IS 2955 Special Topics: SAHI
Course Introduction and Overview
Lecture 1

James Joshi
Professor,
School of Computing and Information
Aug 29, 2018

Contact

- James Joshi
- 706A, IS Building
- Phone: 412-624-9982
- E-mail: jjoshi@pitt.edu
- Web: http://sis.pitt.edu/jjoshi/courses/IS2955/Fall18/
- Office hours: By Appointment or Drop by
- GSA/GSR: Runhua Xu (runhua.xu@pitt.edu)

Course objectives

- Understand the use/adoption of and impact of emerging technologies in healthcare and security and privacy challenges there of.
  - will specially focus on adoption of emerging technologies such as mobile computing, social networks, cloud/edge computing in healthcare and the cybersecurity challenges thereof.
- Understand *secure-by-design* approach to building next generation healthcare applications.
  - *Lab projects will aim towards*: building secure and privacy-aware health app that incorporates mobile technologies, cloud infrastructure, social networking platforms, etc.

Grading (tentative)

- Assignments, presentations, exam/quizzes: 60 – 70%
  - Read/Review and/or present research papers or articles
  - Assignments (HWs and Labs)
  - Participation in the class discussion
- Final project: 40 – 30%

Pre-requisite

- IS 2150/TEL 2810 Information Security & Privacy
  - OR background in security
- Following courses are preferred but not required:
  - IS 2170/TEL 2820 Cryptography; TEL 2821 Network Security
- OR - talk to me if you are not sure of the background
- Course Reference: Check website

Course Policy

- Your work MUST be your own
  - Zero tolerance for cheating/plagiarism
  - You get an F for the course if you cheat in anything however small – NO DISCUSSION
  - Discussing the problem is encouraged
- Homework
  - Penalty for late assignments (15% each day)
  - Ensure clarity in your answers – no credit will be given for vague answers
- Check webpage for everything!
  - You are responsible for checking the webpage for updates

Overview of Healthcare IT/Industry

Healthcare Ecosystem:

Healthcare and Public Health (HPH) Sector as a CI

Laboratories, Blood & Pharmaceuticals

Pharmaceutical Manufacturers
Drug Store Chains
Pharmacists' Associations
Public and Private Laboratory Associations
Blood Banks

Medical Materials

Medical Equipment & Supply Manufacturing & Distribution
Medical Device Manufacturers

Health Information Technology

Medical Research Institutions
Information Standards Bodies
Electronic Medical Record System and Other Clinical Medical System Vendors

Federal Response & Program Offices

Coordinated Response Activities Under Emergency Support Function 8 Government Coordinating Council
Federal Partners (e.g., HHS, DoD, other sector partners)

Direct Patient Care

Healthcare Systems
Professional Associations
Medical Facilities
Emergency Medical Services
Consumer Devices \ BYOD

Mass Fatality Management Services

Cemetery, Cremation, Morgue, and Funeral Homes
Mass Fatality Support Services (e.g., coroners, medical examiners, forensic examiners, & psychological support personnel)

Health Plans and Payers

Health Insurance Companies & Plans
Local and State Health Departments
State Emergency Health Organizations

Public Health

Governmental Public Health Services
Public Health Networks

Large .. Diverse .. Open

Vast, complex, public-private IT systems

Source: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Unique culture within HHS

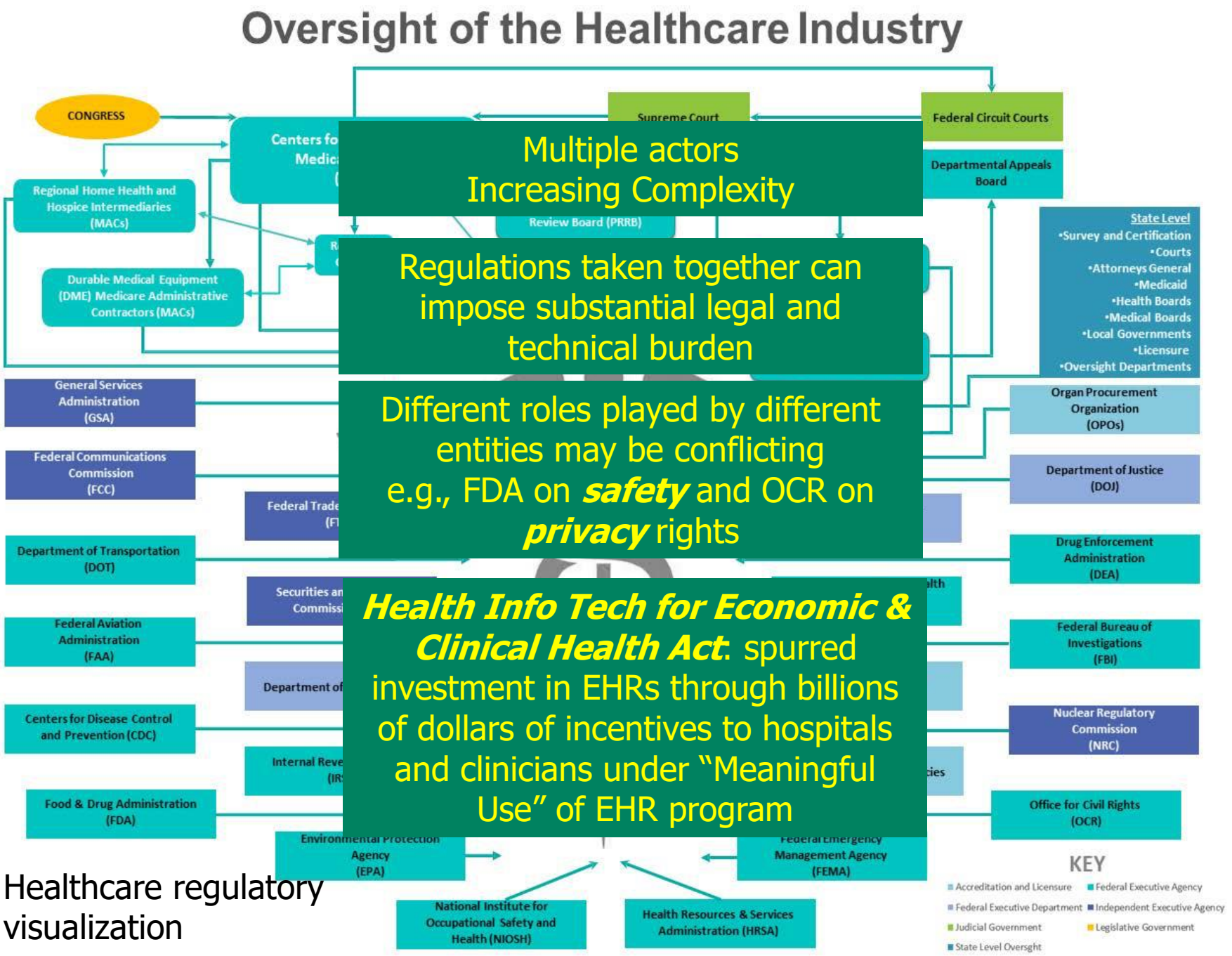
- Open, and sharing – towards mission
- Services provided to huge number of patients and related entities
- Need to access info quickly – makes staff make potential mistakes
  - E.g., leave workstations open
- Hospitals are public institutions – open!
- Staffs/Physicians change/rotate
  - All these impact Cybersecurity issues

Cybersecurity in Healthcare Industry

- Typically viewed as an IT Challenge
- Approached reactively
  - Not seen as protecting patients !!
- Limited financial resources
- A lot of legacy devices –
- Increasing connectivity – sensors, IoT devices
- Lack of understanding of cyber risks
- Limited education and awareness programs

Need organizational culture shifts and increased support and direction from leadership

A majority of healthcare sector made financial investments only in last five years



Healthcare regulatory visualization

Some key issues related security & privacy risks

- Healthcare data – does not change over time and value may increase
  - Reflected in price of medical records in dark web
  - Use when appropriate (job, when prominent, etc.)
- Potential for fraud (prescription medicine, insurance, medicare, etc.)
- Impacting safety and health, & social image
- Competitive disadvantage, brand damage, negative impact on confidence of patients, lawsuits, etc.

DARK WEB:
- Complete medical records: $60
- SSN: $5
- Stolen CC: $1-$3

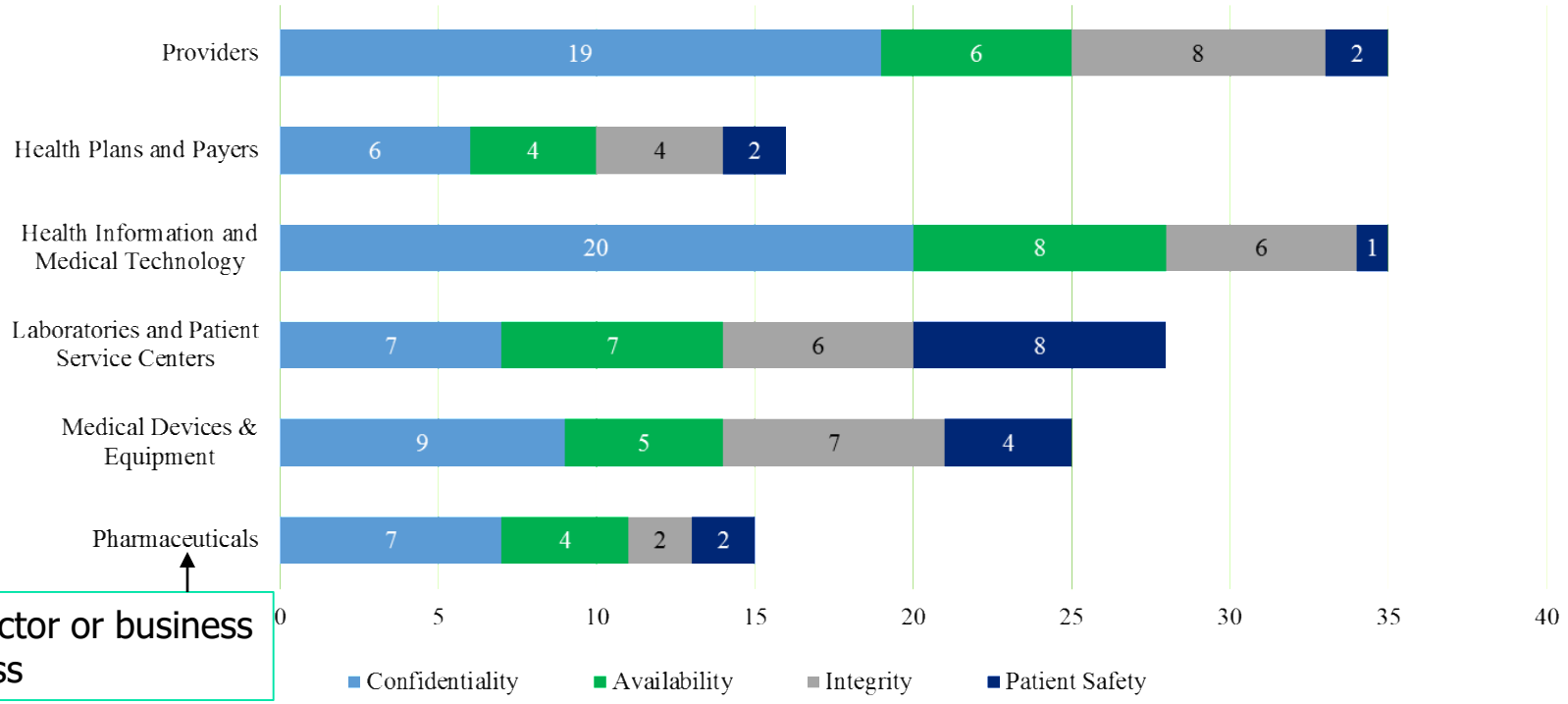
Medical Identity Theft: *"The info crime that can kill you"*
https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE_Spring15.pdf

Risk in Healthcare industry

- 2015 – HPH experienced more cybersecurity incidents resulting in data breach than any of the other 15 critical CI sectors
- Hospital ransomware attack is growing

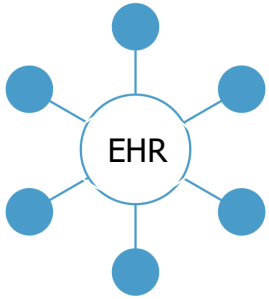
151 potential risks across the value chain
- 68 confidentiality (C) risks,
- 30 availability (A) risks,
- 30 integrity (I) risks, and
- 23 patient safety (PS) risks.

Figure 4 Health Care Subsector Risks across the Value Chain



Subsector or business process

Risks to EHR



- Regulatory mandates – will force all HER vendors to have a shared, publicly-available application interface
  - Goal – patients can use "third party applications" to gain access to their health data for improved service delivery
  - Can exacerbate cybersecurity – need secure interoperability!!
- "*EHR is the hub and connected devices are spokes*"
  - Complex mix of applications, programs, and interfaces from a variety of vendors
  - Attack surface increases!!
- Massive support and governance structure needed to support
  - patch management and
  - significant data flow change
  - connection to "spokes" which have their own software may be fragile

The ecosystem is as strong as the Weakest link

Risks to Networked environment & Medical Devices

- Increased attack surface because increased connectivity of medical devices
  - On the other hand provides opportunity for improving healthcare delivery
- Patients may be physically affected

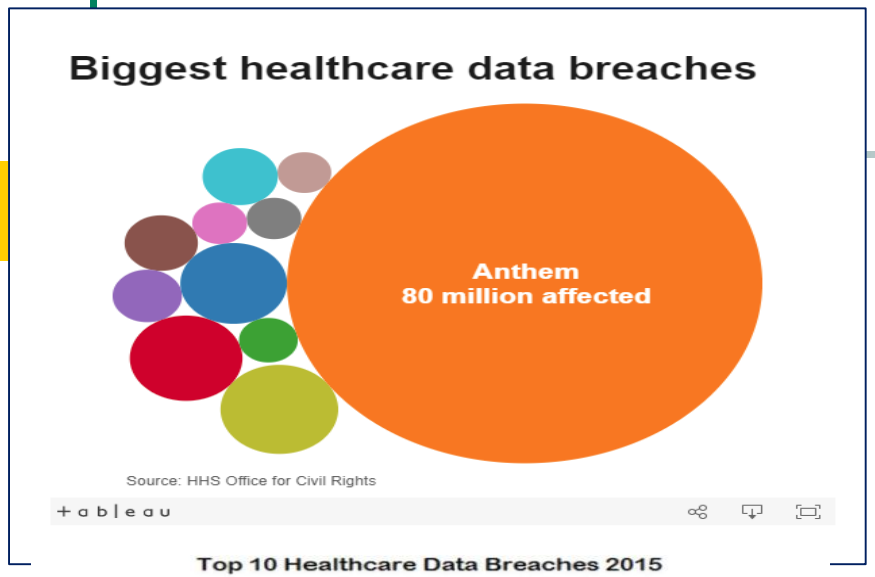
Table 1

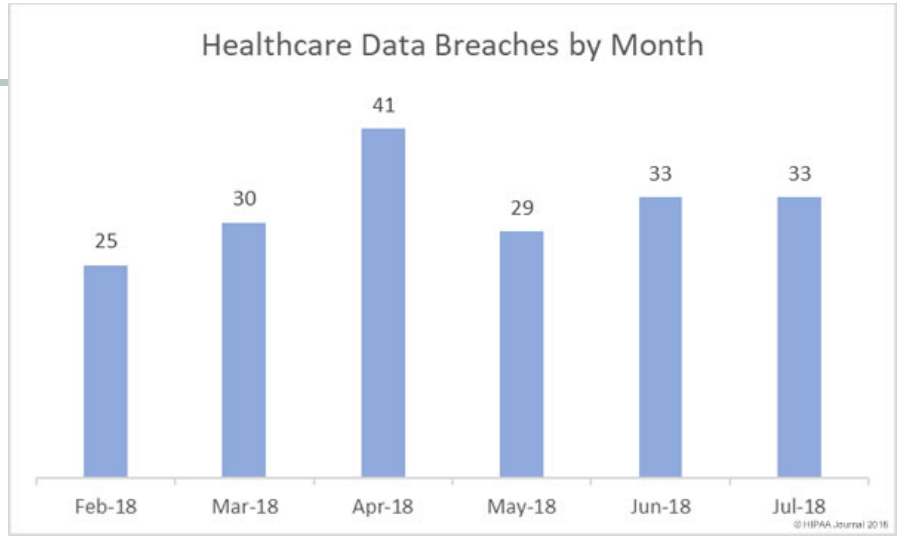
Risk Description	C	A	I	PS
Unauthorized access to the health care network, which allows access to other devices.	x	x	x	x
Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel).	x	x	x	x
Security vulnerabilities in off-the-shelf software due to poorly designed software security features.	x	x	x	x
Improper disposal of patient data or information, including test results or health records.	x			
Misconfigured networks or poor network security practices.	x	x	x	x
Open, unused communication ports on a device which allow for unauthorized, remote firmware downloads.	x	x	x	x

Recent Data Breaches in Healthcare from other sources

In 2018

https://www.hipaajournal.com/july-2018-healthcare-data-breach-report/

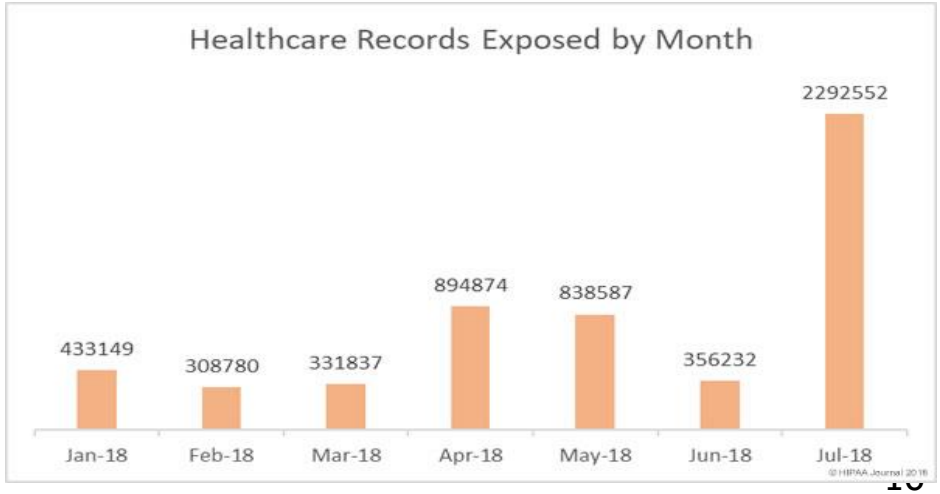




July 2018 impacted 2,292,552 patients (543.6% more than in June) – worst in 2018 so far

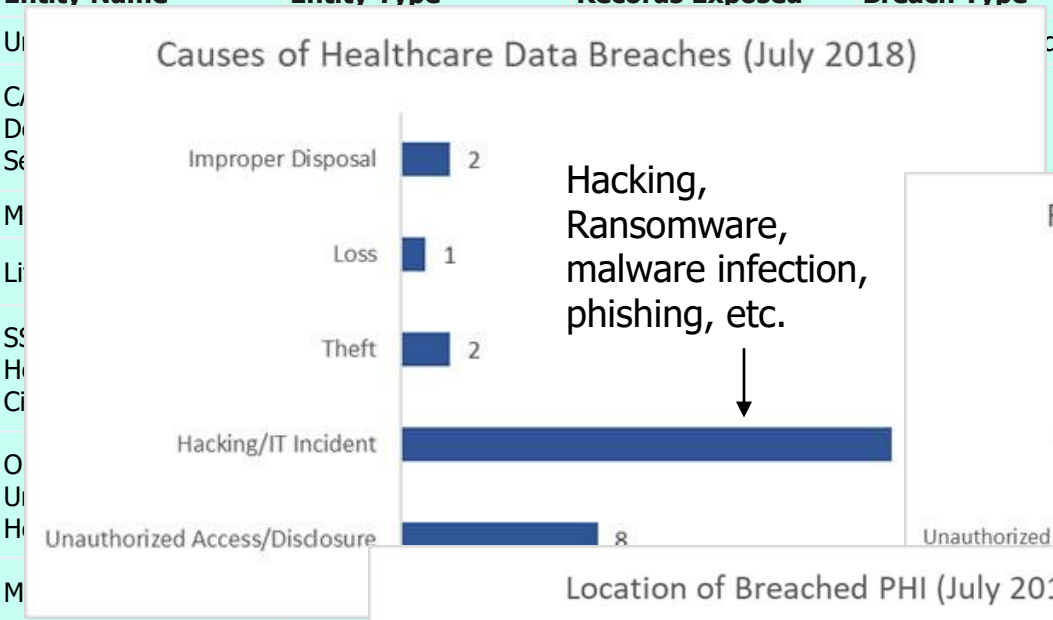
Top 10 Healthcare Data Breaches 2015

Organization	Records Breached	Type of Breach
Anthem	78,800,000	Hacking / IT Incident
PREMERA BLUE CROSS	11,000,000	Hacking / IT Incident
Excellus	10,000,000	Hacking / IT Incident
UCLA Health	4,500,000	Hacking / IT Incident
mie	3,900,000	Hacking / IT Incident
CareFirst	1,100,000	Hacking / IT Incident
DMAS	697,586	Hacking / IT Incident
Georgia Department of Community Health	557,779	Hacking / IT Incident
BEACON HEALTH SYSTEM	306,789	Hacking / IT Incident
DJO GLOBAL	160,000	Laptop Theft
2015 Total	111,022,154	(almost 35% U.S. population)

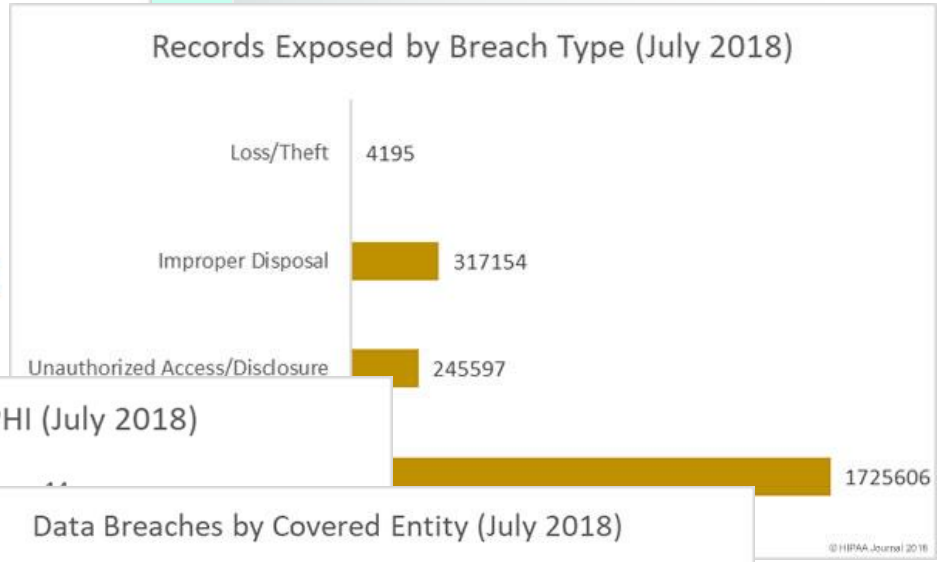


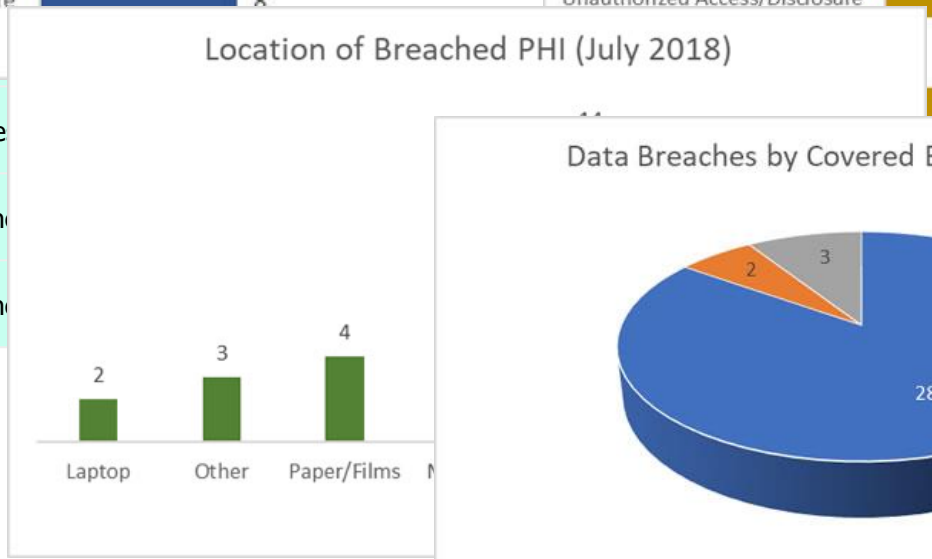
Largest Healthcare Data Breaches of 2018 (Jan-July)

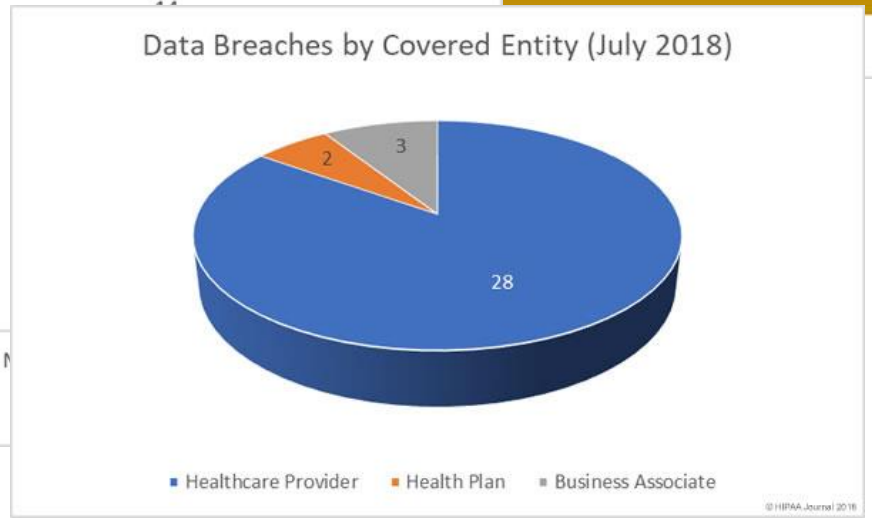
Entity Name	Entity Type	Records Exposed	Breach Type
MedEvolve	Busine		
St. Peter's Surgery & Endoscopy Center	Health		
Boys Town National Research Hospital	Health		



Hacking, Ransomware, malware infection, phishing, etc.







https://www.hipaajournal.com/july-2018-healthcare-data-breach-report

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

All these contribute to increased risk

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

Source: Healthcare Industry Cybersecurity taskforce June 2017

Risk Management Approach (Macro-level)

Uses NIST CSF:
- identify
- Protect
- Detect
- Respond &
- Recover

Not specific to Healthcare !!

FDA, ONC, OCR guidance important

Task force recommendation

Six high-level imperatives ***that must be achieved to address cybersecurity in Healthcare***

- Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
- Increase the security and resilience of medical devices and health IT.
- Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
- Increase health care industry readiness through improved cybersecurity awareness and education.
- Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.
- Improve information sharing of industry threats, weaknesses, and mitigations.

$158.7 B Invested in Healthcare R&D In 2015 →

Each imperative has a set of Recommendations !

Each recommendation has a set of Actions !

Imperative 2:Increase the security and resilience of medical devices and health IT.

Recommendations

- 2.1: Secure legacy systems.
- 2.2: Improve manufacturing and development transparency among developers and users.
- 2.3: Increase adoption and rigor of the secure development lifecycle (SDL) in the development of medical devices and EHRs.
  - Risk management in each phase is key !!
- 2.4: Require strong authentication to improve identity and access management for health care workers, patients, and medical devices/EHRs.
  - Trust !!
  - Device-device authentication – support interoperability
  - NIST 800-46 for remote access – interoperation with external system; includes use of tw0-factor authentication
- 2.5: Employ strategic and architectural approaches to reduce the attack surface for medical devices, EHRs, and the interfaces between these prod
- 2.6: Establish a Medical Computer Emergency Readiness Team (MedCERT) to coordinate medical device-specific responses to cybersecurity incidents and vulnerability disclosures.

Overview of Privacy and HIPAA

First – recap of "Privacy"

- Hard to define
- "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"
  - Alan Westin, Privacy and Freedom, 1967

OECD Guidelines on the Protection of Privacy (1980)

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2

FTC Fair Information Practice Principles

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress

(http://www.ftc.gov/reports/ … find documents)

(OR: https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/)

EU's General Data Protection Regulation

EU's Data Protection Directive

HIPAA

- Health Insurance Portability & Accountability Act Of 1996 (HIPAA),
  - also known as the Kennedy-Kassebaum Act
  - Protects confidentiality and security of health care data by establishing and enforcing standards and standardizing electronic data interchange
  - Requires organizations that retain health care information to use information security mechanisms to protect this information, as well as policies and procedures to maintain them
  - Requires comprehensive assessment of organization's information security systems, policies, and procedures

HIPAA (Continued)

- Five fundamental privacy principles:
  - Consumer control of medical information
  - Boundaries on the use of medical information
  - Accountability for the privacy of private information
  - Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
  - Security of health information

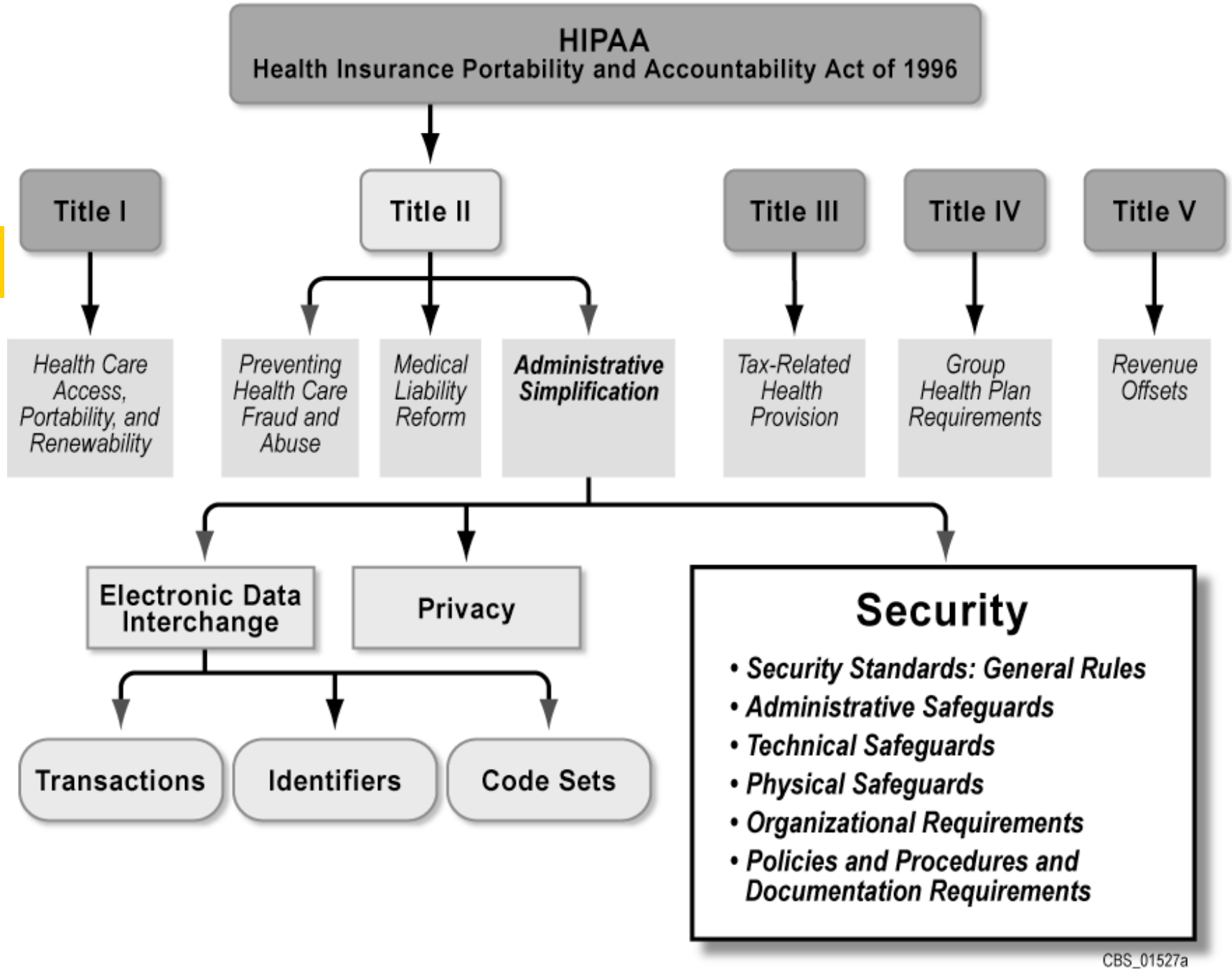


Figure 1. HIPAA Components

HIPAA Rules

- **HIPAA Rules**: provide federal protections for patient health information held by *Covered Entities* (CEs) and *Business Associates* (BAs) and give patients an array of rights with respect to that information.
  - **Privacy Rule** -- protects the privacy of individually identifiable health information;
  - **Security Rule** -- sets national standards for the security of *electronic Protected Health Information* (ePHI); and
  - **Breach Notification Rule**-- requires CEs and BAs to provide notification following a breach of unsecured Protected Health Information (PHI).

CEs must comply with these.

BAs must comply with the HIPAA **Security Rule** and **Breach Notification Rule** as well as certain provisions of the HIPAA Privacy Rule.

Reading: Guide to Privacy and Security of Electronic Health Information
https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

HIPAA

- CEs include
  - ***Health care providers*** who conduct certain standard administrative and financial transactions in electronic form,
  - ***Health plans***: Individual and group plans that provide or pay the cost of medical care
  - ***Health care clearinghouses***: entities that process nonstandard information they receive from another entity into a standard

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Covered Entities Guidance:
https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf

HIPAA: Business Associate

- **Privacy rule** - allows CEs to share to disclose PHI to BAs if they provide appropriate assurances
- BA is:
  - "person or entity, other than a workforce member (e.g., a member of your office staff), who performs certain functions or activities on your behalf, or provides certain services to or for you, when the services involve the access to, or the use or disclosure of, PHI."
    - **BA functions or activities include**: claims processing, data analysis, quality assurance, certain patient safety activities, utilization review, and billing
  - **Examples**:
    - Health Information Organizations or Exchanges (HIOs/HIEs);
    - An entity that a CE contracts with to provide patients with access to a Personal Health Record (PHR) on behalf of a CE

Patients Rights under HIPAA

- Notice of privacy practices (NPP)
- Patient Access to Information (within 30 days of request)
- Amending Patient Information (within 60 days of request)
  - Can file "statement of disagreement"
- Accounting of Disclosures (limited)
  - Not needed for ones made for treatment, payment, operations and other purposes.
- Rights to Restrict Information (use and disclosure)
- Rights to confidential communications
  - Receive communications by means and from locations patients specify

Designated Record Set – is a group of records CE or BA maintains to make decisions about individuals (e.g., medical and billing records)

HIPAA Privacy Rule

- Privacy Rule
  - Protects most individually identifiable health information held by a CE and BA – called PHI (Protected Health Information) related to
    - Demographic information
    - The individual's past, present, or future physical or mental health or condition,
    - The provision of health care to the individual, or
    - The past, present, or future payment for the provision of health care to the individual.

Also - identifies the individual OR there is a reasonable basis to believe it can be used to identify the individual

List of 18 Identifiers

1. Names;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

HIPAA Privacy Rule

- Establishes national standards for the protection of certain health information.
- The Privacy Rule standards address
  - "the use and disclosure of PHI as well as standards for individuals' privacy rights to understand and control how their health information is used and shared, including rights to examine and obtain a copy of their health records as well as to request corrections"
  - "limits Uses and Disclosures of Patient Information "
- Rules related to
  - Permitted Uses and Disclosures, etc. (Usage and Disclosure related)
  - Notice and Other Individual Rights
  - Administrative requirements – policies and procedures

(Check for more info: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)

HIPAA Security Rule

Establishes national set of minimum security standards for protecting all ePHI that a CE /BA create, receive, maintain, transmit.

Six main sections

- **Security standards: General Rules**
  - general requirements all CEs must meet;
  - establishes flexibility of approach;
  - identifies standards and implementation specifications (both required and addressable);
  - outlines decisions a CE must make regarding addressable implementation specifications; and
  - requires maintenance of security measures to continue reasonable and appropriate protection of **electronic *protected health information***.
    - Ensure the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits;
    - Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI; and
    - Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

HIPAA Security Rule

- Administrative Safeguards
  - "administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."
- Physical Safeguards
  - physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

HIPAA Security Rule

- Technical Safeguards
  - the technology and the policy & procedures for its use that protect electronic protected health information and control access to it
- Organizational Requirements
  - includes standards for business associate contracts and other arrangements, including memoranda of understanding between a CE and a business associate when both entities are government organizations; and requirements for group health plans.

HIPAA Security Rule

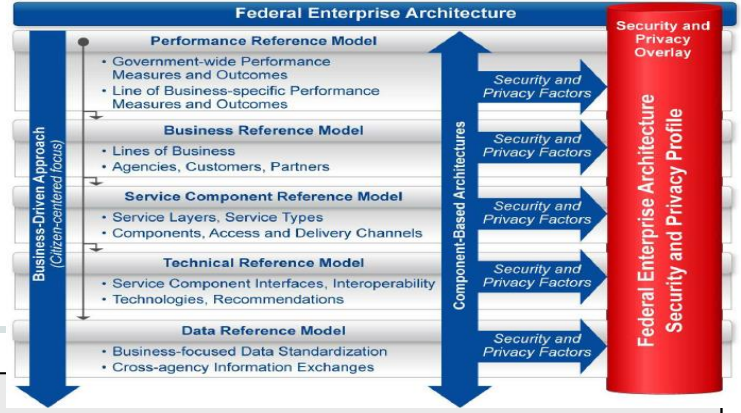
- Policies and Procedures and Documentation Requirements
  - Requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule;
  - maintenance of written (which may be electronic) documentation and/or records that includes policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation.

NIST 800-66R1 on HIPAA

- HIPAA Security Rule is all about effective risk management
- Assessment, analysis of risk is foundation for CEs compliance efforts

Can apply:

NIST-RMF



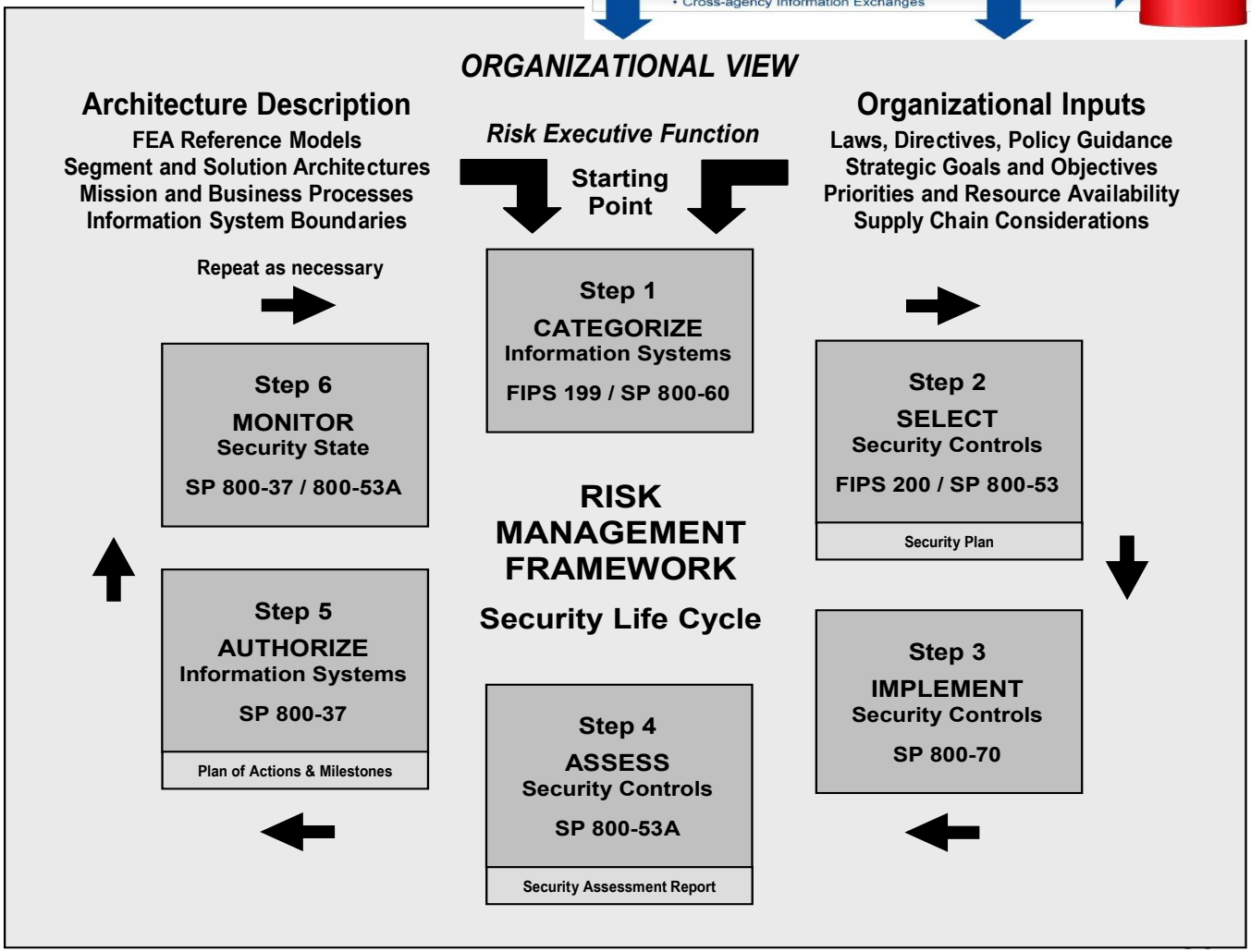


Table 2: Linking the NIST RMF and the Security Rule

RMF Phase	RMF Step Description	Security Rule Link
Categorize Information Systems	Security categorization, the first and arguably the most important step in the RMF, employs FIPS 199 and NIST SP 800-60 to determine the criticality and sensitivity of the	Identify assets and information systems that create, receive, transmit, or maintain EPHI.
	organizational requirements, and environments of operations; and □ Supplementation of tailored baseline security controls with additional controls based on an assessment of risk and local conditions including specific and credible	the security control baseline should be based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances. The agreed-upon set of security controls will consist of the
Select Security	Assess Security Controls	Security Controls Assessment, the fourth step in the RMF, employs NIST SP 800-53A to evaluate the information system security controls for effectiveness using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security objectives and requirements for the system.	Evaluate the implemented specifications using assessment methods and procedures to determine the extent to which the controls are implemented correctly and operating as intended with respect to protecting EPHI. *Related Standards and Implementation Specifications:* 164.308(a)(8) – Evaluation
	Authorize Information System	Authorize information system operation (with implemented security controls) based upon a determination of the risk to organizational operations, organizational assets, individuals, and other organizations, and an explicit decision to accept this risk.	Inherent in any risk management process is the acceptance of those identified risks that are deemed acceptable to the organization. *Related Standards and Implementation Specifications:* 164.308(a)(1)(ii)(B) – Risk Management
Implement Secu	Monitor Security State	Threats and vulnerabilities to an operating environment, as well as safeguards designed to combat them, can change frequently. The assessment and evaluation of security controls on a continuous basis provides oversight and monitoring of the security controls to ensure that they continue to operate effectively and as intended. Monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the system security status to appropriate organizational officials on a regular basis.	A covered entity must periodically review and update its security measures and documentation in response to environmental and operational changes that affect security of its EPHI. *Related Standards and Implementation Specifications:* 164.308(a)(8) – Evaluation 164.308(a)(1)(ii)(D) – Information System Activity Review

Administrative Safeguards

- **Security Management Process**: <HIPAA Standard:> Implement policies and procedures to prevent, detect, contain, and correct security violations.
- **Assigned Security Responsibility**: <HIPAA Standard:> Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
- **Workforce Security**: <HIPAA Standard:> Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, as provided [under paragraph … of this section] from obtaining access to ePHI.
- **Information Access Management**: <HIPAA Standard:> Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of subpart E of this part.
- **Security Awareness and Training:** <HIPAA Standard:> Implement a security awareness and training program for all members of its workforce (including management)
- **Security Incident Procedures**: <HIPAA Standard:> Implement policies and procedures to address security incidents
- **Contingency Plan**: <HIPAA Standard:> Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.
- **Evaluation**: <HIPAA Standard:> Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
- **BA Contracts and Other Arrangements:** <HIPAA Standard:> A CE, in accordance with§164.306, may permit a BA to create, receive, maintain, or transmit ePHI on the CE's behalf only if the covered entity obtains satisfactory assurances, in accordancewith§164.314(a), that the BAwill appropriately safeguard the information

Physical Safeguards

- **Facility Access Controls**: <HIPAA Standard:> Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
- **Workstation Use**: <HIPAA Standard:> Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.
- **Workstation Security**: <HIPAA Standard:> Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
- **Device and Media Controls**: <HIPAA Standard:> Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility

Technical Safeguards

- **Access Control**: <HIPAA Standard:> Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
- **Audit Controls**: <HIPAA Standard:> Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- **Integrity**: <HIPAA Standard:> Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
- **Person or Entity Authentication**: <HIPAA Standard:> Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one
- **Transmission Security**: <HIPAA Standard:> Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network

Organizational Requirements

- **Business Associate Contracts or Other Arrangements**: (i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.

- **Requirements for Group Health Plans**: Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

Policies and Procedures and Documentation Requirements

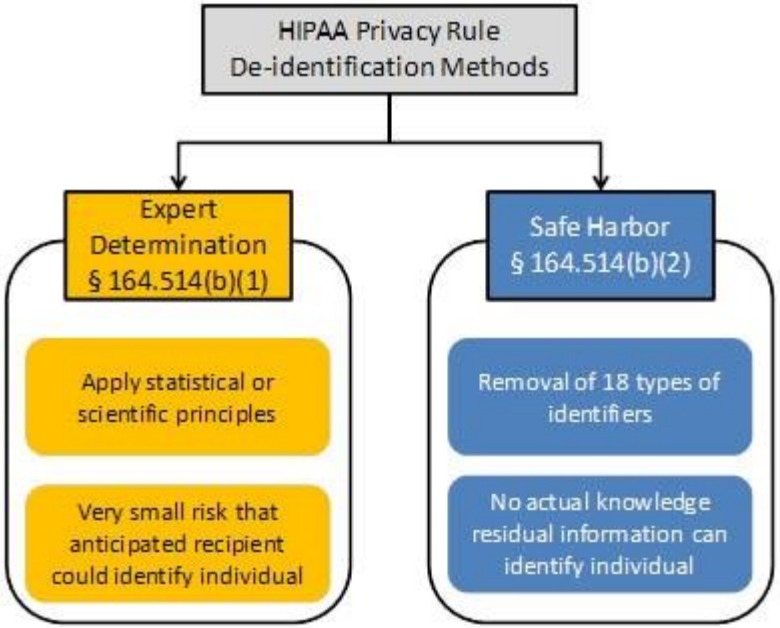
- **Policies and Procedures:** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
- **Documentation**: (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

Other regulatory components

- FDA (Food & Drug Administration)
  - charged with ensuring approved and cleared medical devices are safe and efficacious – including those from cybersecurity risks
- OCR (Office for Civil Rights)
  - charged with oversight of the privacy and security regulations under HIPAA, which applies only to "covered entities" (e.g., most health care providers, health plans, and health care clearinghouses), and contractors acting on their behalf, known as "business associates."

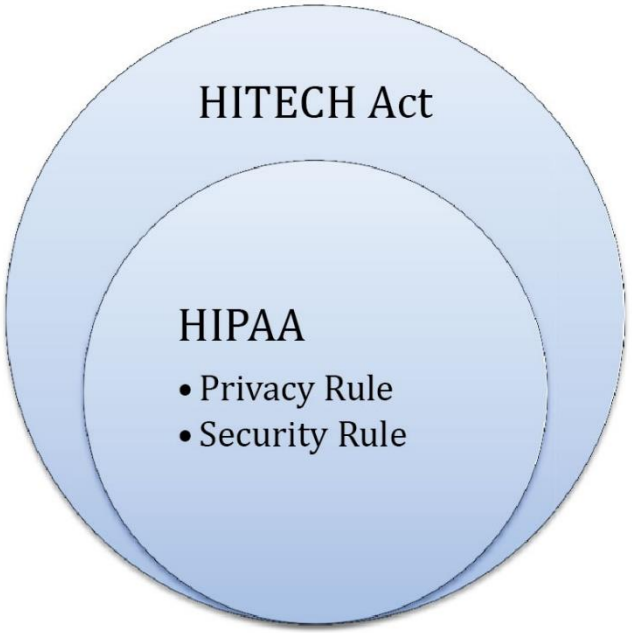
Protection & Confidential Handling of Health Information

- HIPAA
  - The Privacy Rule
  - The Security
  - The Omnibus Final Rule; includes:
    - Enforcement Rule and the Breach Notification Rule
  - The HITECH Act
- PHI → 18 identifiers



The American Recovery and Reinvestment Act (ARRA) of 2009

- After great recession!!
- Most significant changes
  - The final breach notification rule
  - Updates to business associate responsibilities
  - Expansion of penalty consequences
  - Investigative authority for potential violations to the Attorney General of each state

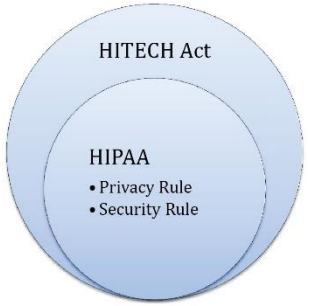


OCR

"The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules."

Strengthens HIPAA

HITECH Act



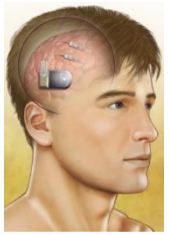
- Expands Administrative Simplification provision and added business associates to the list of those who are directly culpable for compliance to HIPAA
- OCR took control of enforcement of HIPAA vis the HITECH Act – dramatic effect
- HITECH requires
  - Business associate to implement each of the CIA safeguards under the HIPAA Security Rule that already applied to covered entities
  - Also imposes new requirements for covered entities to limit disclosures of PHI "to the extent practicable" to limited data set or, if needed by the CEs, to the min necessary to accomplish the intended purpose
  - Also changes to HIPAA –
    - Providing individuals with right to obtain PHI in e-format,
    - Enhancing fines and penalties for breaches
    - Dramatically changes the definition of "breach" as – an acquisition, access, or disclosure of unsecured PHI that is not otherwise permitted under HIPAA that compromises the security and privacy of PHI

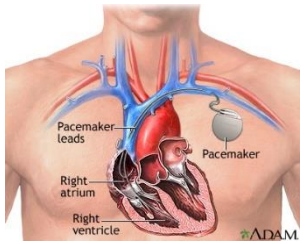
HITECH Act

- HIPAA Beach Notification – did not exist prior to HITECH Act
  - One of the most drastic change!!
  - Any breach that impacts 500 or more individuals – needs to be reported
- Scope of CEs also clarified to include business associates such as
  - Billing providers
  - Health information exchanges
  - Software companies
  - Cloud computing providers
  - In some cases Banks
- Safe harbor in HITECH for encrypted info
  - If the info breached was encrypted with certified FIPS 140-2 encryption – the breach does not have to be reported
- Provides funding for auditors to review the security practices of covered entities in US

Paradigm Shift in Health care:
Anywhere anytime, personalized health

Continuous Monitoring and On-time intervention





in-body/out-body implantable/ wearable devices, sensors

- *Anywhere*, *Anytime* Personalized Healthcare/medicine

Enablers

- Medical devices, IoT & Sensor technologies
- Mobile and Web technologies,
- Social networking, Cloud computing, Location based services
- Big Data analytics – AI, ML, ….

Integrated Care

Self-care

Many value added features/services

Social Support

mHealth App Spectrum

Simple ⟷ *Complex*

Single use mHealth

Focuses on a single purpose for a single user, typically consumer initiated:

- smartphone apps and wearable tech products that support the user to record data which may be communicated to others
- consumer driven, focus on wellness, diet and exercise.

Fitness tracker, weigh loss apps

Social mHealth

Draws upon the support and encouragement provided through social networks:

- gamification and competition based apps which encourage users to meet goals
- consumers likely to pursue activities independently.

Fitness tracker sharing vis a SN

Integrated mHealth

Links apps and devices with the formal healthcare system:

- mobile technology linking patients and HCPs
- tailored to multiple end users: consumers, physicians and administrators.

Information from multiple apps that a patient uses is incorporated into the patients overall health record, giving a physician a more complete view

Complex mHealth

Leverages advanced, integrated analytics for decision support:

- predictive analytics applied to complex data generated through mHealth applications
- focus on achieving optimal management of a specific disease.

Data mining using algorithms to analyze data collected via mobile devices to deliver insights on an individual's patterns of behavior for individual health management purposes. Data analysis oriented towards improving public health responses through analysis of sub-populations with different risk profiles and appropriate targeting of public health interventions

Source: Four Dimensions of Effective mHealth, Deloitte US Center for Health Solutions, 2014

mHealth App market
10 takeaways

325,000 health apps
available in 2017
78,000 new health apps
added to major app stores in the last year
Android overtaking Apple
in numbers of available health apps
84,000 health app publishers
releasing apps
Gap of demand and supply widening
with high number of developers, low downloads growth rates
$5.4bn investment into digital health start-ups
fueling the market

3.6bn apps will be downloaded
by users in 2017 (estimated)
18% not developing health apps
due to uncertain regulations
Insurers are the #1 future distribution channel
53% of digital health practitioners expect health insurances to be future distribution channel with best market potential
28% pure digital market players
in the digital health industry

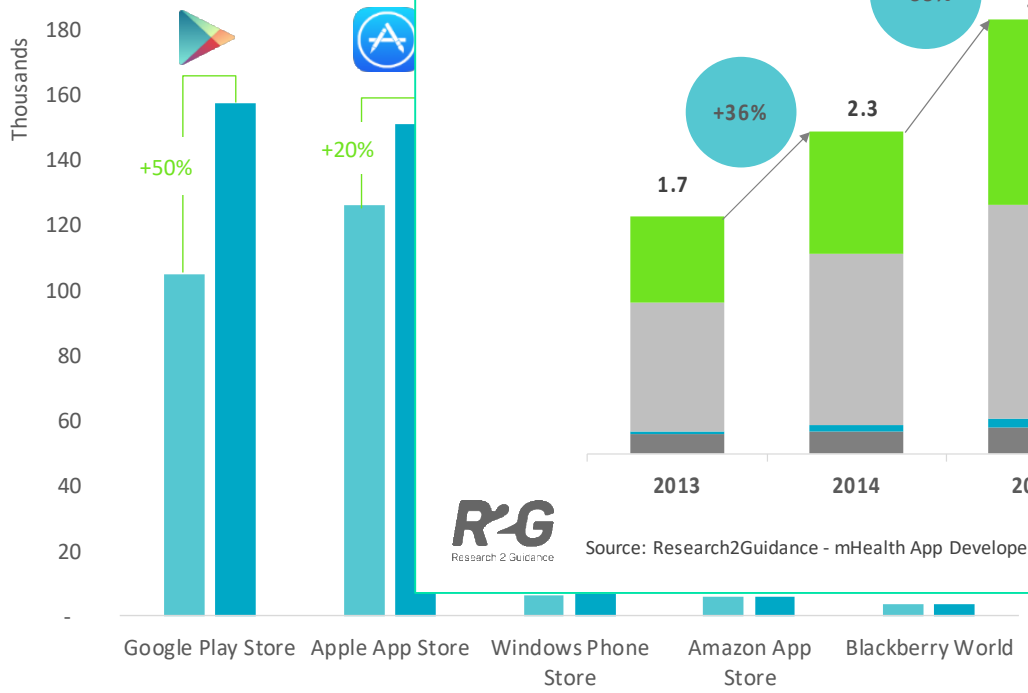
Source: mHealth App developer survey economics 2017/2018

mHealth App market

325,000 mHEALTH APPS AVAILA

NUMBER ONE FOR HEALTHCARE A

Number of mHealth apps displayed in App St

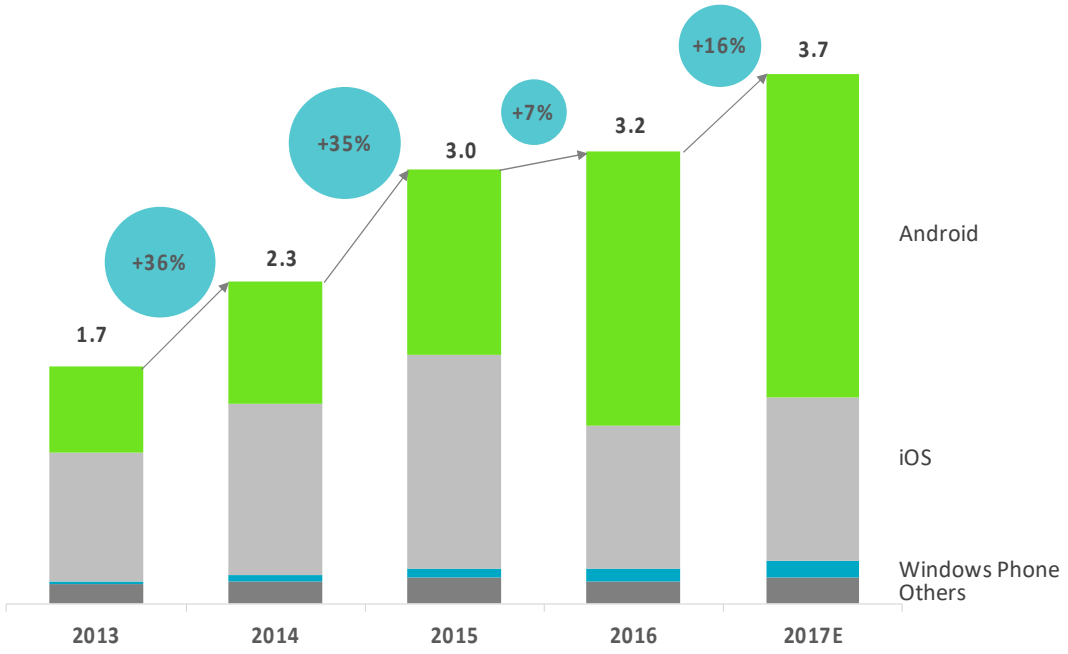


Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

3.7 BN HEALTH APPS WILL BE DOWNLOADED IN 2017

BIGGEST SHARE COMES FROM ANDROID

Estimated total downloads of mHealth apps (billions)



Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

Diverse mHealth publishers

DIGITAL INTRUDERS: TH
PURELY DIGITAL MARKET

Your organization is best describe

Gover
Education/Training compar
Non-profit organization (NGO) 3
University 4%
Telecommunications 1%
App developer/ Agency 4%
Consultancy/ Market research company 5%
IT/Tech company 13

Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

AI SEEN AS THE MOST DISRUPTIVE TECHNOLOGY; SUCCESSFUL APP PUBLISHERS ARE GENERALLY MORE BULLISH ABOUT NEW TECHNOLOGIES

Most disruptive technologies to the data health sector within the next five years

*Successful publishers = >1M USD revenue and max 500 employees

Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

SUPPLY IS OUTGROWING DEMAND – GROWTH RATE OF APP PUBLISHERS IS HIGHER THAN ANNUAL DOWNLOAD GROWTH RATE OF MHEALTH APPS

Number of dow

80,000

60,000

40,000

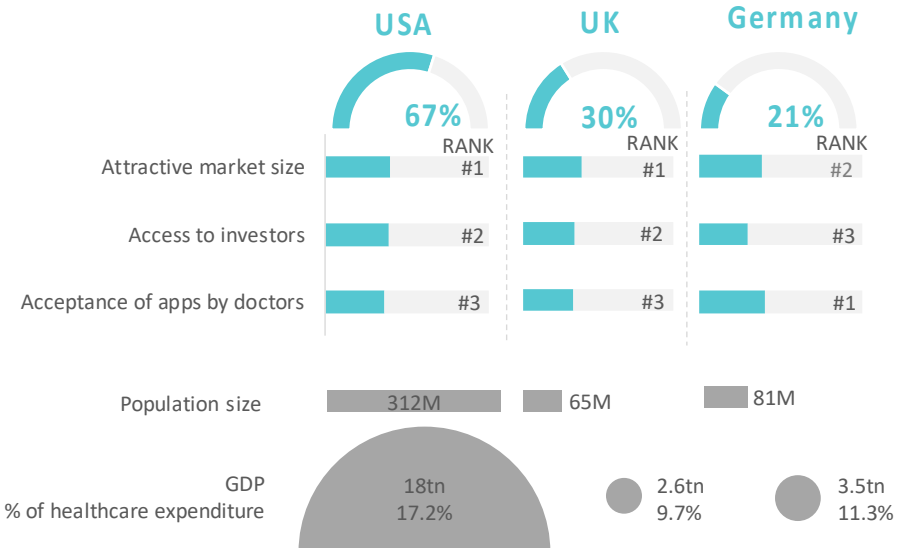
20,000

-

Source

USA, THE UK AND GERMANY ARE THE MOST ATTRACTIVE COUNTRIES FOR DIGITAL HEALTH SOLUTIONS – MARKET SIZE IS MOST IMPORTANT FACTOR

Countries currently offering the most favorable environment for digital health solutions; reasons for most favorable environment; population size; GDP and % of health expenditure of GDP



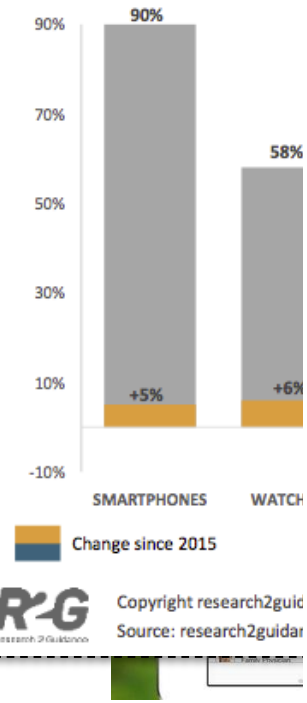
Top 15 countries

Rank	Country	%
1	USA	67%
2	UK	30%
3	Germany	21%
4	Israel	16%
5	Canada	14%
6	The Netherlands	12%
7	Denmark	12%
8	India	11%
9	Sweden	10%
10	China	8%
11	Finland	8%
12	Switzerland	7%
13	Estonia	6%
14	Spain	6%
15	Norway	5%

Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

SMARTPHONES REMAIN THE MAIN PREFERRED DEVICE FOR MHEALTH APPS

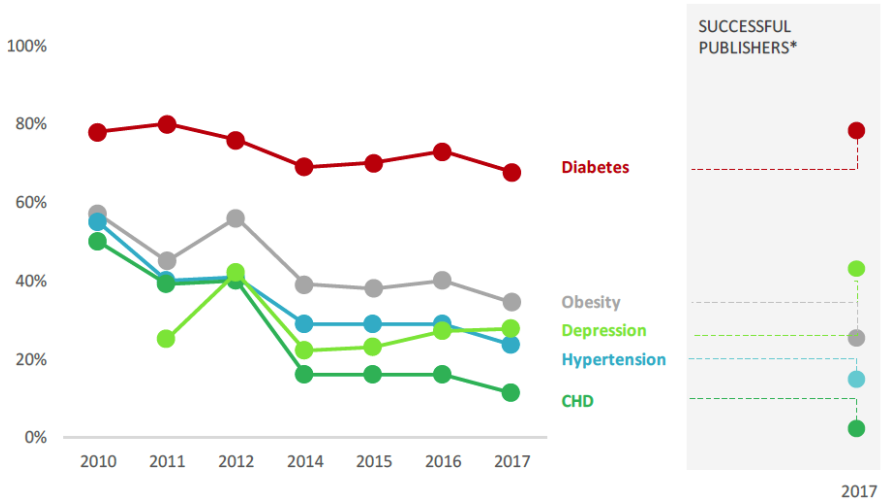
Which devices offer the best market potential for mHealth in the next 5 years?



"depression". Depression is now ranked third as having the best market potential.

DIABETES REMAINS THE LEADING THERAPY FIELD FOR MHEALTH SOLUTIONS; DEPRESSION AS FIELD FOR MHEALTH ON A STEADY RISE

Therapy fields with the best market potential for mHealth in the next 5 years



Note: Study wasn't conducted in 2013.

*Successful publishers = >1M USD revenue and max 500 employees

Source: Research2Guidance - mHealth App Developer Economics study 2017 - n = 2,400

Source: https://www.pcmag.com/art

Source:mHealth App developer su

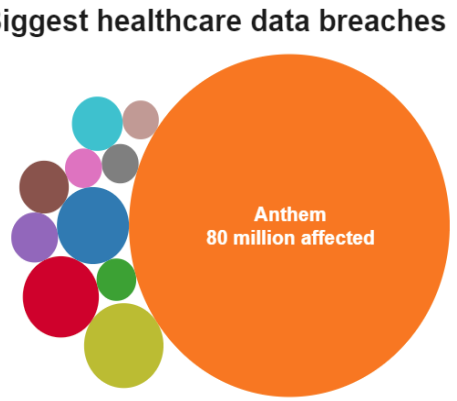
Successful mHealth app publishers have a slightly different opinion about the future best therapy

But … Security & Privacy significant concerns

Privacy and Security are the most important concerns

Healthcare is ar vulnerable industr

David Kotz et.al, "Privacy and Security in Mobile Health: A Research Agenda,



"57% of consumer .. report being skeptical of the overall benefits of health information technologies such as patient portals, mobile apps, and electronic health records mainly because of recently reported data hacking and a perceived lack of privacy protection by providers"

"The unwillingness of patients to comprehensively divulge all their medical information rose to 87 percent in the fourth quarter of 2016"

Alarming: Users are concerned " … that their pharmacy prescriptions (90 percent), mental health notes (99 percent) and chronic condition (81 percent) data is being shared beyond their chosen provider and payer to retailers, employers, and or the government without their acknowledgement."
(**as per a Black Book survey**)

Security and Privacy Issues/Challenges

- At-large

Enablers

- Medical devices, IoT & Se
- Mobile and Web technolog
- Social networking, Cloud c Location based services
- Big Data analytics – AI, M

Inherit all their

Levera

Security & Privac Healthcare IT

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

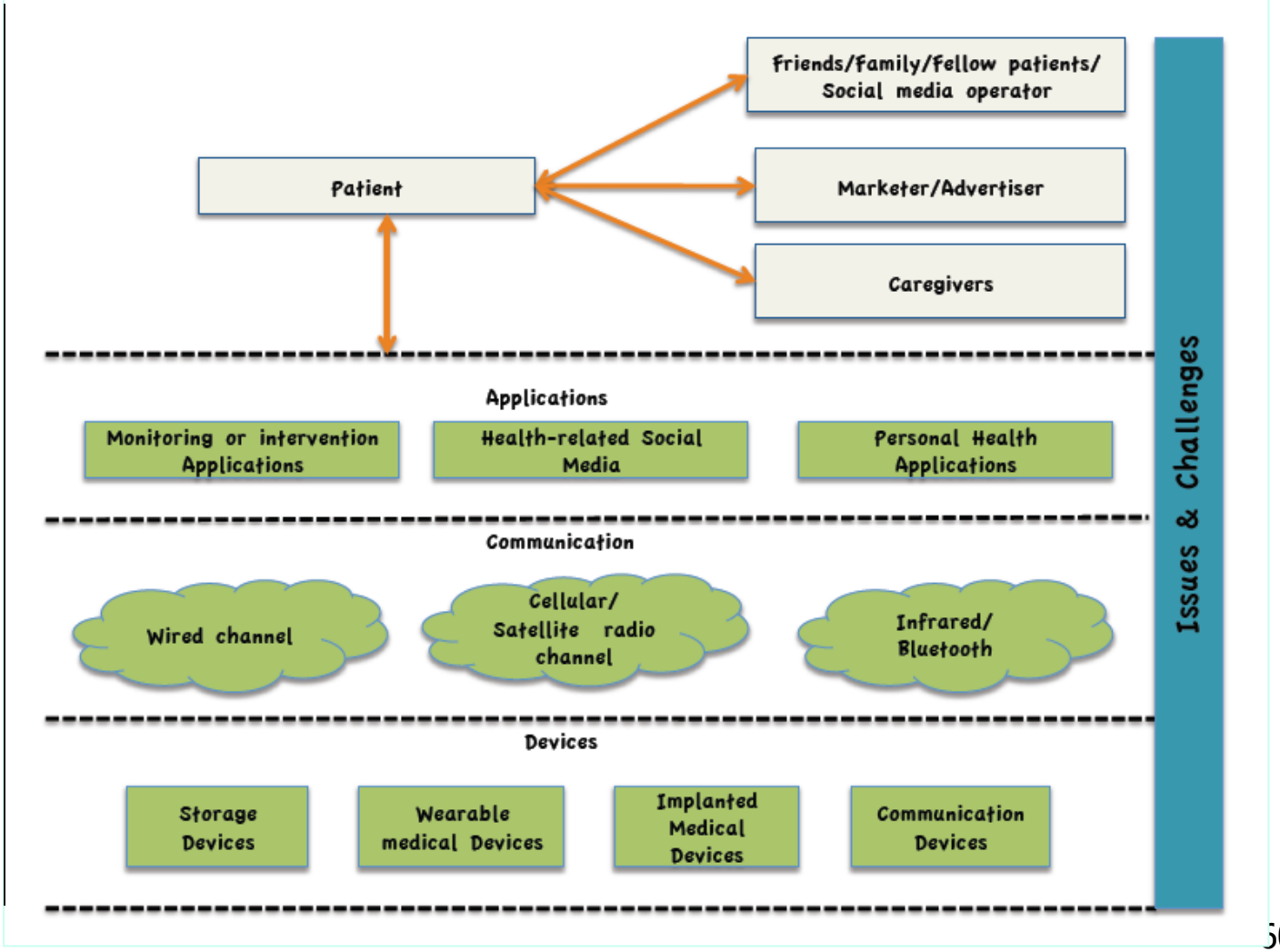
Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

Source: Healthcare Industry Cybersecurity taskforce June 2017

Security and Privacy Issues/Challenges

Laws, Regulations, Policies

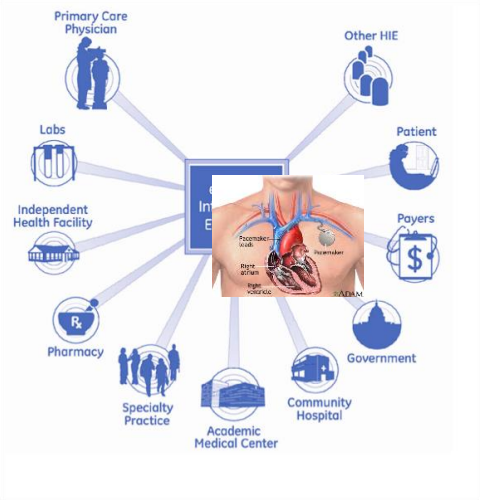


Security and Privacy Issues/Challenges

		Issues	Security problems	Approaches	Challenges
	User Plane Demographics, Health condition, Physical ability, Mental ability	Demographic profiles and physical & mental abilities of patients are not the same.	- Attacks using non-technical and unintentional vulnerabilities - Targeted attacks on patients with certain characteristics	Human and social factor analysis	- Rich & diverse privacy & security requirements - Security solutions are challenged by human and social factors
Legacy / Mobile / Cloud Infrastructure	**Application Plane** EMR, Tele-Health apps, Personal Health Apps (PHR mgmt, tracking), Health-related social media (OSN, VC)	- Health records are fragmented and dispersed in many facilities - In Tele-Health, a mosaic of applications work with each other, creating a highly collaborative environment - Personal health apps collect extraneous personal info - Quality of information in social media is highly variable	- De-anonymization and inference attacks by linking different data trails - Many possibilities of unauthorized access and identity theft - Social engineering attacks cripple social support systems	- Testing and certification - Design-by-contract - Principle of least privilege - Access control - Data Masking - Cryptographic protocols - Education and training	- Closed systems are hard to analyze - "Break the glass" situations circumvent access control - Cryptographic solutions are computationally intensive and not flexible -"Big data" challenges protection mechanisms
	Communication Plane Wire (copper, coax, fiberoptics, etc.), bluetooth/Zigbee, Satellite/Cellular radio, Infrared wave	- Sensitive patient information is transmitted over public Internet - From monitoring devices to EHR, data travels through multiple vulnerable communication modalities - Wireless communication may cause electromagnetic interference to medical devices (disruption)	- Denial of service impacting monitoring, integrated care, self-care, and social support - Breach of confidentiality of patient info due to tapping or emanation - Loss of data integrity causing erroneous monitoring & wrongful intervention	- Virtual private networks - Intrusion detection - Message authentication - EMI testing	-Wireless, Ad-hoc and opportunistic networks are naturally vulnerable - Cryptographic solutions are computationally intensive and not flexible - Tele-health and emergency care rely on on-time data transmission
	Device Plane Embedded/wearable Medical Devices, Mobile/ Smartphone, Application Hosting Devices, Storage Devices	- Medical devices are resource-constrained - Implanted devices are sensitive to modification - Wearable devices are easily exposed, prone to interference - Healthcare providers have little or no control over the 3rd party cloud infrastructure	- Prone to sleep deprivation attacks - Attacks on patients' physical safety - Offline hardware attack - Failed or compromised devices impacting integration, self-care, and social support	- Device encryption - Fail-secure device design - Device-level access control	- Hardware is hard and expensive to analyze - Unrealistic trust on cloud provider & auditing in cloud is challenging - Researchers have limited or no access to device hardware and firmware

BigData & Security and Privacy Threats

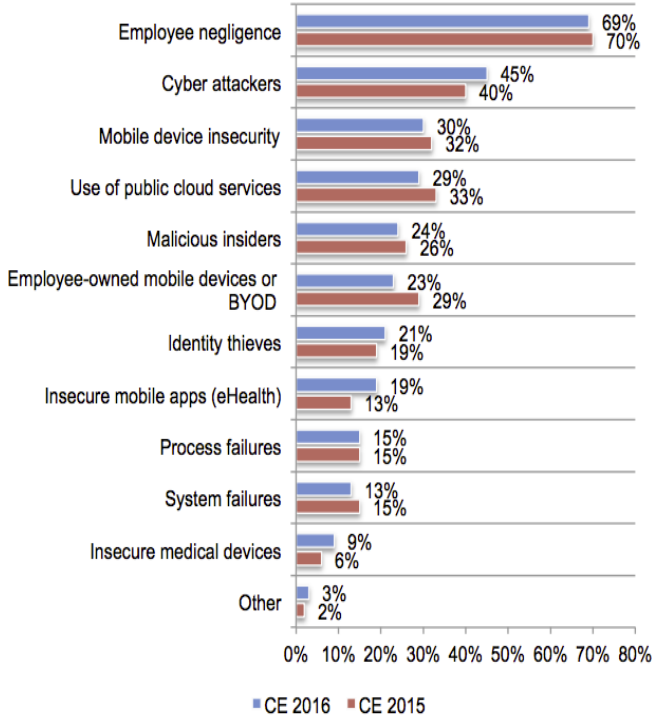
- Newer data mining, machine learning/ AI tools can unearth/infer sensitive information
  - Consent to new info may not be possible (inference) !!
  - Notice is not really there
  - Data quality/accuracy is not guaranteed
    - Possible false diagnosis, wrong treatment, etc.
  - …



Security and Privacy Issues/Challenges

Threat agents:
Insider OR *Outsider*

Figure 5. Security threats healthcare organizations worry about most
Three responses permitted



Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	5%	53%	42%
2	Information and communications	1%	3%	96%
3	Manufacturing	4%	5%	91%
4	Retail	2%	7%	91%
5	Healthcare	25%	46%	29%

Fewer
More

Figure 9: Attack sources by industry – 1 January 2016 through 31 December 2016.

Some of our efforts: Intimate Partner Violence (IPV)

30% of women impacted globally (as per WHO, CDC)

Collaboration with:

- Rose Constantino (School of Nursing)
- Balaji Palanisamy (SCI)

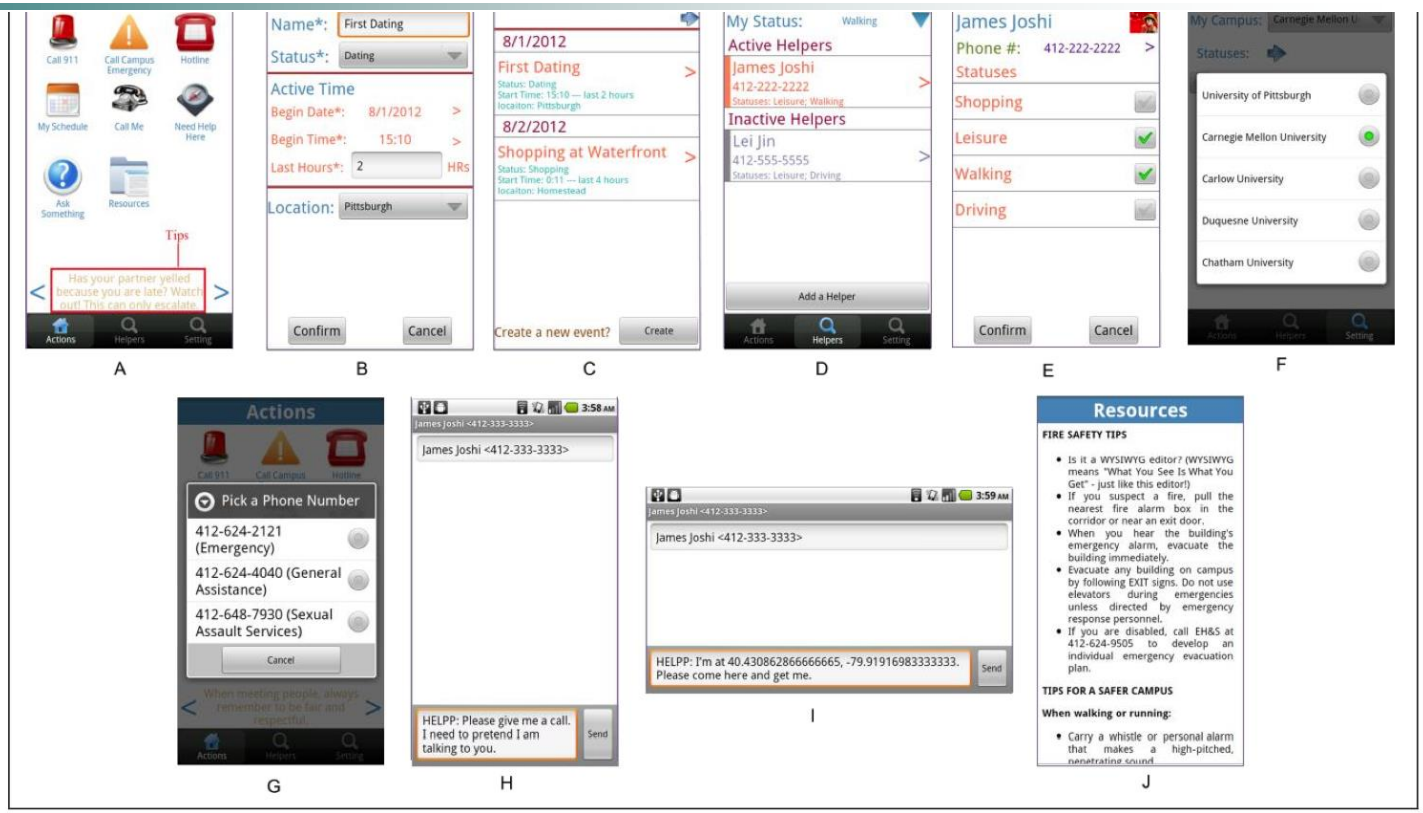
HELPP Zone

(Health, Education on safety, Legal Participant Preferred)

Just-in-time communication and intervention from and by trusted contacts

Text based messasing

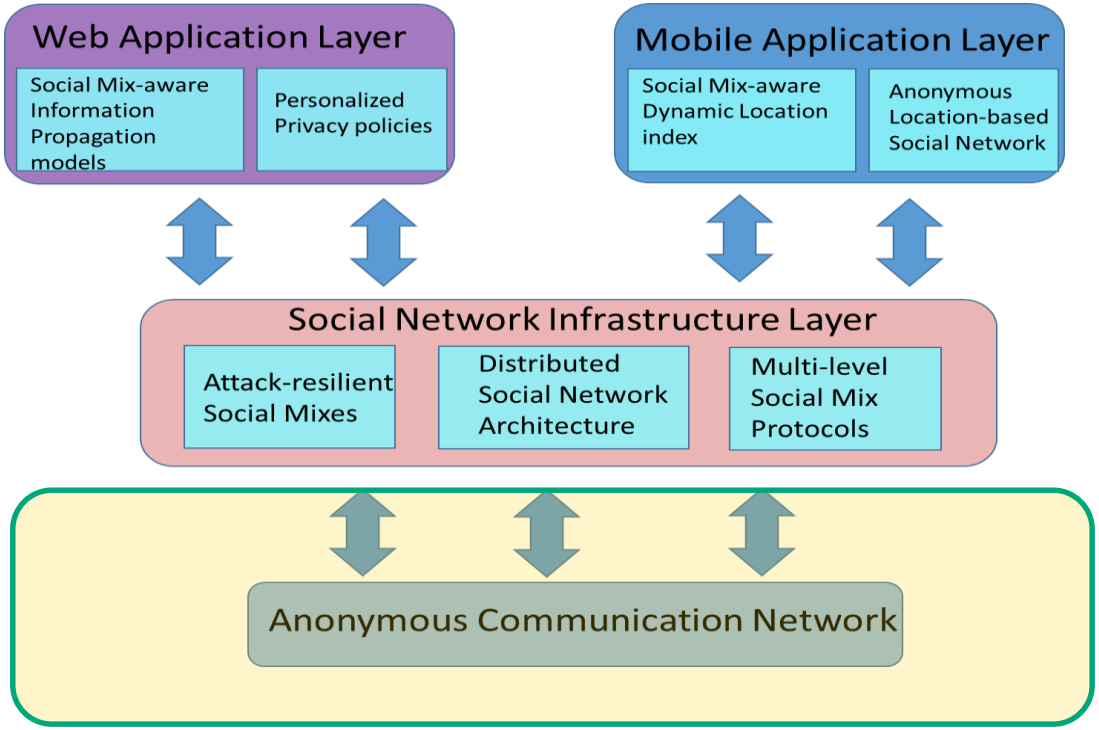
Dynamic trusted contacts



Rose Constantino, Amirreza Masoumzadeh, Lei Jin, James Joshi, Joseph Burroughs, Dominique de la Cruz, "HELPP Zone App and TMI: Disrupting Intimate Partner Violence in College Students" 2013 International Nursing High-end Forum (INHF), China, 22nd - 23rd June, 2013.

A. Masoumzadeh, L. Jin, J. Joshi, and R. Constantino, "HELPP Zone: Towards Protecting College Students from Dating Violence," in iConference 2013 Proceedings, 2013, pp. 925-928.

LEAF System:
(Lending Encouragement, Affirming Futures)



Web app
Social Network
Mobile app

LEAF:A Privacy-conscious Social Network-based Intervention Tool for IPV Survivors

Balaji Palanisamy Sheldon Sensenig James Joshi Rose Constantino†
School of Information Sciences, University of Pittsburgh †*School of Nursing, University of Pittsburgh*

LEAF Social Network

(a) An example LEAF netw

Privacy and Anonymity

Protecting Source Privacy
sender's identity cannot be inferred

Protecting Participant Privacy
willingness to participate increases when anonymity is guaranteed

Protecting Recipient Privacy
Recipient may wish to forward a message from another user to his friends remain anonymous

Protecting Location Privacy
Users should be able to use location-aware resources without revealing their location

Social Mix Mechanism

ymous communication

Summary

- Course overview
- Healthcare Ecosystem & HIPAA Overview
- mHealth – anytime, anywhere!
- mHealth Market data