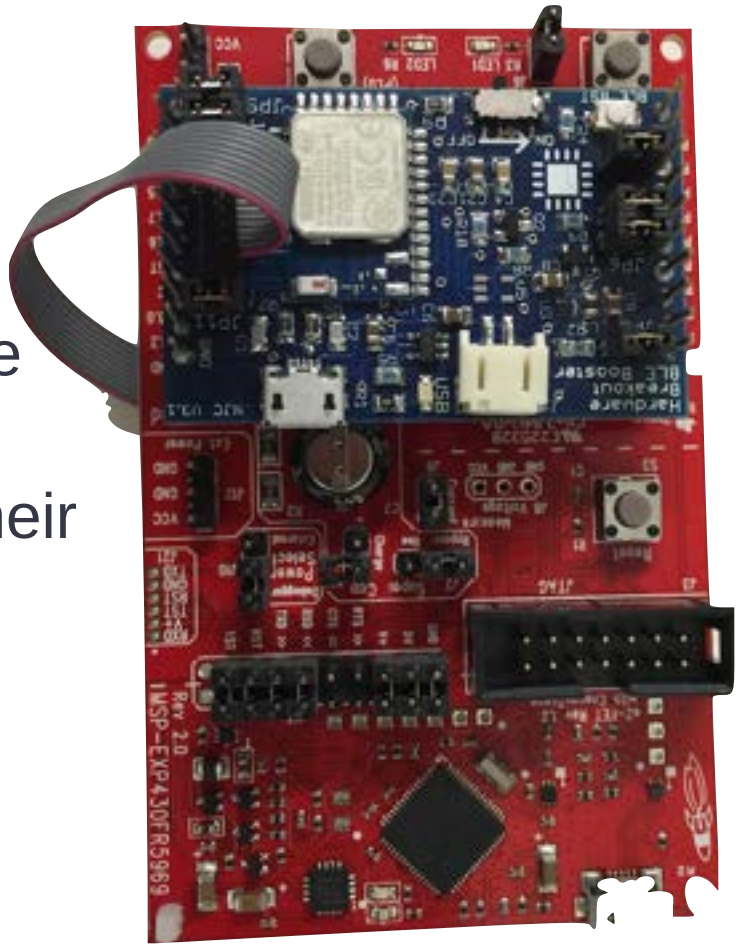
Beacon Highlights

- Beacons are small and inexpensive ($5-10)
- Room-level accuracy and sub-second latency
- Long battery life
- Standard protocols
- Extensible framework for applications
- Supported by most smartphones

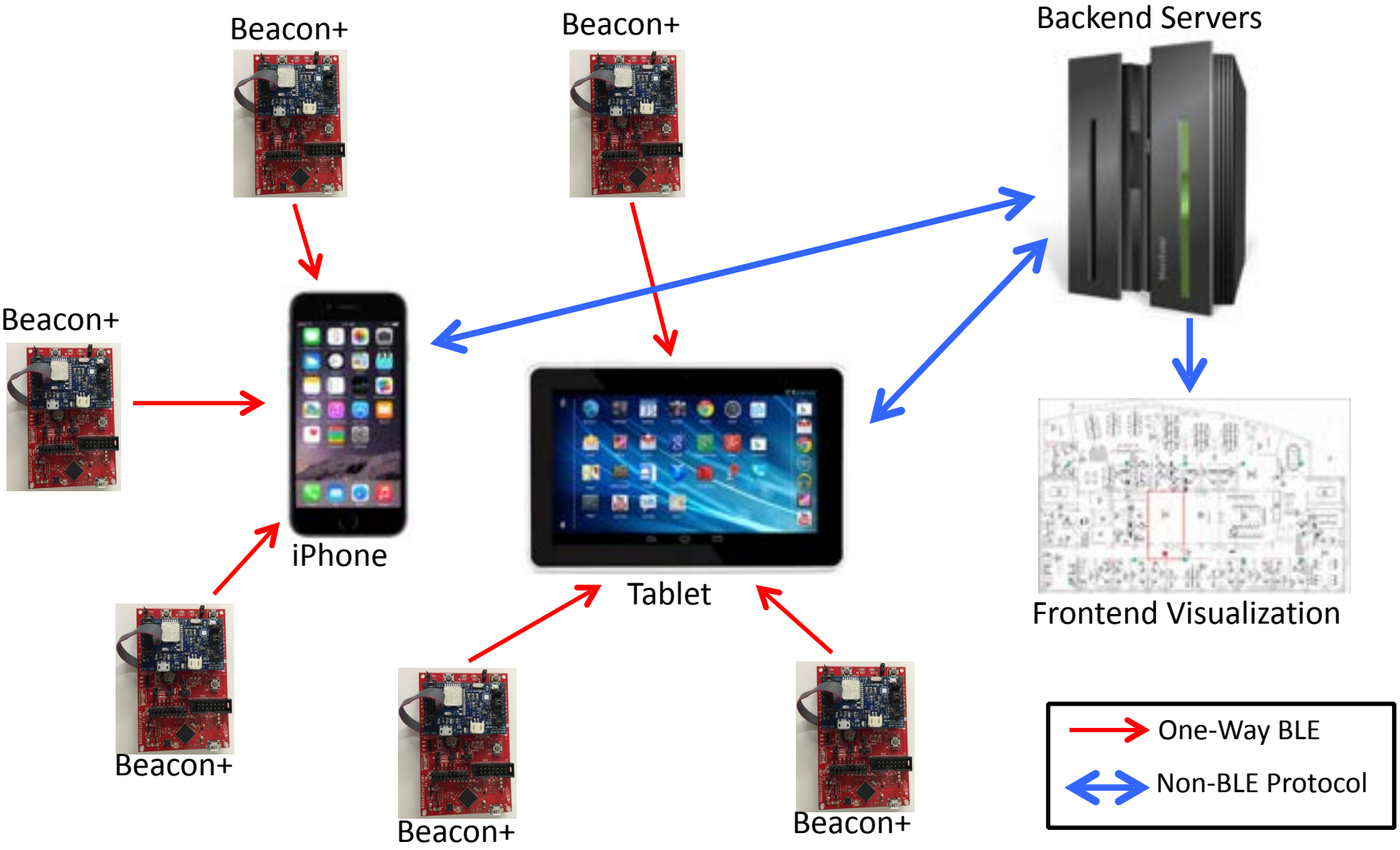
example: estimote.com

Beacon+ adds crypto to beacons

- Standard beacons have no security
- THaW prototype at JHU
  - built from MSP430 LaunchPad
  - uses standard beacon protocol
  - adds message authentication code (AES CBC-MAC)
- Result: beacons securely attest to their location



System architecture



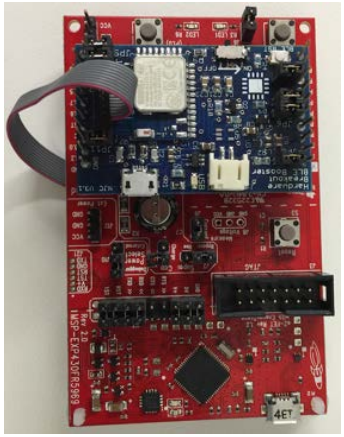
Beacon+ supported applications

- **Location-based access control**
  - Two-factor access-control policies for sensitive data:

    identity (fingerprint or password)

    +

    location (or proximity)



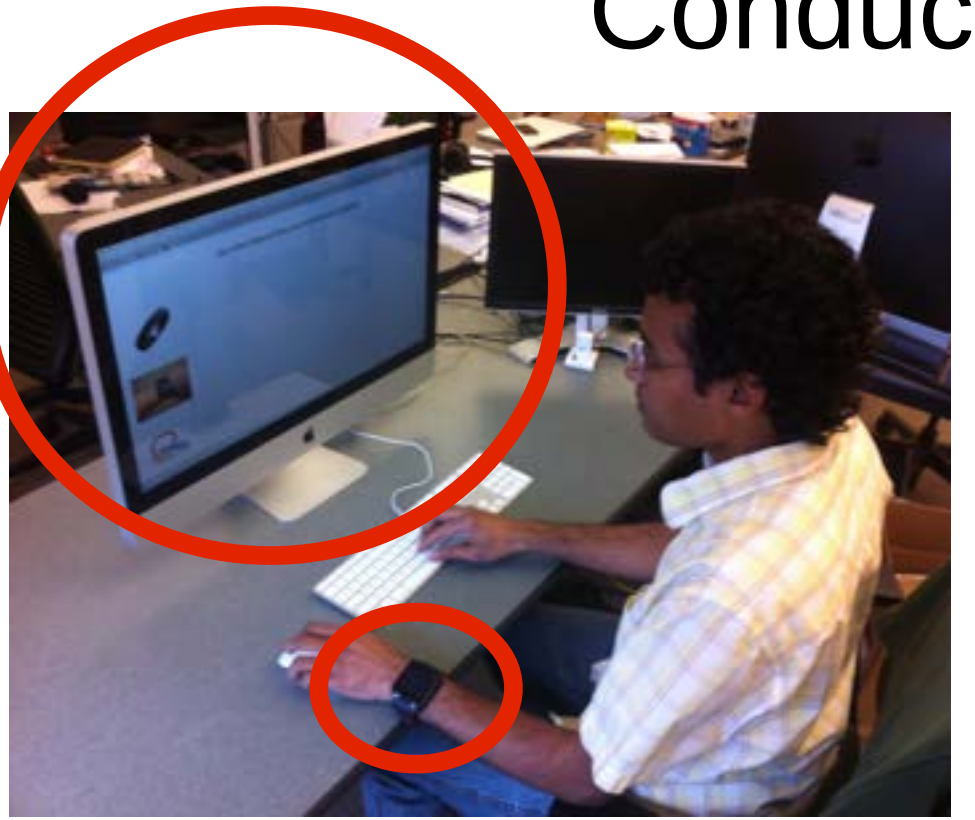
- **Real-time indoor navigation**
  - App to guide unfamiliar visitors to their destination
  - Increases staff productivity

Continuous authentication

Shrirang Mare

BRACE

Bilateral Recurring Authentication Conducted Effortlessly



Formerly known as "ZEBRA"

Shrirang Mare, IEEE S&P 2014

Motivation

Security and Privacy issues in hospitals

Photo courtesy of ortho.wustle.edu

Motivation: Clinical workstations

- Unattended logged-in computers
- Security risk
- Compliance issues

The De-authentication Problem

- Users forget to logout, or
- They intentionally do not logout

http://millerhealthlaw.com/company

Motivation

- Timeouts are too long, or too quick
- Human proximity detector
  - Styrofoam cup story [Sinclair et al. 2013]

Motivation

- RF proximity-based authentication
  - Authenticate if user is in radio proximity

www.sonomacountyconnections.org

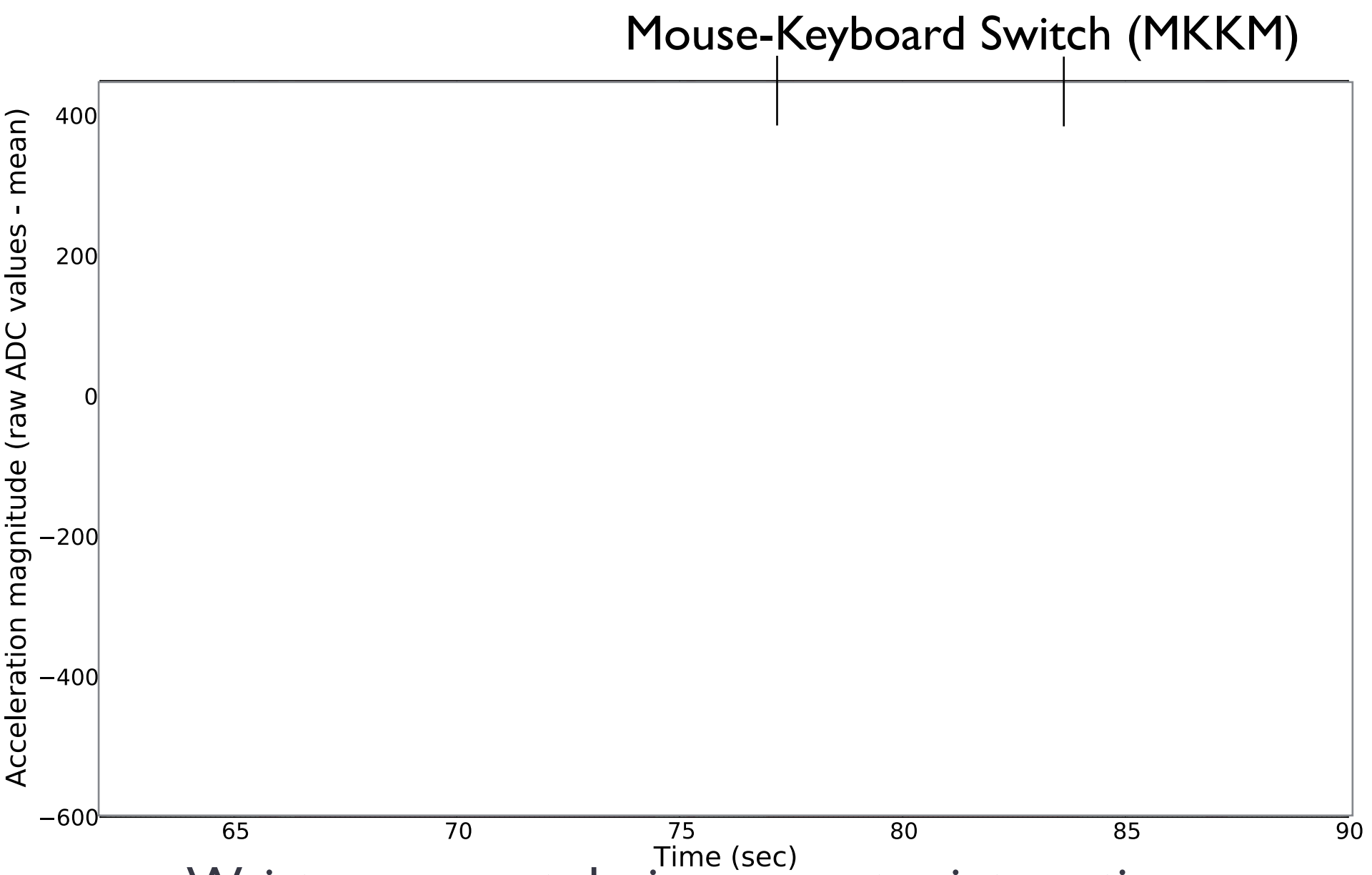
ShutterStock video under license

But who is actually using the device?

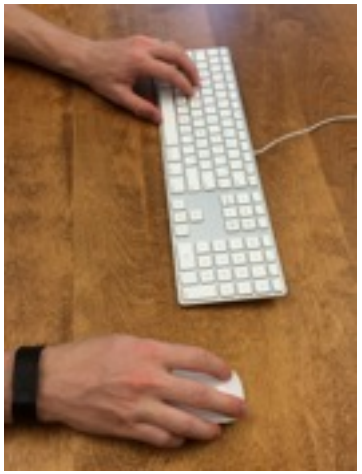
Our solution: BRACE

What interactions a user performs

- Monitor wrist movement with wristband (BRACElet)
- Correlate wrist movement and input to computer

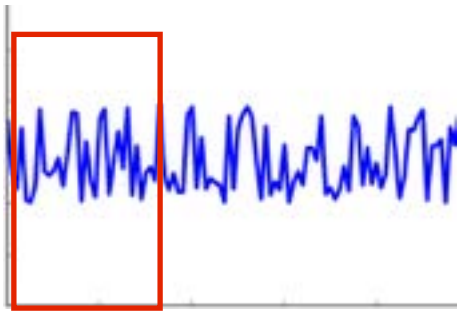


Wrist movement during computer interaction



Interactions

1. Typing
2. Scrolling
3. Mouse-Keyboard switch



I_0, t_s^0, t_e^0

Actual

Sequence of Interactions

Correlate

I_0', t_s^0, t_e^0

F_0

Classifier

Sequence of Interactions

Estimated

BRACE does **not** use behavioral biometrics

- BRACE classifiers are trained once, for all users
- a biometric bracelet could provide additional assurance
  - Cornelius (MobiSys'14) demonstrated bio-impedance bracelet that can identify its wearer

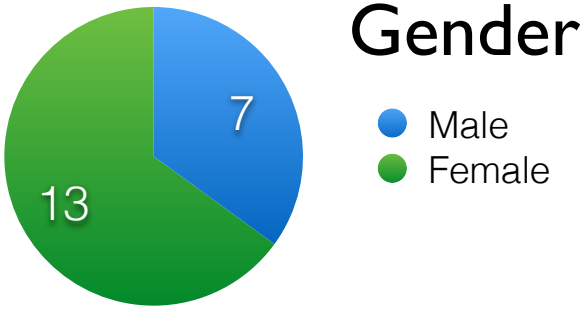
Early results

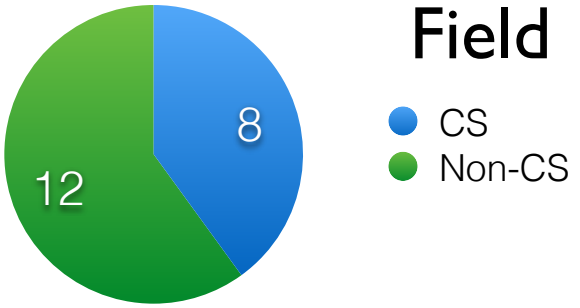
User study

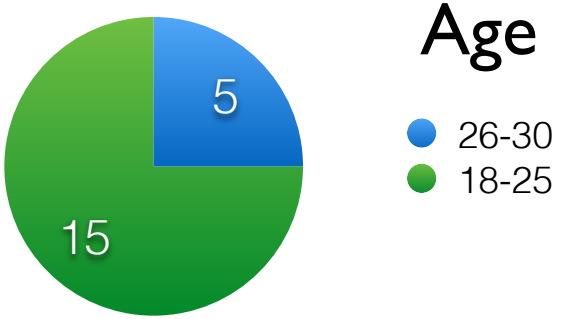
- 20 subjects
- 30-40 mins study session

Tasks during study:

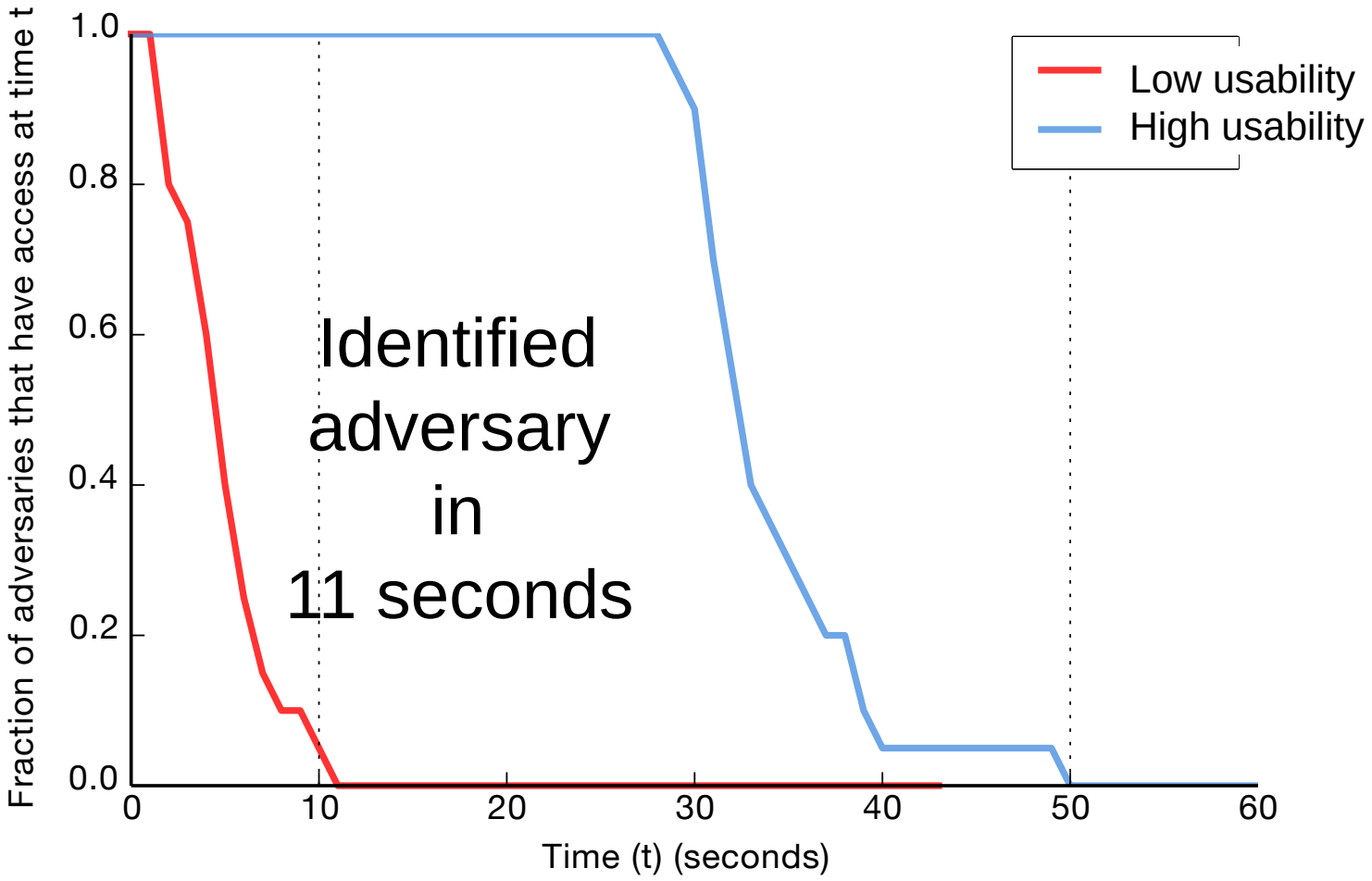
- Fill out web survey
- Browse internet
- Mimic another user







Security



Fraction of **adversaries** that have access at time *t*

BRACE and its extensions

- **Continuous authentication** (BRACE today):
  - BRACE continuously verifies the user after s/he logs in with an initial authentication method (such as username/ password)
- **Initial authentication** (work in progress):
  - BRACE verifies the user who taps the keyboard or wiggles the mouse, then logs her into the computer
- **Smartphone and Tablet computers** (work in progress):
  - BRACE compares motion of wrist to motion of the phone or tablet, to verify who is holding/using the device

TH&W

Small health networks

Tim Pierson

Managing medical devices in Small Health Networks (SHNs) is difficult

Examples of small health networks

Focus of our research

Small clinic
2-3 doctors plus support staff

Assisted-living
Support staff may cover large number of residents

Home health care
No full-time professional staff

Common characteristics

- Medical devices increasingly computerized
- Increasing reliance on specialized medical devices (more devices used)
- Generally no dedicated IT department
- Devices behind firewall (we hope!)

Implications

- Configuring/installing devices challenging
- Tracking/updating devices difficult
- No one on site to assist when things go wrong
- Remote support difficult or impossible

Procedures that are simple in a large environment can be difficult in a SHN

Concrete example: monitor blood pressure at home

Take home a blood pressure monitor so I can track your health

Simple, right?

Doctor's intention:

- Patient will use a mobile medical device at home (e.g., blood-pressure monitor)
- Patients will take regular readings of a health condition using the medical device (e.g., measure blood pressure daily)
- The readings will readily available for the doctor to review (e.g., via EHR)

Two major issues:

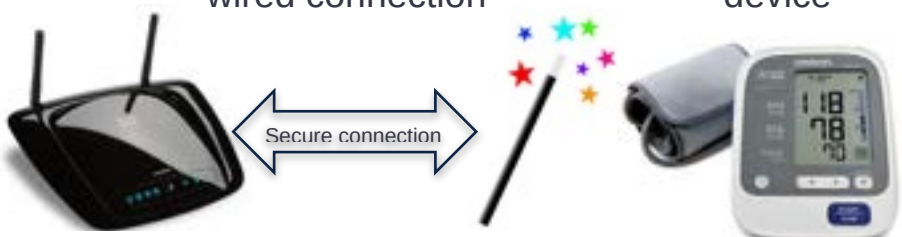
1. How does the blood-pressure monitor get online to transmit its data?
   - No long range radio or Ethernet
   - Limited device displays make connecting with existing telecom infrastructure difficult
   - Different device manufacturers have different procedures
2. How does the data get to the right medical record?
   - What patient ID/ passwords to use?
   - What web service end points?

We introduce a tool to make configuring new medical devices extremely easy

Example: four steps to configure new medical device for WiFi Access Point

1. Tool lives attached to AP; gets SSID/ password over secure wired connection

2. User detaches tool from AP and brings close to new medical device



WiFi Access Point (AP)

Detachable tool

Medical device

3. Tool injects SSID/ password of AP into medical device using novel RSSI technique

4. Medical device uses AP's SSID/password to make WiFi connection

Benefits

- **Fast** - can impart 128 bits onto device in 0.5 secs
- **Easy** - tool learns config info, user need not even know it; just point tool at new device to impart config info; provides consistent interface
- **Secure** - Resistant to both passive and active attackers > 12 cm away from new device
- **Versatile** - can impart any type of information onto any type of wireless device, even devices with limited displays/interfaces; no hardware modification to new device
- **Mobile** - useful even if new device cannot be physically moved in close proximity to AP

Detecting close encounters

Aarathi Prasad

Contagious diseases

Dartmouth College Cafeteria on flickr.com

Courtesy: wordpress.com

- Diseases such as flu, measles, and gastroenteritis are spread through physical contact via airborne diseases or shared objects.
- In case of measles, the virus survives in the air for two hours

Leverage smartphones

Courtesy: Images obtained on Google search

- To detect encounters (physical co-location)

Leverage smartphones

Courtesy: Images obtained on Google search

- To detect encounters (physical co-location)
- To detect close encounters (spatial and temporal proximity)

We plan to use smartphones and beacons to detect encounters and close encounters and contain the spread of contagious diseases using a privacy-preserving cryptographic techniques

amulet

image: shutterstock.com

image: thetimes.co.uk


image: winarticles.net

image: techgc.net

Amulet

- a wrist-mounted mHealth platform
- that is with the user at all times,
- can authenticate its wearer,
- can be secured independently of other apps on the mobile phone or home computer,
- can provide a trustworthy interface to the user, and
- can support mHealth devices with computation and a network link.

Amulet

computational jewelry, in a bracelet form, to provide a secure multi-application platform for body-area mHealth applications.

Amulet – the big picture

App Developer

app source

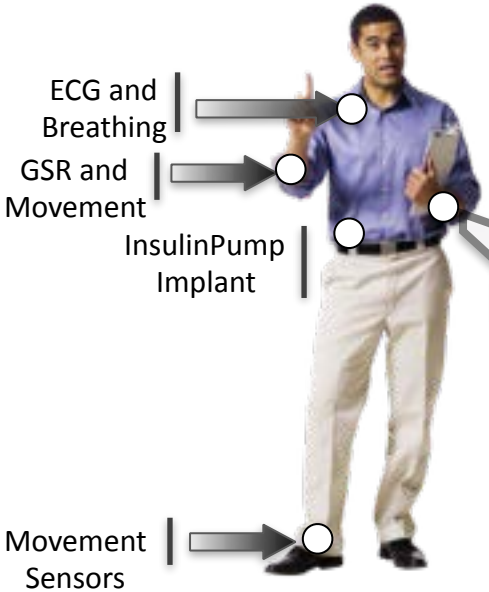
Amulet Cloud

app recommendations

Clinician

customized & signed firmware

data upload



Patient

amulet

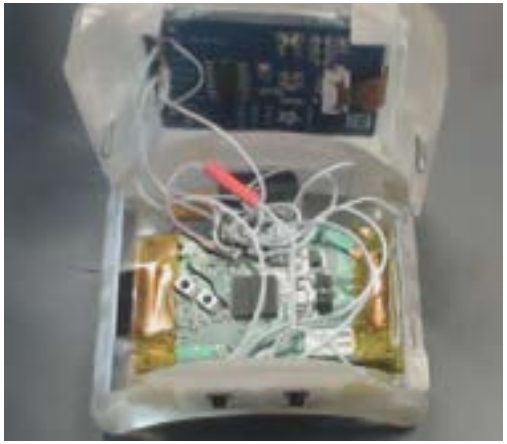
companion smartphone

See amulet-project.org

Amulet wearable

- Two buttons
- Scroll wheel
- Zero-energy display
- Light, sound temp sensors
- IMU sensor

Wearable Prototype (2015)



App Board
~2.3x4.1cm

Sensors
- 9-axis motion sensor, Invensense MPU-9250
- 3-axis low power accelerometer, ST Electronics LIS3DH
- Ambient light, temp, sound, battery

Computing
- Nordic nRF51822, ARM Cortex M0, 16K RAM, 256K FLASH
- TI MSP430FR5969, 2KB SRAM, 64KB FRAM
- microSD card slot

Network
- BLE radio (Central & Peripheral), USB

Output
- Monochrome 96x96 Sharp Memory LCD
- or two single color LEDs

Input
- two buttons
- scroll wheel
- accelerometer

Battery
- Polymer Li-Ion, 110 mAh, 3.7V

Radio Board

Amulet inside

Amulet apps (so far)

- **Stress monitoring**
  - internal (IMU) and external (GSR, heart) sensors
  - computes and logs the wearer's stress level
  - later, creative intervention at times of stress
- **Drowsiness detector**
  - uses external "Mio" heart-rate monitor
- **Fall detection**
  - uses internal accelerometer
  - triggers emergency mode upon a fall
- **Emergency access for EMTs**
  - via USB to EMT laptop: recent sensor data

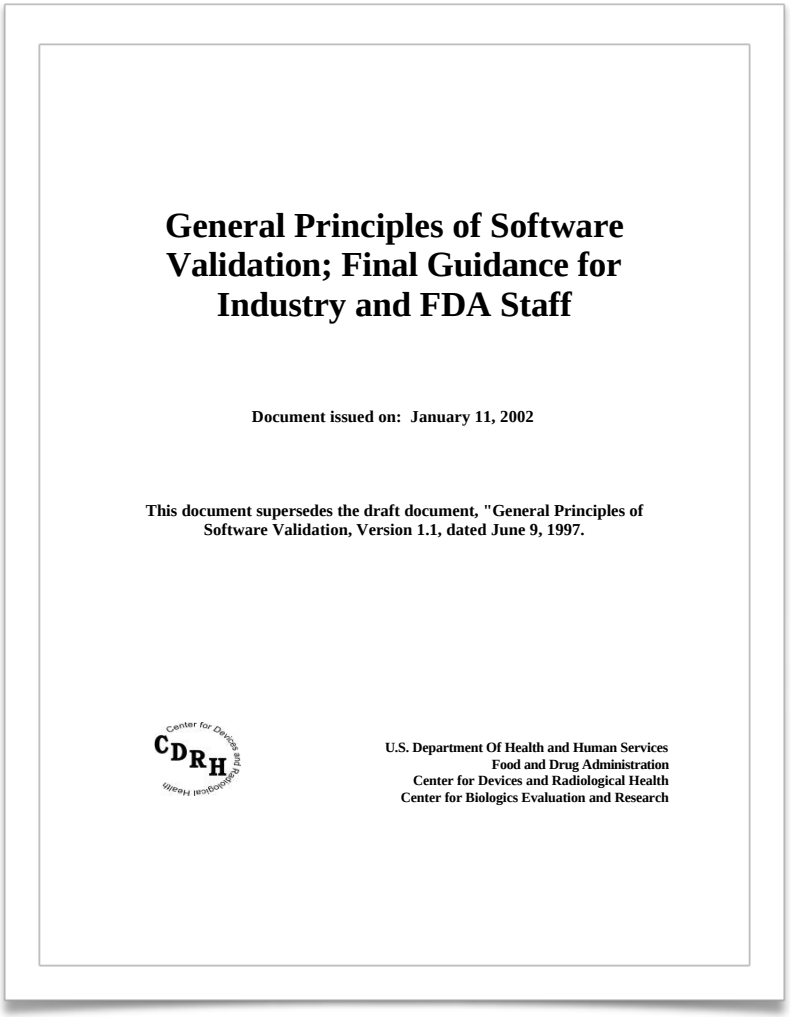
mHealth regulatory status

in the United States

caveat:
I am not a lawyer

FDA 2002: principles of software validation

"This guidance outlines general validation principles that the Food and Drug Administration (FDA) considers to be applicable to the validation of medical device software or the validation of software used to design, develop, or manufacture medical devices." – 2002



General Principles of Software Validation; Final Guidance for Industry and FDA Staff

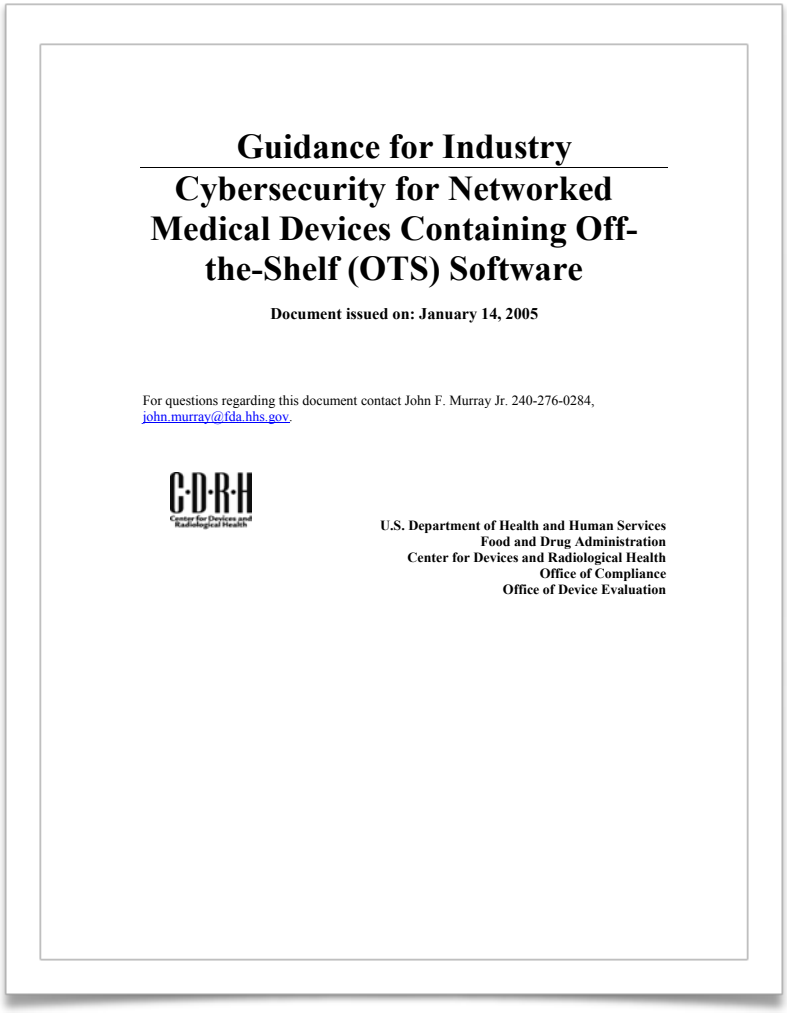
Document issued on: January 11, 2002

This document supersedes the draft document, "General Principles of Software Validation, Version 1.1, dated June 9, 1997.

U.S. Department Of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

FDA 2005: cybersecurity for medical devices containing OTS software

"This guidance provides recommendations for medical devices that incorporate off-the-shelf (OTS) software and that can be connected to a private intranet or the public Internet. This guidance is addressed to device manufacturers who incorporate OTS software in their medical devices."



Guidance for Industry

Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software

Document issued on: January 14, 2005

For questions regarding this document contact John F. Murray Jr. 240-276-0284, john.murray@fda.hhs.gov.

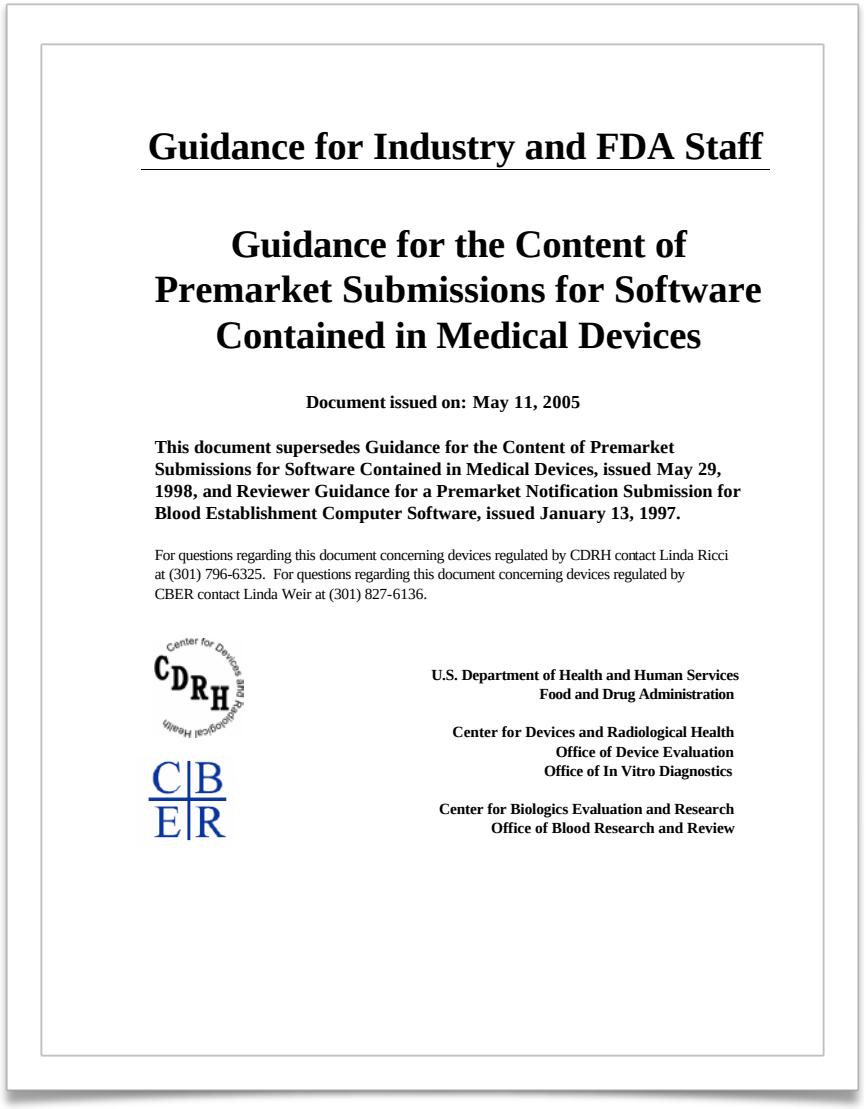
C·D·R·H
Center for Devices and Radiological Health

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Compliance
Office of Device Evaluation

FDA 2005: Software Contained in Medical Devices

"we refer to devices that contain one or more software components, parts, or accessories, or are composed solely of software as 'software devices,' including:

- firmware and other means for software-based control of medical devices
- stand-alone software applications
- software intended for installation in general-purpose computers
- dedicated hardware/software medical devices.
- accessories to medical devices when those accessories contain or are composed of software."



Guidance for Industry and FDA Staff

Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Document issued on: May 11, 2005

This document supersedes Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, issued May 29, 1998, and Reviewer Guidance for a Premarket Notification Submission for Blood Establishment Computer Software, issued January 13, 1997.

For questions regarding this document concerning devices regulated by CDRH contact Linda Ricci at (301) 796-6325. For questions regarding this document concerning devices regulated by CBER contact Linda Weir at (301) 827-6136.

Center for Devices and Radiological Health
CDRH

CBER

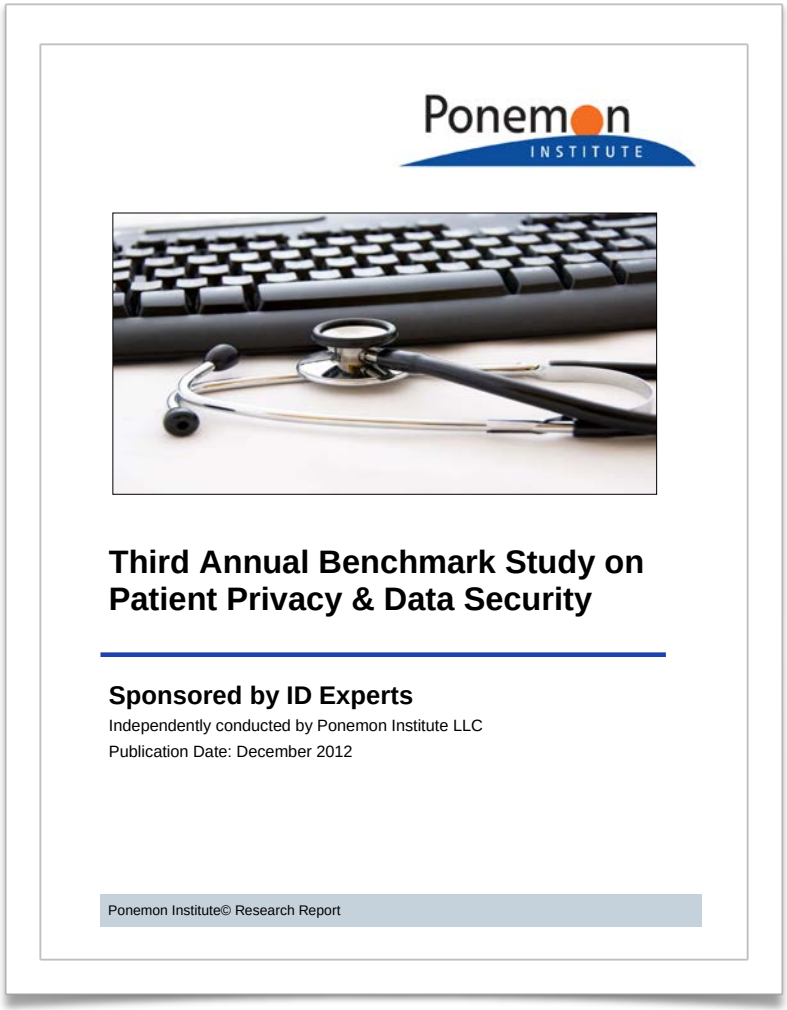
U.S. Department of Health and Human Services
Food and Drug Administration

Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics

Center for Biologics Evaluation and Research
Office of Blood Research and Review

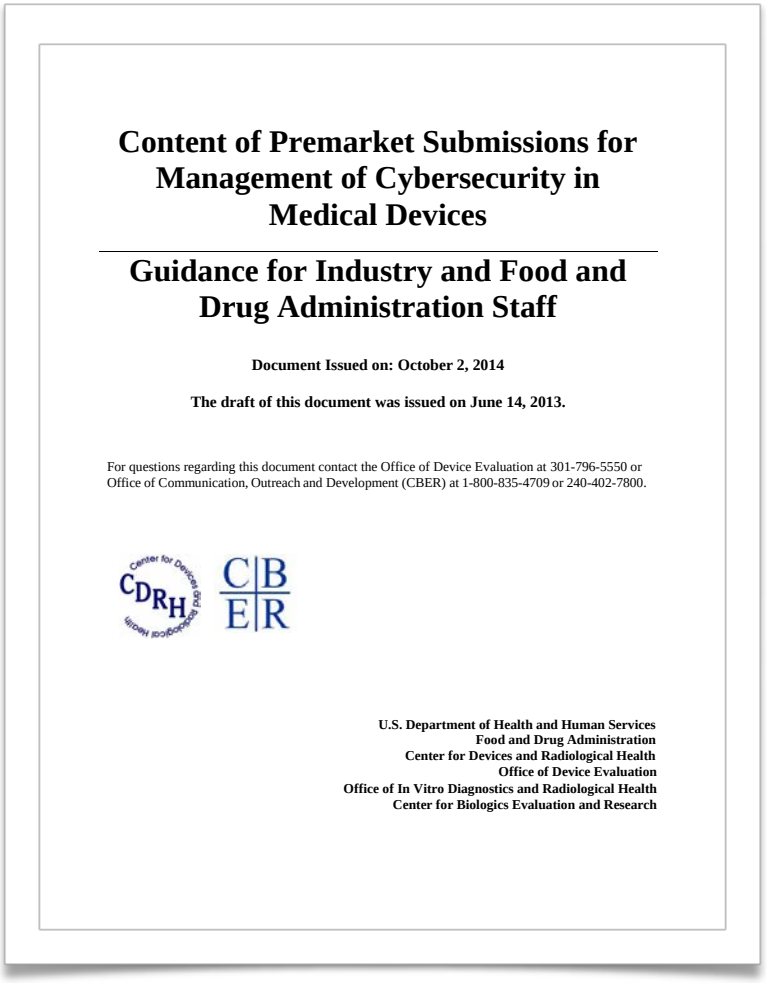
FDA 2012: Human Factors in Medical Device Software Development

Ponemon 2012: Benchmark Study of Patient Privacy & Data Security



FDA 2014: Management of Cybersecurity in Medical Devices

- "Manufacturers should develop a set of cybersecurity controls to assure medical device cybersecurity and maintain medical device functionality and safety."
- "This guidance provides recommendations to consider and information to include in FDA medical device premarket submissions for effective cybersecurity management."



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

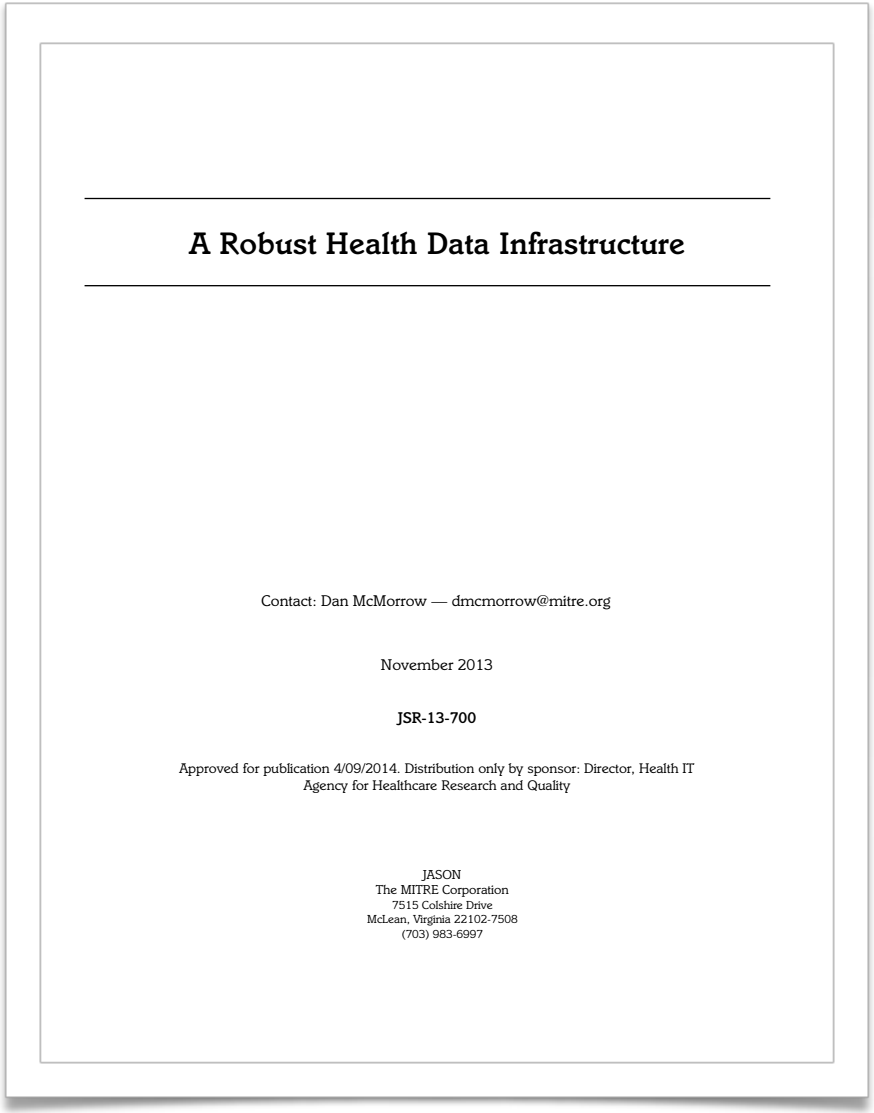
The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

JASON 2014: A Robust Health Data Infrastructure

- "ONC [should] define an overarching software architecture for the health data infrastructure.
- "ONC should solicit input… to ensure that the health data infrastructure meets the needs of researchers.
- "The adopted software architecture must have the flexibility to accommodate new data types that will be generated by emerging technologies, ….
- "ONC should exert leadership in facilitating international interoperability for health data sharing for research purposes…
- "Large-scale data mining techniques and predictive analytics should be employed to uncover signatures of fraud."



A Robust Health Data Infrastructure

Contact: Dan McMorrow — dmcmorrow@mitre.org

November 2013

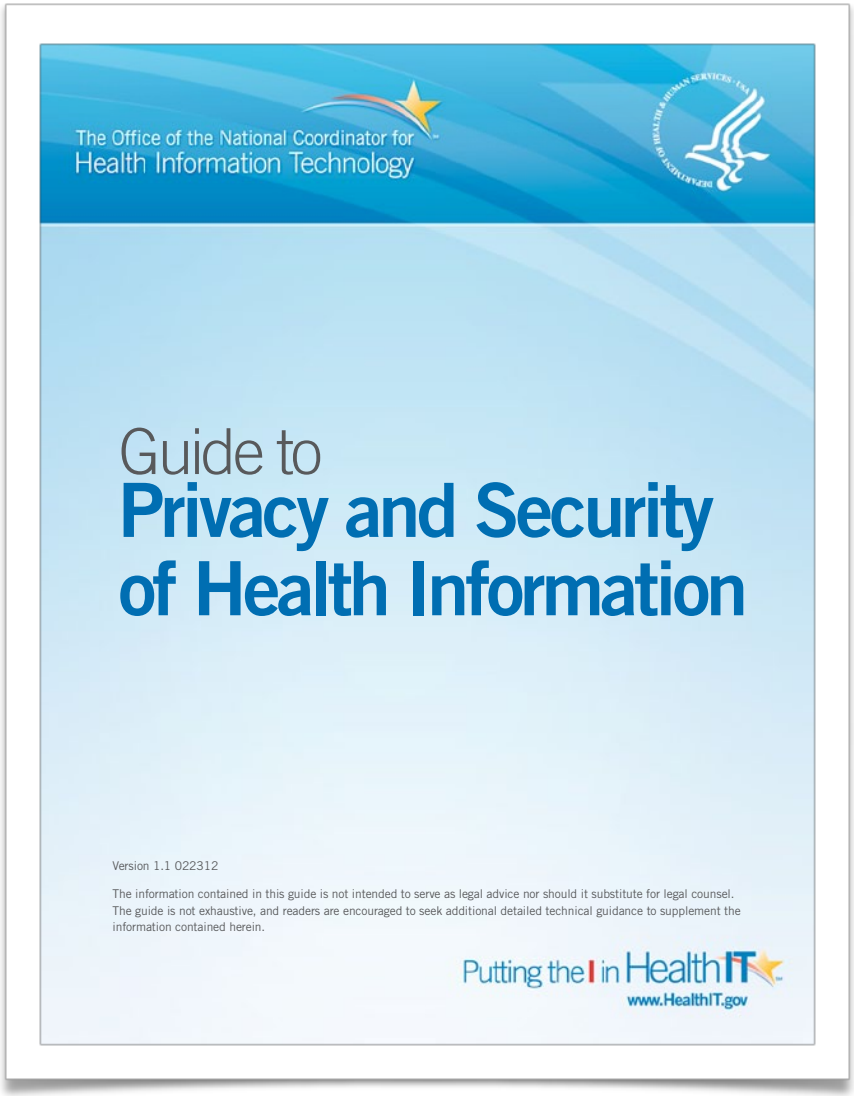
JSR-13-700

Approved for publication 4/09/2014. Distribution only by sponsor: Director, Health IT Agency for Healthcare Research and Quality

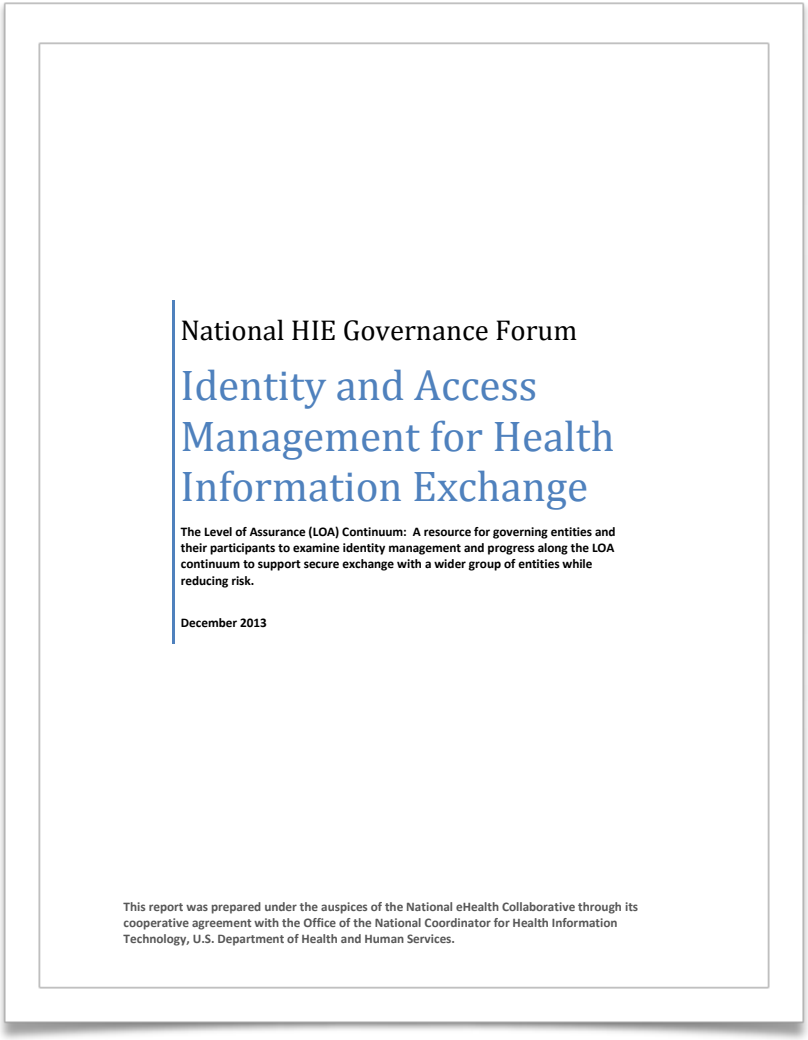
JASON
The MITRE Corporation
7515 Colshire Drive
McLean, Virginia 22102-7508
(703) 983-6997

ONC 2012 Privacy and Security of Health Information

- Appendix with links to relevant resources



NeHC 2013: Identity and Access Management for Health Information



National HIE Governance Forum

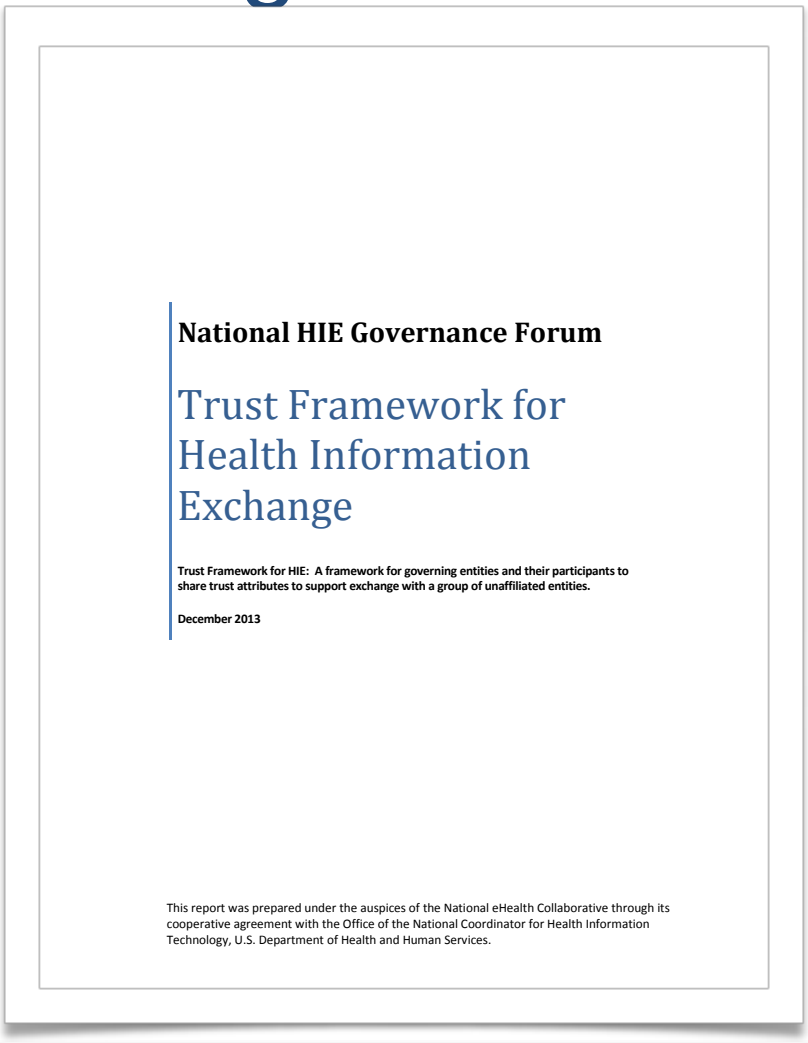
Identity and Access Management for Health Information Exchange

The Level of Assurance (LOA) Continuum: A resource for governing entities and their participants to examine identity management and progress along the LOA continuum to support secure exchange with a wider group of entities while reducing risk.

December 2013

This report was prepared under the auspices of the National eHealth Collaborative through its cooperative agreement with the Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services.

NeHC 2013: Trust Framework for Health Information Exchange



National HIE Governance Forum

Trust Framework for Health Information Exchange

Trust Framework for HIE: A framework for governing entities and their participants to share trust attributes to support exchange with a group of unaffiliated entities.

December 2013

This report was prepared under the auspices of the National eHealth Collaborative through its cooperative agreement with the Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services.

Coalfire 2013: HIPAA and HITRUST

TrustLaw 2013: Patient Privacy in a Mobile World – legal framework

PATIENT PRIVACY
IN A MOBILE WORLD
A FRAMEWORK TO ADDRESS
PRIVACY LAW ISSUES
IN MOBILE HEALTH

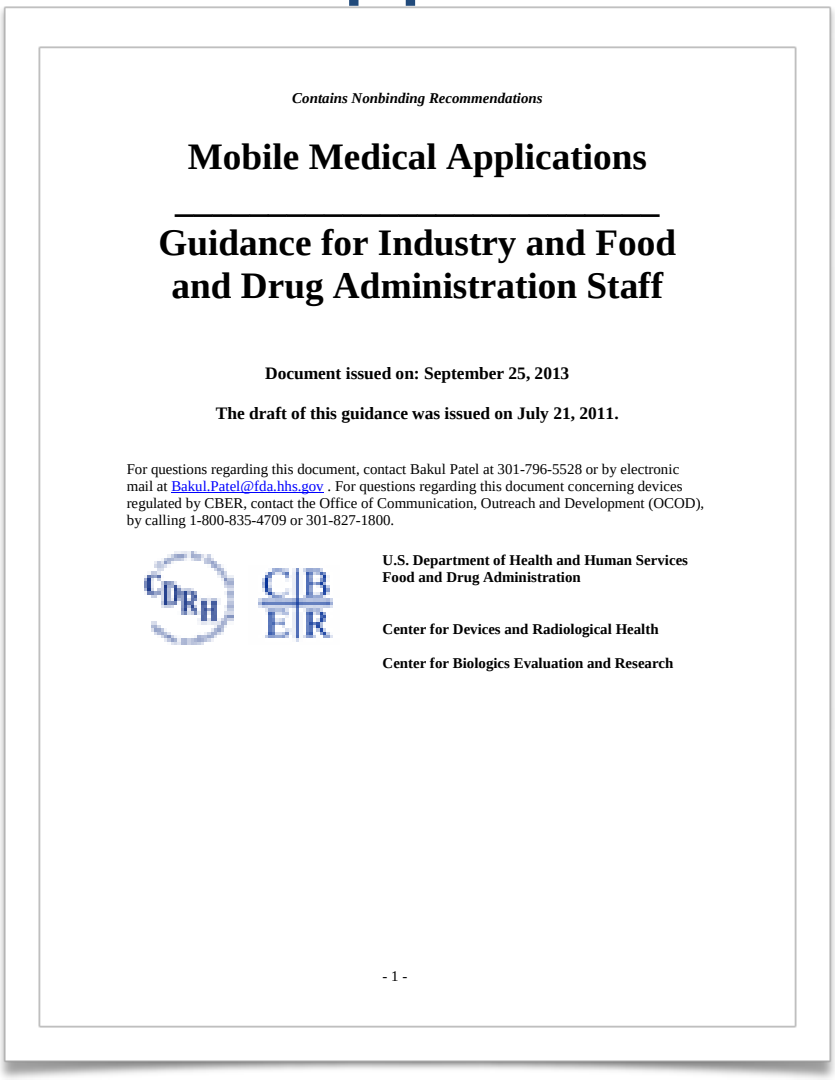
JUNE 2013

TrustLaw mHealth Alliance MSD Be well

Rakitin 2014: Regulation of Mobile Medical Applications

FDA 2013: Mobile Medical Applications

- "The FDA is issuing this guidance document to inform manufacturers, distributors, and other entities about how the FDA intends to apply its regulatory authorities to select software applications intended for use on mobile platforms (mobile applications or 'mobile apps')."



Contains Nonbinding Recommendations

Mobile Medical Applications

Guidance for Industry and Food and Drug Administration Staff

Document issued on: September 25, 2013

The draft of this guidance was issued on July 21, 2011.

For questions regarding this document, contact Bakul Patel at 301-796-5528 or by electronic mail at Bakul.Patel@fda.hhs.gov . For questions regarding this document concerning devices regulated by CBER, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 301-827-1800.

U.S. Department of Health and Human Services
Food and Drug Administration

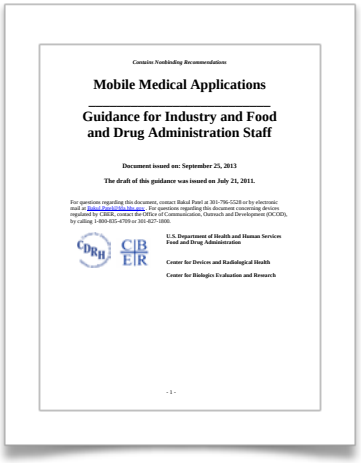
Center for Devices and Radiological Health

Center for Biologics Evaluation and Research

- 1 -

FDA 2013: Mobile Medical Applications

- Defines “mobile app” and “mobile medical app”
- Defines “mobile medical app manufacturer”
- Indicates FDA plans **regulatory oversight** of
  - Mobile apps that are an extension of one or more medical devices
  - Mobile apps that transform the mobile platform into a regulated medical device
  - Mobile apps that become a regulated medical device (software) by performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations.



Contains Nonbinding Recommendations

Mobile Medical Applications

Guidance for Industry and Food and Drug Administration Staff

Document issued on: September 25, 2013

The draft of this guidance was issued on July 21, 2011.

For questions regarding this document, contact Bakul Patel at 301-796-5528 or by electronic mail at Bakul.Patel@fda.hhs.gov. For questions regarding this document concerning devices regulated by CBER, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 301-827-1800.

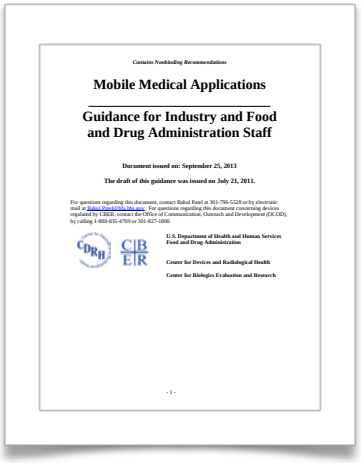
U.S. Department of Health and Human Services
Food and Drug Administration

Center for Devices and Radiological Health

Center for Biologics Evaluation and Research

- 1 -

FDA 2013: Mobile Medical Applications



Contains Nonbinding Recommendations

Mobile Medical Applications

Guidance for Industry and Food and Drug Administration Staff

Document issued on: September 25, 2013

The draft of this guidance was issued on July 21, 2011.

For questions regarding this document, contact Bakul Patel at 301-796-5528 or by electronic mail at Bakul.Patel@fda.hhs.gov. For questions regarding this document concerning devices regulated by CBER, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 301-827-1800.

U.S. Department of Health and Human Services
Food and Drug Administration

Center for Devices and Radiological Health

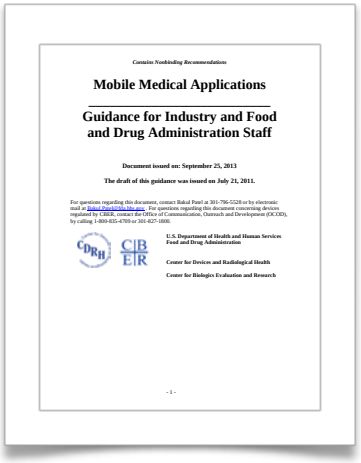
Center for Biologics Evaluation and Research

- 1 -

- FDA plans **enforcement discretion** for
  1. Mobile apps that provide or facilitate supplemental clinical care, by coaching or prompting, to help patients manage their health in their daily environment.
  2. Mobile apps that provide patients with simple tools to organize and track their health information.
  3. Mobile apps that provide easy access to information related to patients' health conditions or treatments (beyond providing an electronic "copy" of a medical reference).

FDA 2013: Mobile Medical Applications

- FDA plans **enforcement discretion** for
  4. Mobile apps that are specifically marketed to help patients document, show, or communicate to providers potential medical conditions.
  5. Mobile apps that perform simple calculations routinely used in clinical practice.
  6. Mobile apps that enable individuals to interact with PHR systems or EHR systems.



Contains Nonbinding Recommendations

Mobile Medical Applications

Guidance for Industry and Food and Drug Administration Staff

Document issued on: September 25, 2013

The draft of this guidance was issued on July 21, 2011.

For questions regarding this document, contact Bakul Patel at 301-796-5528 or by electronic mail at Bakul.Patel@fda.hhs.gov. For questions regarding this document concerning devices regulated by CBER, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 301-827-1800.

U.S. Department of Health and Human Services
Food and Drug Administration

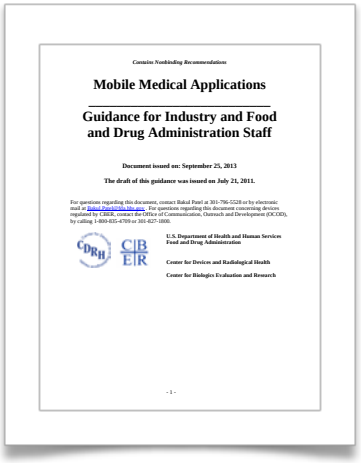
Center for Devices and Radiological Health

Center for Biologics Evaluation and Research

- 1 -

FDA 2013: Mobile Medical Applications

- Report provides **examples** in appendices:
  A. Examples of mobile apps that are *not* medical devices
  B. Examples of mobile apps for which FDA intends to exercise enforcement discretion
  C. Examples of mobile apps that are the focus of FDA's regulatory oversight (mobile medical apps)



Contains Nonbinding Recommendations

Mobile Medical Applications

Guidance for Industry and Food and Drug Administration Staff

Document issued on: September 25, 2013

The draft of this guidance was issued on July 21, 2011.

For questions regarding this document, contact Bakul Patel at 301-796-5528 or by electronic mail at Bakul.Patel@fda.hhs.gov. For questions regarding this document concerning devices regulated by CBER, contact the Office of Communication, Outreach and Development (OCOD), by calling 1-800-835-4709 or 301-827-1800.

U.S. Department of Health and Human Services
Food and Drug Administration

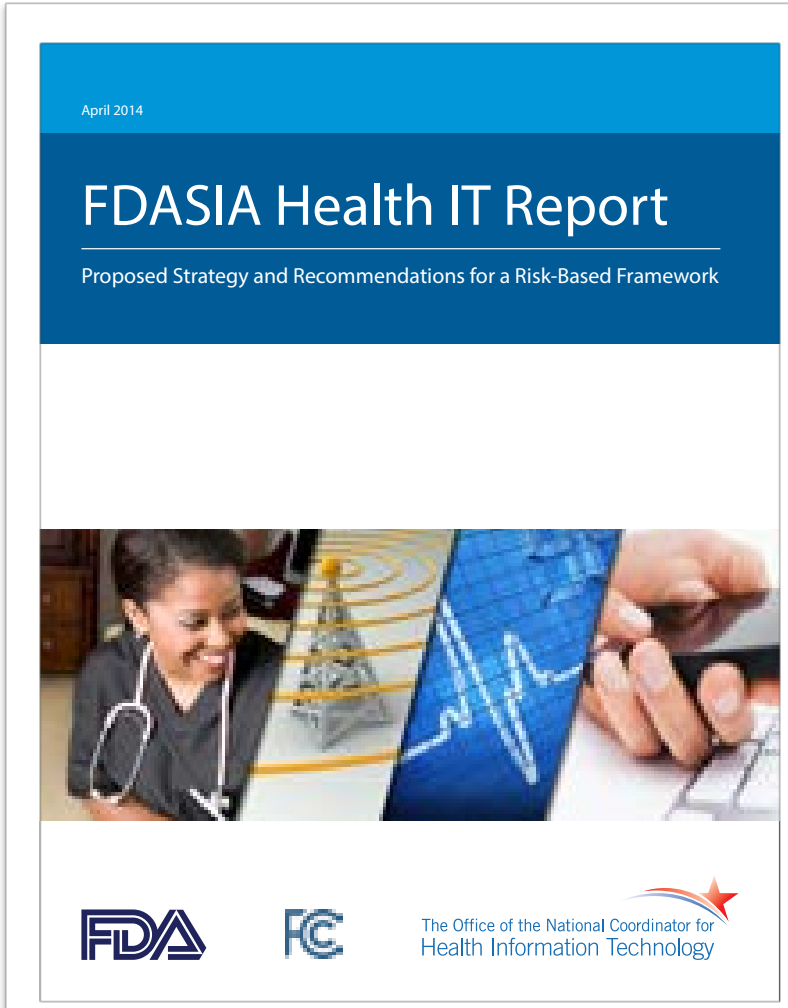
Center for Devices and Radiological Health

Center for Biologics Evaluation and Research

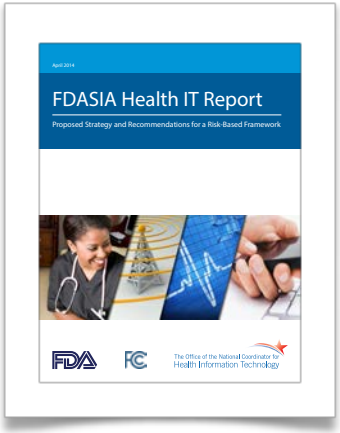
- 1 -

FDASIA 2014: multi-agency approach

- In 2012 law, Food and Drug Administration Safety and Innovation Act ("FDASIA"), Congress required the FDA, the ONC and the FCC to report back in 2014.
- Report: Agency oversight for Health IT should be based on the risk presented by a product's functionality.
- Report proposes the creation of a Health IT Safety Center in 2015.



FDASIA 2014: three categories



1. **Health IT with Administrative Functionality** presents limited or no risk to patient safety;
   - No agency will regulate these technologies.
2. **Health IT with Medical Device Functionality** has the potential to pose greater risk to patients if it does not perform as intended;
   - FDA will regulate these technologies.
3. **Health IT with Health Management Functionality** includes applications that are typically low- to medium-risk;
   - ONC will lead on regulating these technologies.

- Report charges FDA with clarifying the gray area between categories 2 and 3.

mHealth policy

Folder of materials (non-copyright public documents):

tinyurl.com/mHealthPolicy

TH&W

Summary

Take-away messages

- Health & wellness technology has tremendous potential
  - to increase quality, reduce cost, and improve access
- However, it also poses security & privacy challenges
- Trends in healthcare & technology drive these challenges
- Policy is in flux around HIT security/privacy and mHealth
- Many important research problems remain!

THaW mission

To enable the promise of health and wellness technology by innovating mobile- and cloud-computing systems that respect the privacy of individuals and the trustworthiness of medical information.

Follow us at **thaw.org**

Acknowledgements

- Collaborators include Denise Anthony, Kelly Caine (Clemson), Eric Chen, Cory Cornelius, Kevin Freeman (Clemson), Kevin Fu (UMich), Bhargav Golla (Clemson), Emily Greene, Carl Gunter (UIUC), Ryan Halter, Santosh Kumar (Memphis), Xiaohui Liang, Lorie Loeb, Sarah Lord, Shrirang Mare, Lisa Marsch, Andrés Molina-Markham (RSA Labs), Vivian Motti (Clemson), Travis Peters, Ron Peterson, Tim Pierson, Gunnar Pope, Aarathi Prasad, Avi Rubin (JHU), Joe Skinner, Jacob Sorber (Clemson), Jonathan Weiner (JHU), Tianlong Yun.

Institute for Security, Technology, and Society (ISTS)

Acknowledgements

- This research supported by
  - NSF awards TC-0910842, CNS-1314281, CNS-1329686
  - HHS ONC (SHARP program) award 90TR0003-01
- *The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.*

Institute for Security, Technology, and Society (ISTS)

Institute for Security, Technology, and Society at Dartmouth College

www.ists.Dartmouth.edu

www.cs.Dartmouth.edu

amulet-project.org

thaw.org