

# Emerging Healthcare IT Privacy and Security Challenges

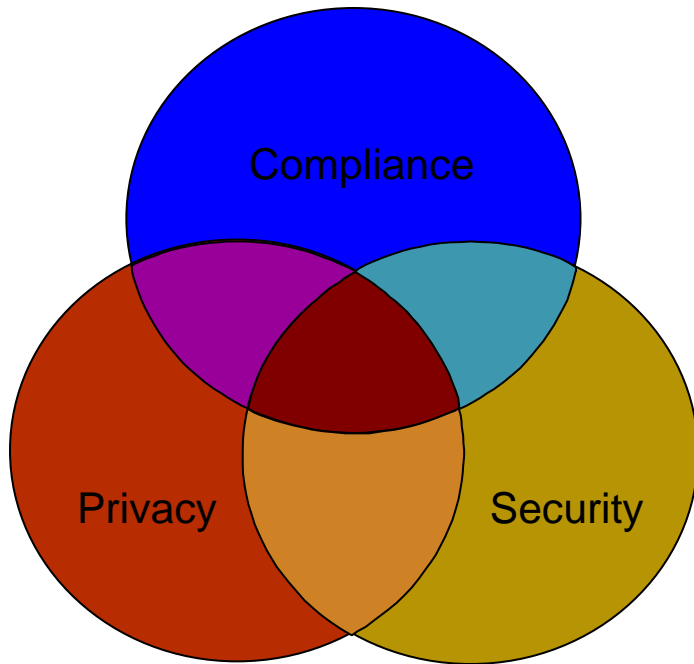
- ▶ Prepared for Carnegie Mellon University Silicon Valley

Jing Wang MacKenzie, MD, MHA  
Date: November 22, 2011

# Table Of Contents

- ▶ Overview of Healthcare Privacy and Security
- ▶ Challenges with Electronic Health Record Snooping
- ▶ Challenges with Health Information Exchange
- ▶ Challenges with Biomedical Devices

# Definitions



pri·va·cy

/ˈprɪvəsē/

- ▶ The state or condition of being free from being observed or disturbed by other people.
- ▶ The state of being free from public attention.

se·cu·ri·ty

/siˈkyʊərɪtē/

- ▶ The state of being free from danger or threat.
- ▶ The safety of a state or organization against criminal activity such as terrorism, theft, or espionage: "national security".

com·pli·ance

/kəmˈpliəns/

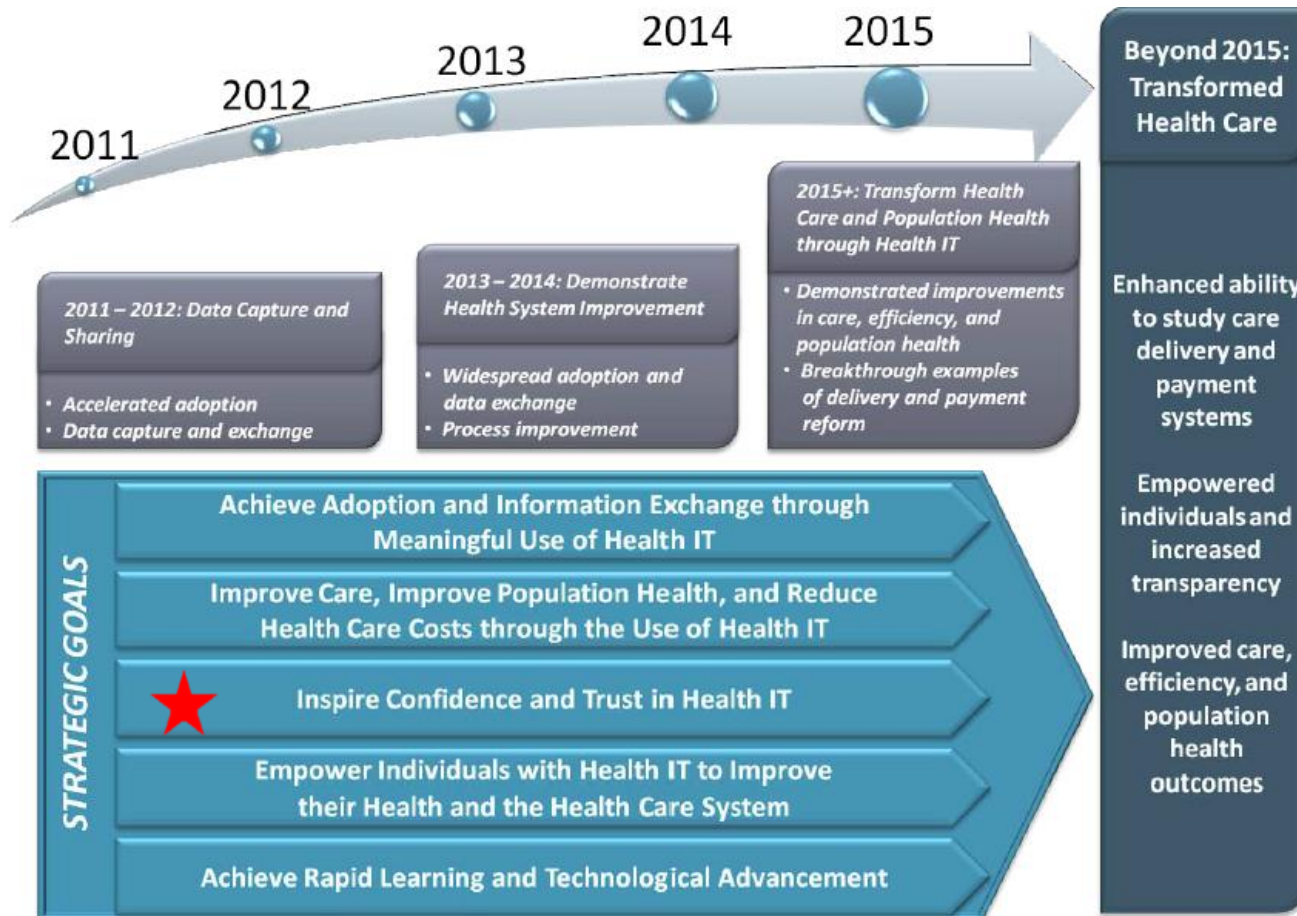
- ▶ The action or fact of complying with a wish or command.
- ▶ The state or fact of according with or meeting rules or standards.

Source: Google Dictionary

# A New Era for Healthcare and Healthcare Information Technology

- ▶ The Patient Protection and Affordable Care Act of 2010 (ACA) mandated the Medicare Shared Saving Program (MSSP), which established regulations toward Accountable Care Organization (ACO) by providing incentives to encourage **high quality and efficiency of care at lower cost**
  - ACOs are legal entities representing collaborative care providers collectively responsible for the full continuum of care for a designated group of Medicare beneficiaries
  - Information sharing across entities and proactive data analytics build the foundation
- ▶ The American Recovery and Reinvestment Act of 2009 (ARRA) was a historical milestone with America's determination to adopt healthcare information technology
  - \$20+ billion funding
  - Meaningful Use of Certified Electronic Health Record
  - Nationwide Health Information Network

# Connectivity and Trust Center of Federal Health IT Strategy



Source: Federal Health IT Strategic Plan – Public Comment Period

## Connectivity has Many Meanings

- Across systems and devices
- Across teams and workflows
- Among the consumers and the care providers
- Within the walls of a health care organization
- Across the lines of care organizations
- Across states lines
- Across governmental and private organizations
- Among healthcare and with other industries
- ...

# The Unintended Consequence of Connected Health Information

- ▶ When records are on paper or in “off-line” systems, ironically, the fact that the information is usually segmented and less accessible provides a natural barrier from privacy and security breaches
- ▶ As connectivity expands, that barrier is vanishing quickly
  - it could become a “single stop shop” for all
  - Damage can happen much faster, deeper and broader
  - It could even enable harm

# Medical Data Breach Can Have Severe and Irreversible Impacts

- ▶ While financial data breaches are costly, there usually is a recourse. This is not always true with medical data breach, and the burden of recourse is much more onerous
- ▶ Medical data breaches are likely to be irreversible, dangerous and even fatal

***“breaches of an individual’s privacy and confidentiality may affect a person’s dignity and cause irreparable harm”and “[unauthorized disclosures] can result in stigma, embarrassment, and discrimination.”***

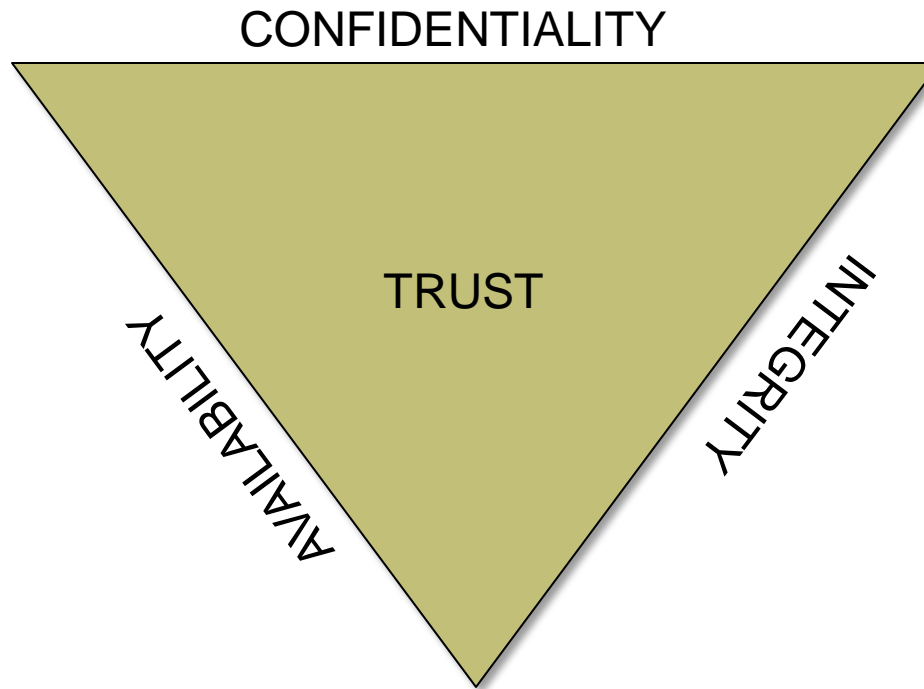
IOM: Beyond the HIPAA Privacy Rule—Enhancing Privacy, Improving Health Through Research, February 4, 2009

# Medical Identity Theft Offers Strong Incentives for Criminals

- ▶ Exploitation of stolen medical records to commit identity fraud lasts four times longer on average as compared to other types of identity theft
- ▶ The World Privacy Forum has reported that the street cost for stolen medical information is \$50, versus \$1 for a stolen Social Security number
- ▶ The average payout for a medical identity theft is \$20,000, compared to \$2,000 for a regular identity theft

Source: RSA “Cybercrime and the Healthcare Industry”

# The CIA Triad for Healthcare



# The Foundation of Patient Trust

*“...ALL THAT MAY COME TO MY KNOWLEDGE IN THE EXERCISE OF MY PROFESSION OR IN DAILY COMMERCE WITH MEN, WHICH OUGHT NOT TO BE SPREAD ABROAD, I WILL KEEP SECRET AND WILL NEVER REVEAL...”*

Hippocratic Oath, Fifth Century B.C.

# Americans' Trust in HIT is not There, yet

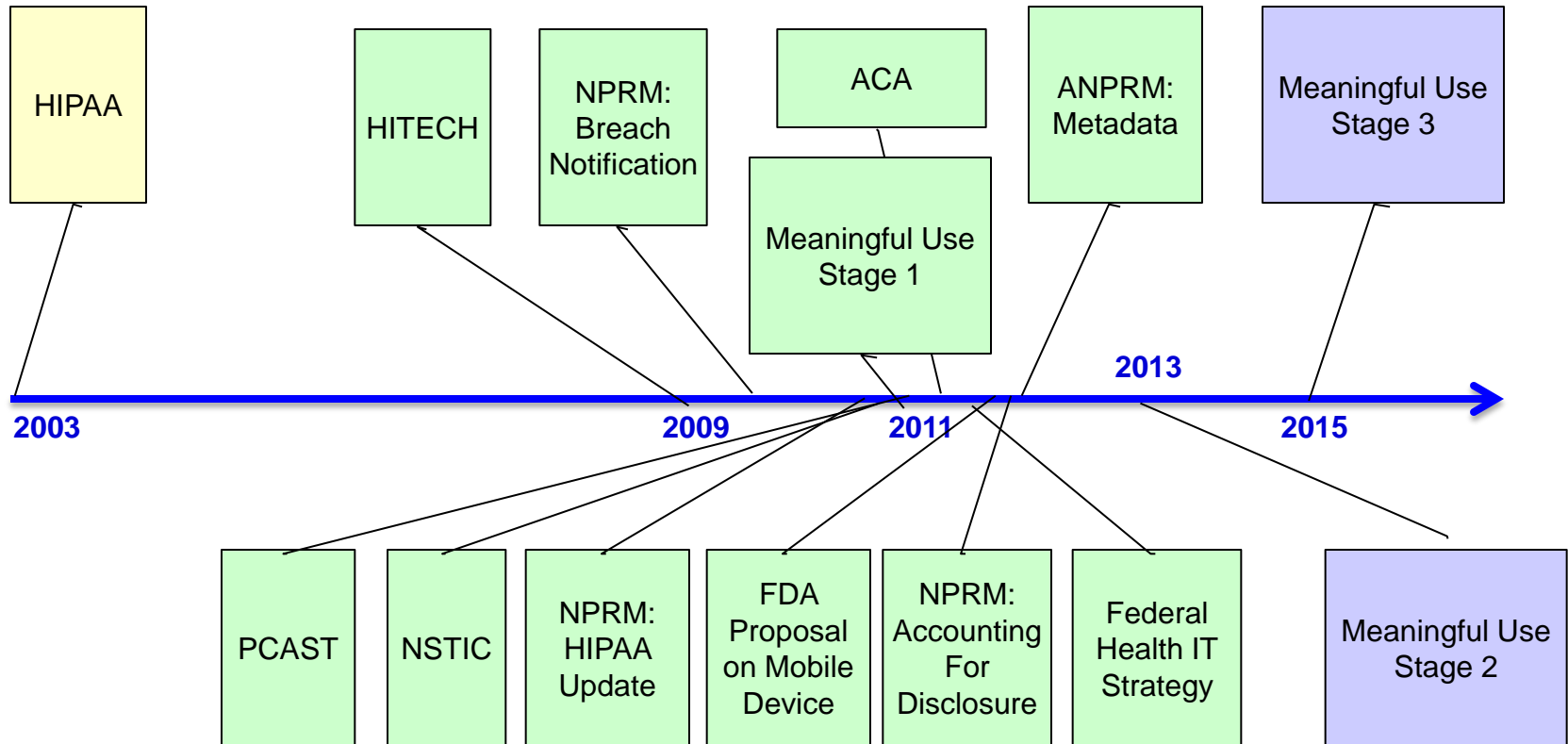
- ▶ According to a 2007 Harris Survey:
  - 25 percent U.S. adults disagree that increased use of computers to record and share patient medical records can be accomplished without jeopardizing proper patient privacy rights.
  - 27% feels that existing federal and state health privacy protection laws do not provide a reasonable level of privacy for their health information;
  - 50% believes that patients have lost control over how their medical records are used by organizations such as life insurers, employers and government health agencies.

# Data Breaches are Costing Billions for US Healthcare

- ▶ The total financial cost due to data breaches on the healthcare industry is nearly \$6 billion annually.
- ▶ Average cost over a two-year period is approximately \$2 million per organization
- ▶ Lifetime value of a lost patient is \$107,580.
- ▶ The average organization had 2.4 data breach incidents from 2008 to 2010.
- ▶ Major factors causing data breaches are unintentional employee action, lost or stolen computing devices and third-party error.

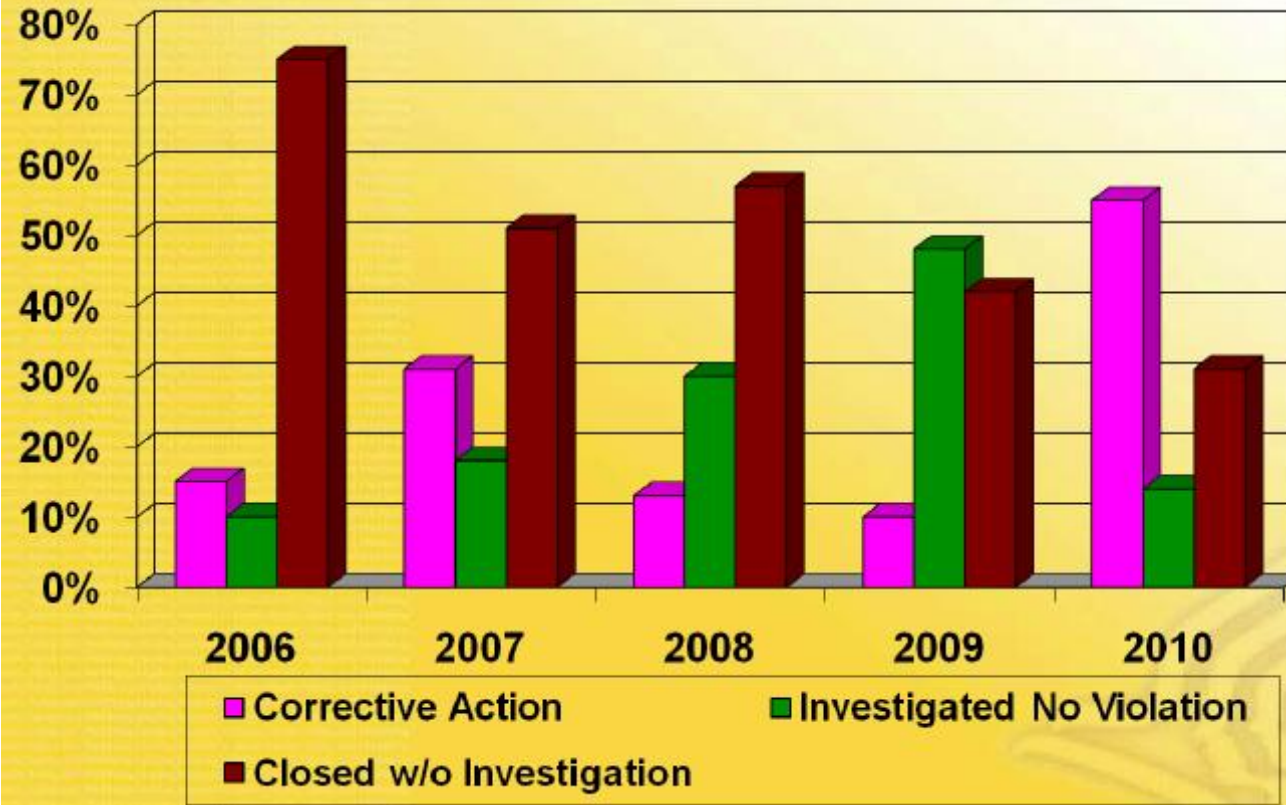
**Benchmark Study on Patient Privacy and Data Security. Ponemon Institute, November 2010**

# The Regulatory Turbulence on Health IT Privacy and Security



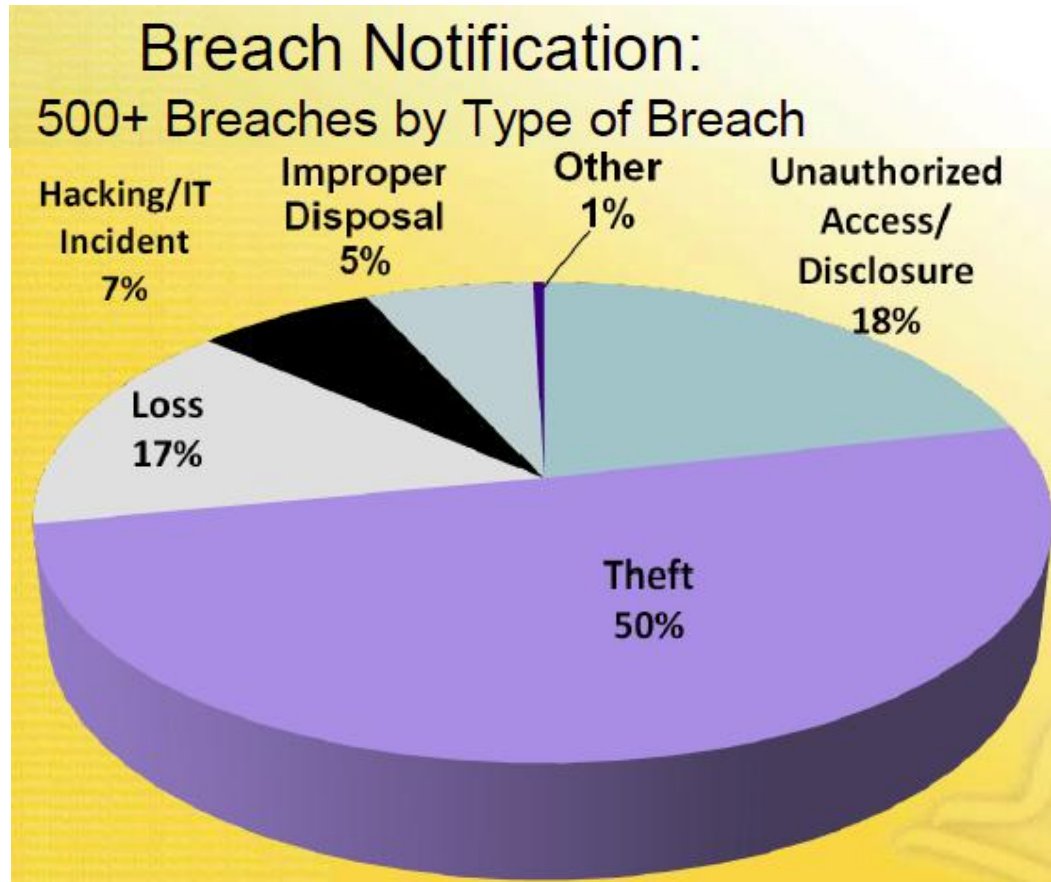
# Uptrend with HIPAA Security Enforcement

## Security Closures by Type



[http://csrc.nist.gov/news\\_events/HIPAA-May2011\\_workshop/presentations/day2\\_HIPAA-conference2011-OCR-Enforcement-Activities.pdf](http://csrc.nist.gov/news_events/HIPAA-May2011_workshop/presentations/day2_HIPAA-conference2011-OCR-Enforcement-Activities.pdf)

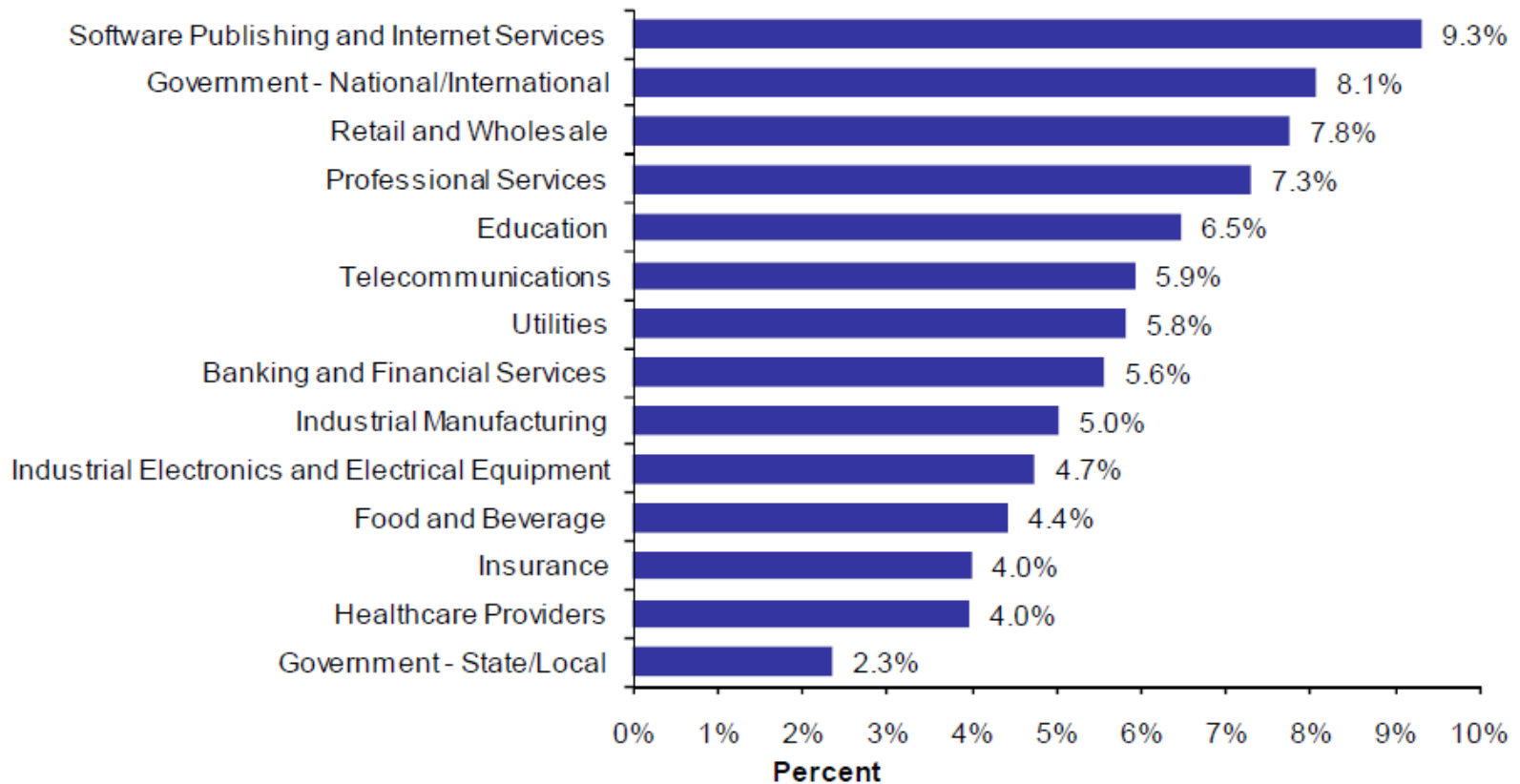
## Majority of Security Breaches are Avoidable



[http://csrc.nist.gov/news\\_events/HIPAA-May2011\\_workshop/presentations/day2\\_HIPAA-conference2011-OCR-Enforcement-Activities.pdf](http://csrc.nist.gov/news_events/HIPAA-May2011_workshop/presentations/day2_HIPAA-conference2011-OCR-Enforcement-Activities.pdf)

# Security Yet not an Investment Focus in Healthcare

## IT Security Spend as a Percent of IT Spend – By Industry



Source: Gartner 2011

# Meanwhile Healthcare Information Technology has Taken Off

- ▶ Electronic Health Records
- ▶ Health Information Exchange
- ▶ Digitized and Networked Medical Devices
- ▶ Other non-health-specific waves including Mobility, Cloud Computing, and Social Networking, etc. are also here
- ▶ ...

## Table Of Contents

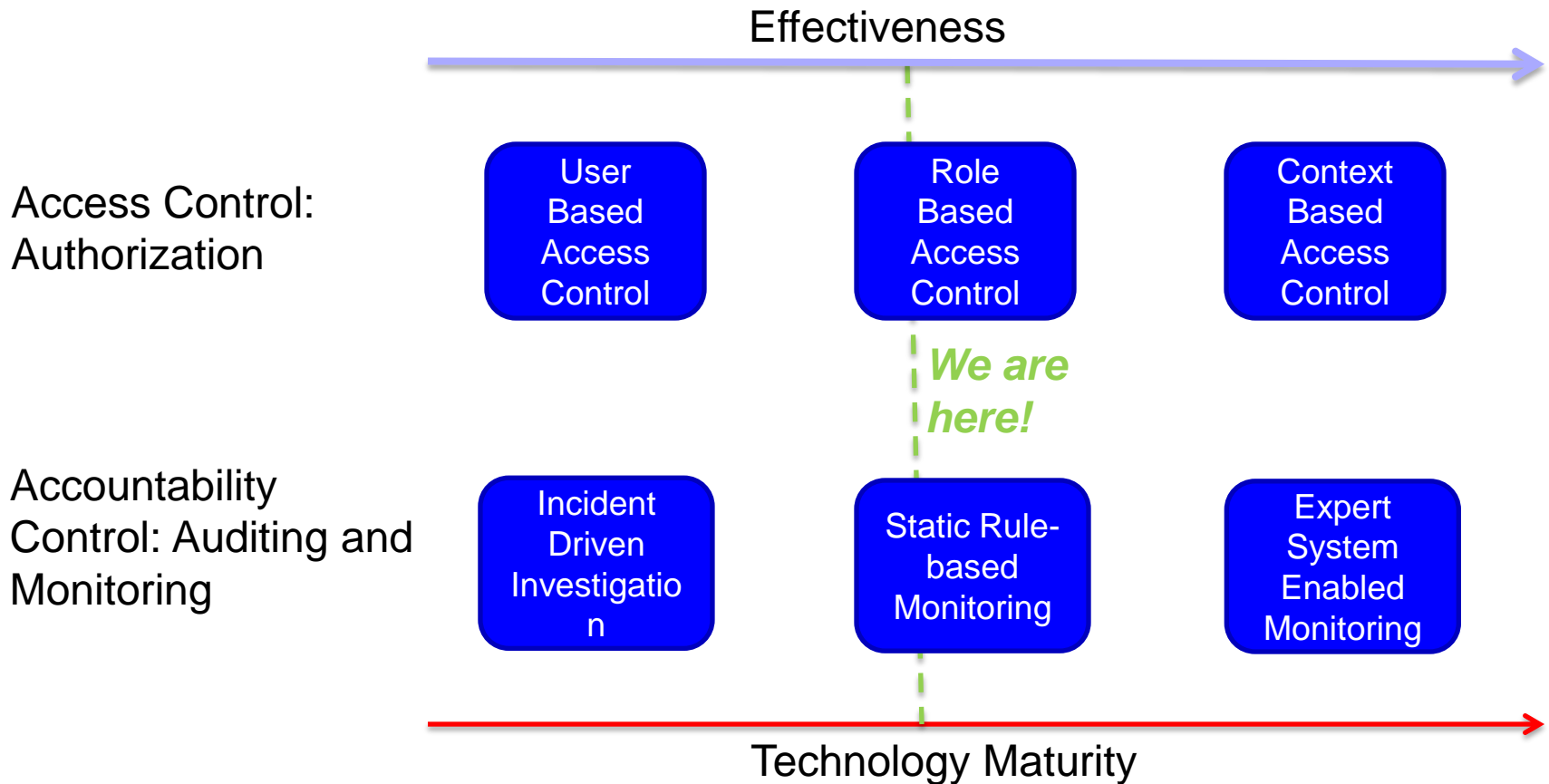
- ▶ Overview of Healthcare Privacy and Security
- ▶ Challenges with Electronic Health Record Snooping
- ▶ Challenges with Health Information Exchange
- ▶ Challenges with Biomedical Devices

## About Electronic Health Record (EHR)

“An Electronic Health Record (EHR) is an electronic version of a patient's medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that person's care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.”

Source: Department of Health and Human Services

# The Two Greatest Challenges with EHR Privacy and Security

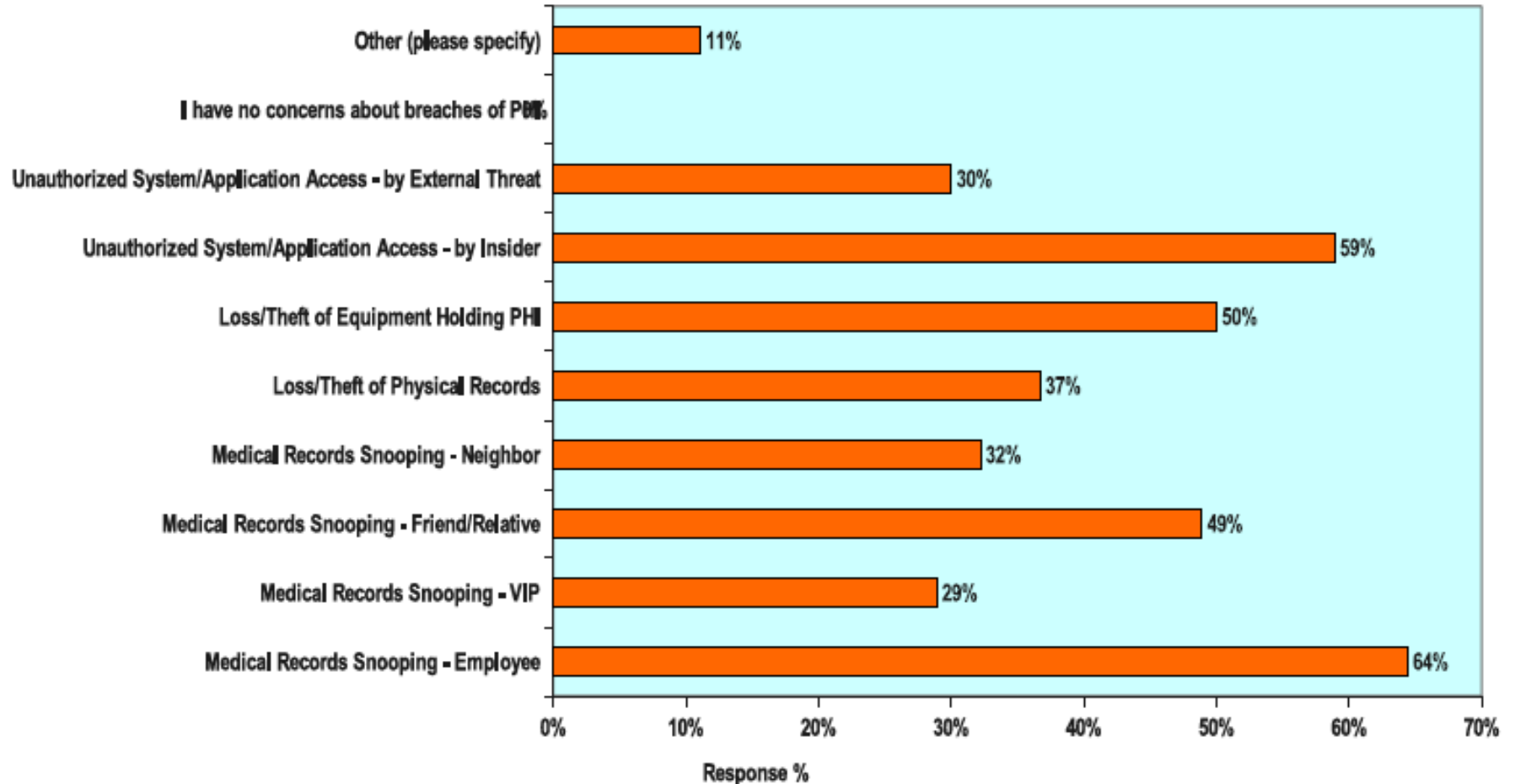


# Why Role Base Access Control is NOT Sufficient

- ▶ Static and coarse-grained
- ▶ Many clinicians carry multiple roles, depending on the location and schedule
- ▶ Temporary coverage among clinical staff a daily event
- ▶ “Break-the-glass” works only for known potential inappropriate access target

# EHR Snooping a Great Concern

I am most concerned about these types of protected health information breaches (more than one choice allowed)

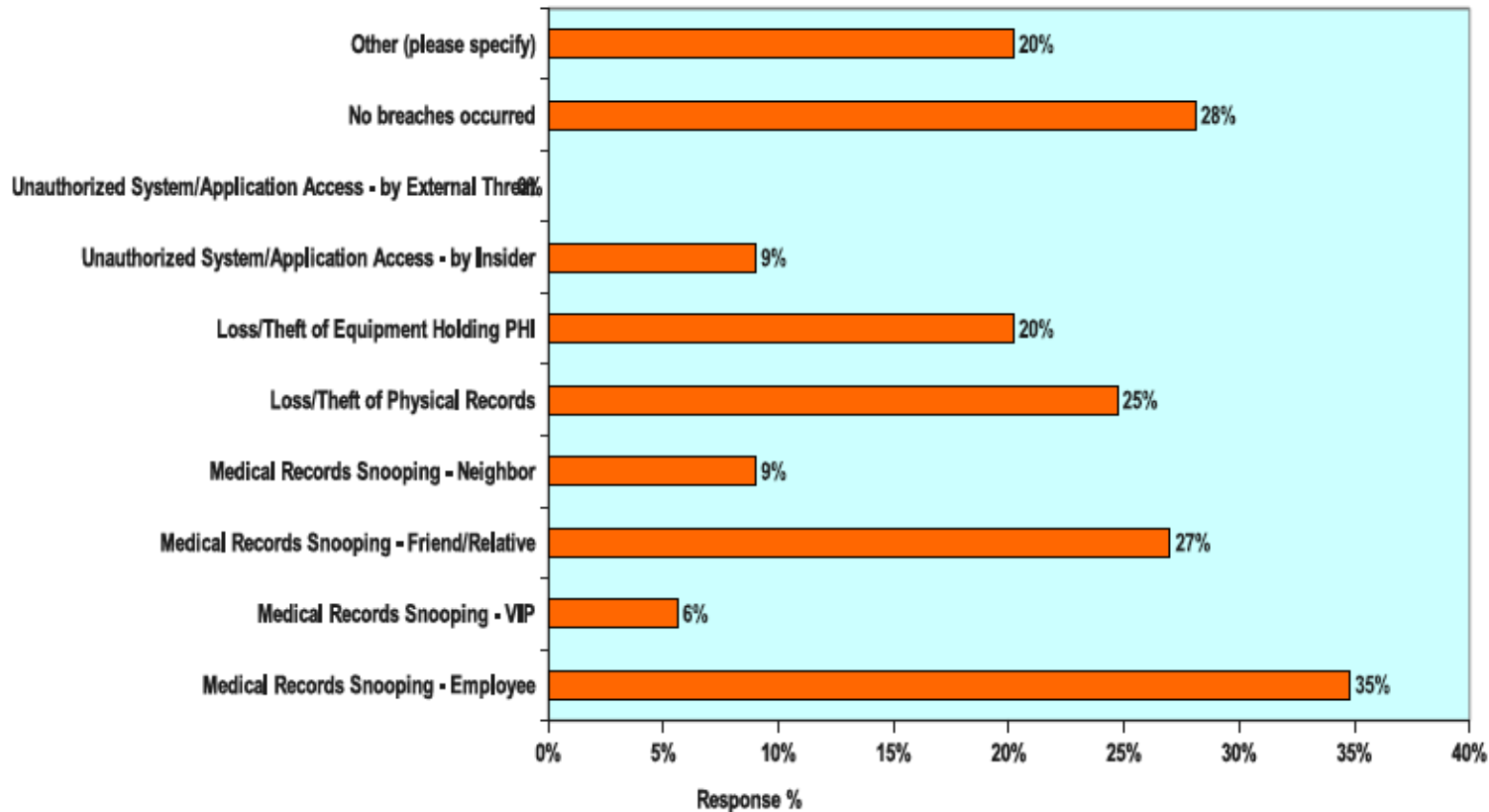


Source: Veriphysr 2011 Survey of Patient Privacy Breaches

Booz | Allen | Hamilton

# EHR Snooping a Real Problem

In the last 12 months, we have suffered a breach of protected health information in the following areas (more than one choice allowed)



Source: Veriphyr 2011 Survey of Patient Privacy Breaches

# Why is Snooping So Tough to Address?

- ▶ Open, caring, sharing culture
- ▶ Complex service - many people need to “touch” a patient record
- ▶ Unpredictability with who needs to be involved in care when and where
- ▶ Lack of technology enabling fine grained, dynamic user access
- ▶ Lack of commercial-off-the-shelf and mature tool for monitoring **inappropriate accesses by authorized users**

# The Technical Challenges with Access Monitoring



- Sheer Data Volume
- Great Data “Width”
- Complexity with Medical Data
- Data Disjointedness
- Variability of Data Access Reasons
- Rule Complexity
- **Low Tolerance on False Positives**
- Demand on business-user friendliness

# The Organizational Challenges

- ▶ Reportable incidents are costly, and proactive monitoring could increase the exposure in the short run
- ▶ Mandatory disciplinary actions can further stress nursing shortage
- ▶ Cultural difficulty holding physicians equally accountable
- ▶ Not a business priority

# Unfortunately, there is NO Silver Bullet

A Comprehensive Approach is Necessary:

- ▶ Clearly defined policy and procedures
- ▶ Awareness and training
- ▶ Tightened Access Controls to the extent possible
- ▶ Proactive identification of potential incidents at the extent feasible
- ▶ Consistent, highly visible, and impactful disciplinary actions with confirmed incidents

## Table Of Contents

- ▶ Overview of Healthcare Privacy and Security
- ▶ Challenges with Electronic Health Record Snooping
- ▶ Challenges with Health Information Exchange
- ▶ Challenges with Biomedical Devices

## About Health Information Exchange

- ▶ The mobilization of healthcare information electronically across organizations within a region or community.
- ▶ HIE provides the capability to electronically move clinical information between disparate healthcare information systems while maintaining the meaning of the information being exchanged.
- ▶ The goal of HIE is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, equitable, patient-centered care.
- ▶ HIEs also provide the infrastructure for secondary use of clinical data for purposes such as public health, clinical, biomedical, and consumer health informatics research as well as institution and provider quality assessment and improvement.

[http://en.wikipedia.org/wiki/Regional\\_Health\\_Information\\_Organization](http://en.wikipedia.org/wiki/Regional_Health_Information_Organization)

# The Privacy and Security Background for HIE

- ▶ Ubiquitous computing across geographical, organizational, judiciary, and public/private boundaries
- ▶ Wide spectrum of key stakeholders with different goals and incentives
- ▶ Wide differences among organization structures and practices
- ▶ Great variation of technology maturity
- ▶ Various architecture and standards
- ▶ Different laws, policies and procedures at both federal and state levels, not always clear, nor consistent
- ▶ Lack of technology maturity in certain areas

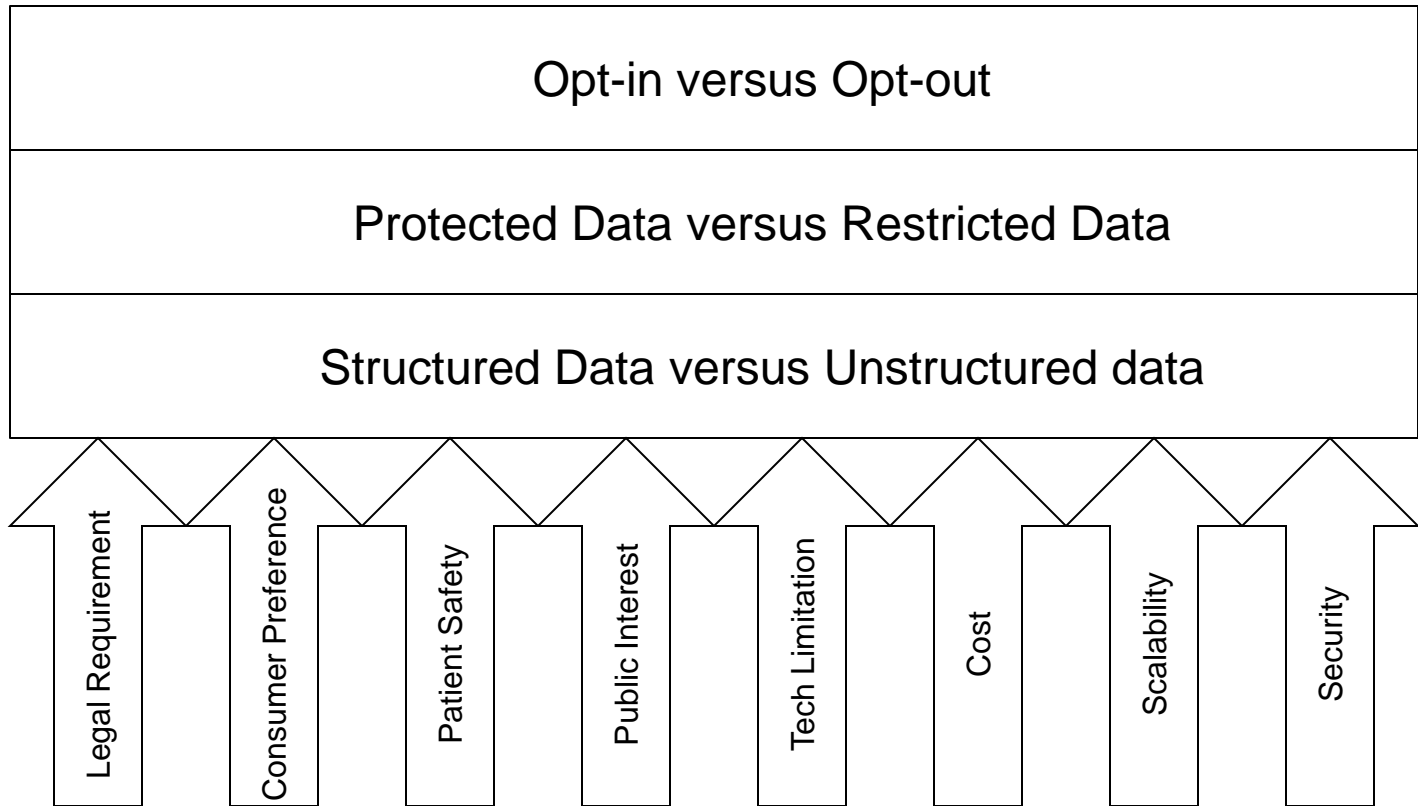
# Key Elements of HIE Privacy and Security

- ▶ Legal Framework: HIPAA, HITECH, State Laws
- ▶ Contractual Framework: DURSA
- ▶ Best Practices and Guidelines: Market Common Framework, CalPSAB Security Guideline
- ▶ Technical Standards: NwHIN Specifications
- ▶ Implementation Architecture: Federated, Centralized, Hybrid
- ▶ Risk Management

## Some Major Privacy and Security Challenges

- ▶ Need for Harmonized, meaningful, reasonable, and automated consent management
  - Opt-in versus Opt-out
  - Protected versus Restricted
  - Structured versus Unstructured data
- ▶ Unique patient identification absent of a national patient identifier
- ▶ Identification and manage risks to mitigate the weakest link in the circle of trust
  - Due diligence with security, not just compliance
  - Accountability
  - Reliable Rapid Security Incident Response

# Consent Management a Complex Decision



# Public Awareness Promotion a Necessity

- ▶ Open and candid discussions of safety, quality and efficiency benefits versus privacy and security risks
- ▶ Increase public vigilance on medical data breaches
- ▶ Establish effective communication feedback loop with policy makers and into policy making processes

## Accurate and Automated Patient Mapping Still A Challenge

- ▶ Data volume – manual processes not sustainable
- ▶ Data quality issues – garbage in garbage out
- ▶ Variable demographic data
- ▶ Inconsistent format of demographic data
- ▶ Low tolerance on both false negatives AND false positives
- ▶ Exception processes

# Security a Distributed and On-going Task

- ▶ Every link on the circle of trust must be sufficiently protected
- ▶ Be secure not just be compliant: meeting the technical security standards does not equate due diligence with risk assessment and management.
- ▶ Commitments through contractual agreement need to be validated regularly. Trust... but verify.
- ▶ Security breaches will happen. Be prepared to respond swiftly and appropriately

## Table Of Contents

- ▶ Overview of Healthcare Privacy and Security
- ▶ Challenges with Electronic Health Record Snooping
- ▶ Challenge with Health Information Exchange
- ▶ Change with Biomedical Devices

# About Medical Devices

- ▶ A manufactured product is defined as a medical device if it is used to:
  - Cope with human disease.
  - Care for human injuries.
  - Meet human anatomical needs.
  - Maintain human physiological functions.
  - Support or sustain human life.
  - Control human conception.
  - Disinfect human medical devices.
  - Examine specimens taken from human bodies.
- ▶ Medical devices can include: instruments, appliances, implants, machines, software, materials, calibrators, apparatuses, in vitro reagents, and related articles
- ▶ Manufactured products that achieve results by pharmacological, immunological, or metabolic means are not medical devices. However, the results achieved by medical devices may be assisted by these means.

Source: ISO 13485 2003

# Recent News on Biomedical Device Hacking

*August 4, 2011*

“A security researcher who is diabetic has identified flaws that could allow an attacker to remotely control insulin pumps and alter the readouts of blood-sugar monitors. As a result, diabetics could get too much or too little insulin, a hormone they need for proper metabolism... All he needed was a USB device that can be easily obtained from eBay or medical supply companies ...With a powerful enough antenna... an attacker could be up to half a mile away.”

[http://www.huffingtonpost.com/2011/08/04/insulin-pumps-monitors-vulnerable-to-hacking\\_n\\_917987.html](http://www.huffingtonpost.com/2011/08/04/insulin-pumps-monitors-vulnerable-to-hacking_n_917987.html)

*October 25, 2011*

“McAfee... exposed the new vulnerability in one model of the Medtronic Paradigm insulin pump on Friday and believes there could be similar risks in others..”

<http://www.guardian.co.uk/business/feedarticle/9913510>

# Information Security Risks with Biomedical Devices

- ▶ Mechanical malfunction caused by device software failures can directly cause patient harm
- ▶ Integrity breach of patients' health care information can adversely impact care decisions
- ▶ Privacy breach of patients' health care information can negatively impact the care organization's reputation
- ▶ Medical devices can expose an organization's network to further breaches
- ▶ ...

# Reported Biomedical Medical Security Incidents

- ▶ In June 2010, VA reported that more than 122 medical devices were infected by malware during the prior 14 months at the U.S. Dept. of Veterans Affairs' network of 50,000 medical devices, representing what one official called a critical challenge to the department's security. (<http://www.informationweek.com/news/healthcare/security-privacy/225200097>)
- ▶ In December 2010, a portable ultrasound diagnostic machine was stolen from a Texas hospital. The hospital estimated the ultrasound machine may have contained two years worth of patient studies. The device does not have the capability of encryption. (<http://www.phiprivacy.net/?p=5929>)

# Reported Medical Device Software Failures

- ▶ Between 1983 to 1997, 2,792 quality problems that resulted in recalls of medical devices and of problems, 383 were related to device software
- ▶ Between 1985 to 1987, software problems with herac-25, a linear accelerators for radiation therapy, lead to 6 well known cases of death or severe adverse events resulting in machine recall
- ▶ Between 2005 and 2009, the FDA received approximately 56,000 infusion pump-related adverse event reports, many of which were associated with software malfunction and/or caused significant morbidity and mortality

# Unique Attributes with Biomed Device Security

- ▶ Biomedical devices are regulated by FDA
  - Security is not a mandatory requirement
  - Changes to the devices are tightly controlled, and take longer to test and approve
- ▶ Biomedical devices are industrial control systems that physically deliver real time care
  - Much lower tolerance with availability impact
  - Extremely high reliance with data integrity
  - Need to maintain the device function even when security fails
  - Limited understanding by IT professionals
- ▶ Medical Devices on average have a life span of 7-10 years, comparing to 2-3 years with IT devices.
  - The underlying Operating System may be outdated but continue to face rapidly evolving threats.

# Industry-Wide Challenges

- ▶ Biomedical device security has historically received inadequate attention from the manufactures
- ▶ Traditional enterprise security tools are often not directly applicable to medical devices because they are designed for general IT systems
- ▶ Security requirements are frequently identified by individual provider organizations, but not collectively defined and demanded and thus not effectively responded by the market.
- ▶ Existing industry standards tend to be high level and vague, and focus on static security features rather than dynamic risks identification such as penetration testing.

# Why have We not Seen More Security Incidents Reported yet?

- ▶ Many devices are not yet digitalized or connected – this is fast changing
- ▶ Vendor proprietary hardware and software is still common, but rapidly migrating to COTS
- ▶ Limited security protections partially effective
- ▶ Mandatory breach notification only started two years ago
- ▶ The perfect storm is nonetheless coming

# What is Needed for Biomedical Device Security

- ▶ Cross industry collaboration
  - Users, Manufacturers, Regulators, Security Solution Vendors, etc
- ▶ Define and measure the issue
  - Scope and Prioritize
- ▶ Develop Best Practices and Guidelines
  - Reasonable technical controls augmented with penetration testing
  - Manage the whole device life cycle
  - Shared accountability between the care provider organization and the manufacture
  - Integration into device procurement processes
- ▶ Resource, Information and knowledge sharing

# Contact Information

**Jing Wang MacKenzie, MD, MHA**  
Senior Associate

**Booz | Allen | Hamilton**

(c) (925) 480-7031  
(e) mackenzie\_jing@bah.com