



ARRA: Is Your Data Safe?



Joseph H. Schneider, MD
VP and Chief Medical Information Officer
Baylor Healthcare System
Alliance For Healthcare Excellence
September 23, 2010

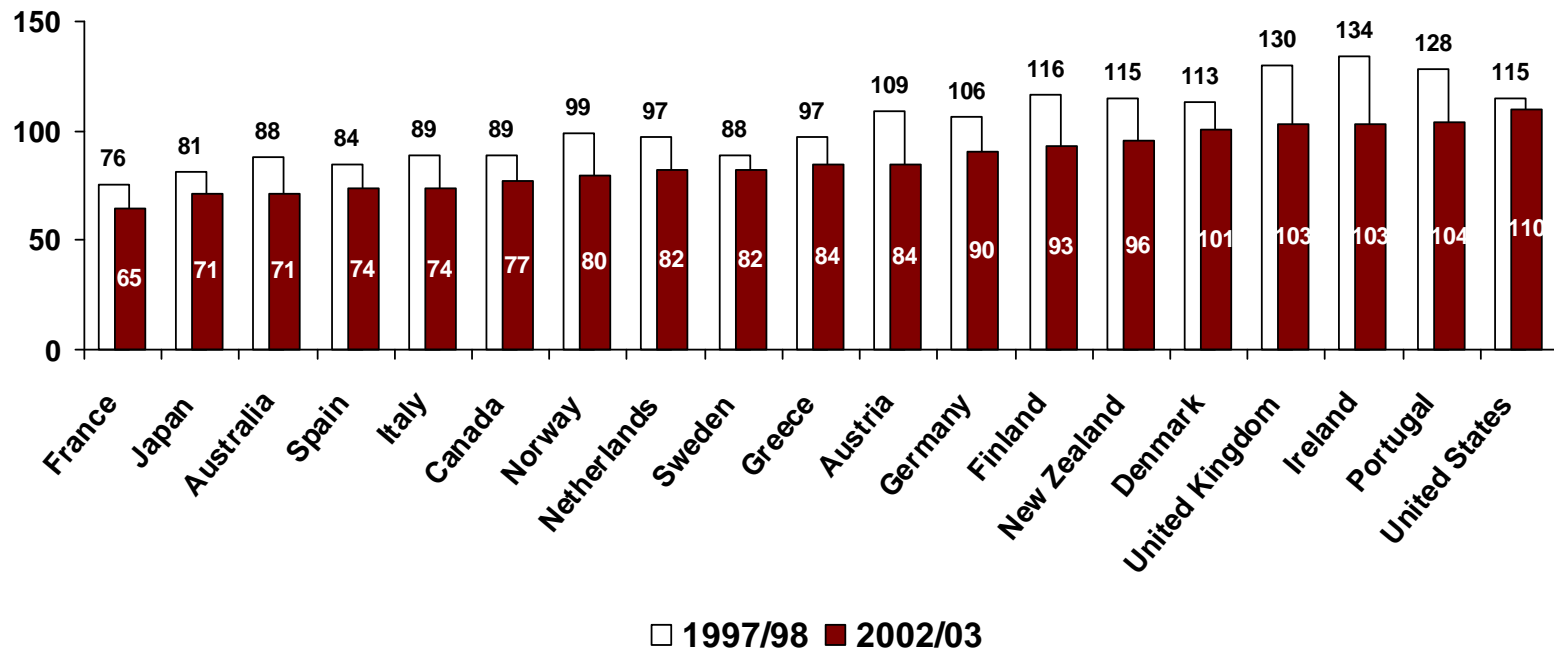
Expert (ek-sprt) *n.*

A person from afar
carrying lots of colorful slides
whose degree of expertise
is measured
by the distance traveled

Our Objectives

- Explain ARRA highlights related to Health IT
- Discuss issues affecting data integrity, security and privacy
- Discuss potential future directions

Age Standardized Death Rates: USA is 37th best overall



US Healthcare spending is ~\$1 trillion.

“ We don't have a healthcare delivery system in this country. We have an expensive plethora of uncoordinated, unlinked, economically segregated, operationally limited micro systems, each performing in ways that too often create sub-optimal performance, both for the overall health care infrastructure and for individual patients.”

George Halverson (CEO Kaiser): “*Healthcare Reform Now*”

NY Times survey (1/29/09): 75 % of patients were unable to name a single doctor assigned to their care. Of the 25% who responded with a name, only 40% were correct.

Why Is Health Information Technology Important?



“Where is Mrs. Jones xray?”

Printer with results from one lab

Unsorted results

About to ring with results

Prescription refill request on fax

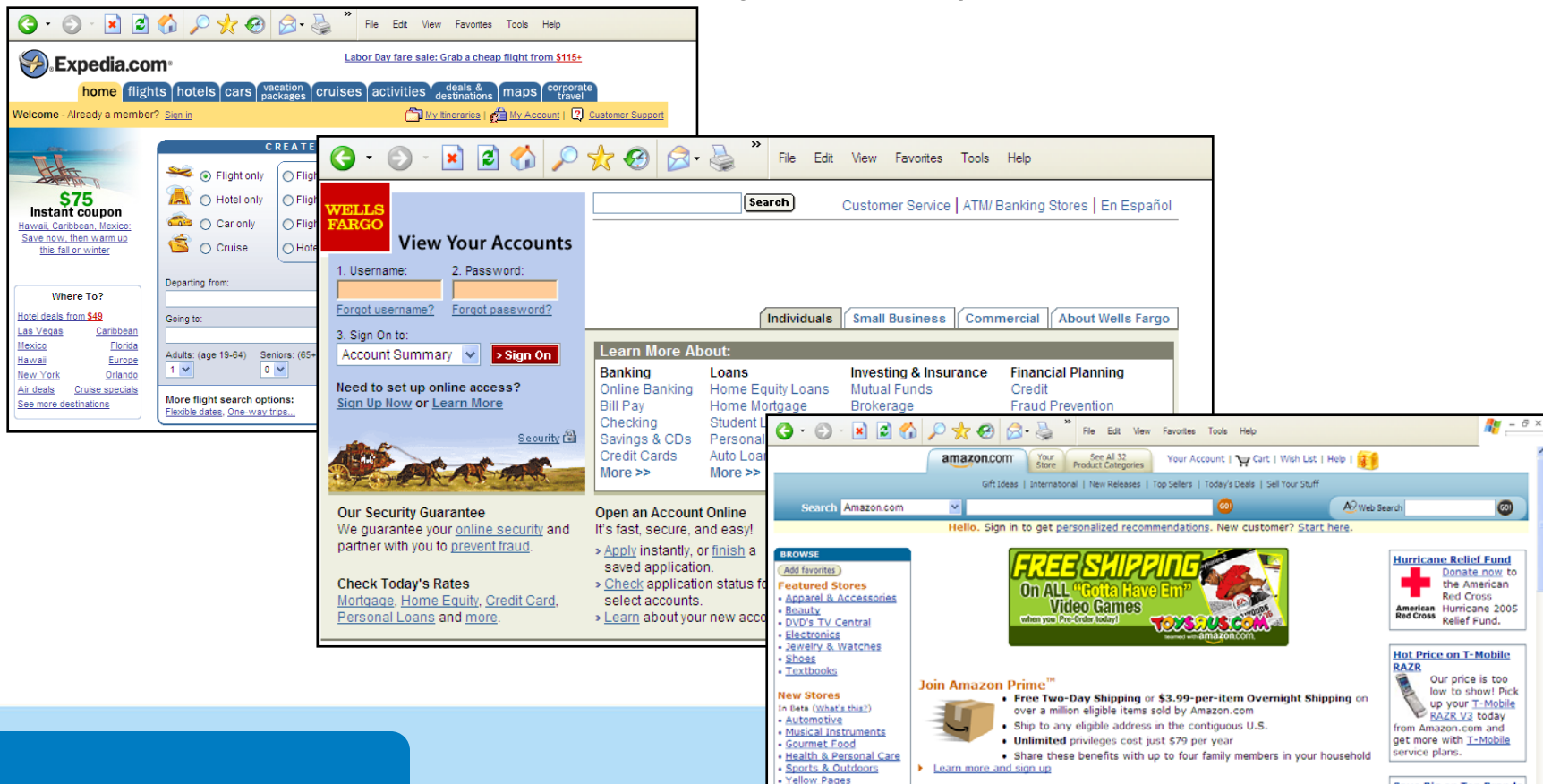
Unopened mail

Courier just dropped off more envelopes

Web portals with different passwords

Why Is Health Information Technology Important?

How We Fly/Bank/Buy...



The image displays three overlapping screenshots of web browsers, illustrating online services:

- Expedia.com:** Shows a search interface for flights, hotels, and cruises. A prominent offer for a "\$75 instant coupon" is visible. The navigation bar includes links for home, flights, hotels, cars, vacation packages, cruises, activities, deals & destinations, maps, and corporate travel.
- Wells Fargo:** Displays the "View Your Accounts" login page. It includes fields for Username and Password, a "Sign On" button, and a "Sign Up Now" link for users needing online access. A security guarantee is also highlighted.
- Amazon.com:** Shows the homepage with a search bar, navigation links, and promotional banners. Key offers include "FREE SHIPPING On ALL 'Gotta Have Em' Video Games" and "Join Amazon Prime™" with details on shipping benefits and costs.

Why Is Health Information Technology Important? *...How We Store Health Records...*

~14% of visits missing clinical information

- Adverse effect in 44%
- Delayed/additional care in 59%
- 3x more likely with complex patients



Why Is Health Information Technology Important? *...And How We Use Health Information*

Health system fails seniors half the time

Care for elderly ailments ignored

By Kathleen Fackelmann
USA TODAY

Older Americans with health problems get the recommended medical care they need only half the time, and the problem is worse when looking only at the treatment they get for age-

The latest study, published in the *Annals of Internal Medicine*, suggests seniors are no different: The report found that seniors got the recommended care for general medical conditions like heart disease just 52% of the time. But the drop-off in medical care worsened when the team homed in on age-related diseases such as dementia or malnutrition. The study found seniors got the appropriate care for these conditions just 31% of the time. The RAND team looked at the med-

Getting the right care only part of the time

A new study shows that older Americans are not getting the care they need.

Percent of time appropriate care is given

Ishemic heart disease	55%
Pneumonia	49%
Depression	31%

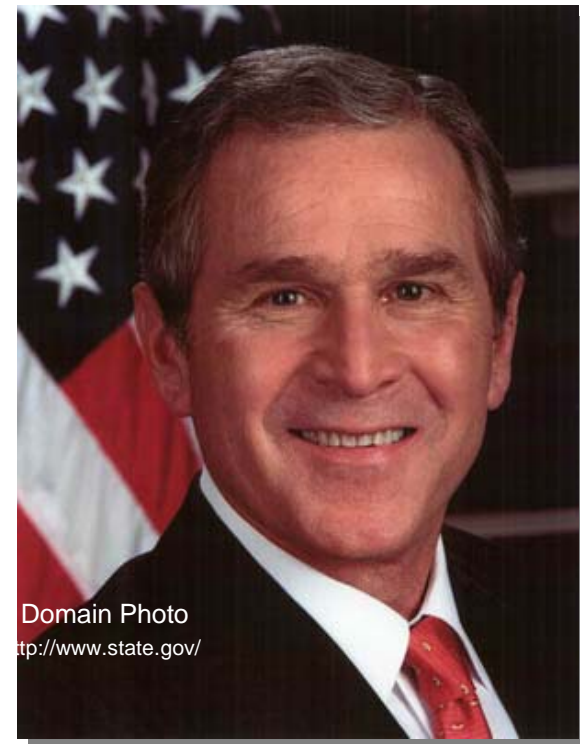
don't get the help they need, like physical therapy to improve their walking ability. Without that therapy, seniors run a greater risk of falling and breaking a hip. A broken hip can, in some cases, trigger an admission to a nursing home, Wenger says.

The new findings fit with other evidence suggesting that the health care system needs to improve, says Daniel Stryer at the Agency for Healthcare Research and Quality, part of the Depart-

Why Is Health Information Technology Important?

“To protect patients, improve care and reduce cost, we need a system where everyone has their own personal electronic medical record that they control and they can give to a doctor when they need to.”

George W. Bush. April 2004



ARRA Legislation

- Passed Feb. 13, 2009.
 - House: 246-183.
 - Senate: 60-38.
- President signed 2/17/09.
- “Meaningful Use” criteria released late July 2010.



ARRA - HIT Organization and Standards Bodies Created

- ARRA created Office of National Coordinator for Health IT within Health and Human Services.
- Established HIT Policy & Standards Committees for:
 - Policy framework
 - Standards
 - Implementation specifications
 - Certification criteria for electronic exchange and use of health information

ARRA - Health Information Technology Provisions

- \$17 billion (\$30 billion net of savings) plus funds for HIT infrastructure to help physicians use certified electronic health records (EHRs).
- Key element — uniform standards to allow systems to communicate with each other
- Competitive grants to states for physician loans to help pay for HIT acquisition/implementation.
- HIT Regional Extension Centers to assist physicians with EMR meaningful use.

ARRA - Other Funding

- \$4.5B for National Telecommunications Program
- \$2.5B for USDA Telemedicine efforts
- \$2B for HIE development (infrastructure)
- \$1.5B for FQHCs/CHCs
- \$1B for Research
- \$500M for Social Security Administration
- \$85M for Indian Health Service
- \$50M for Veterans Administration
- HIT related workforce development/research grants

ARRA Privacy and Security Changes: Making Your Data Safer?

Data Losses – Ripped From The Headlines

- 130,000 former and current patients have been notified that a laptop with personal information was stolen.
- A doctor's laptop was stolen from the Medical Center containing medical information of 22,000 patients.
- Two laptop computers stolen from locked vehicle in the Hospital parking lot hold personally identifiable medical information and SSN of 2,500 patients.
- A laptop with 7,800 uninsured patients' names, birth dates and Social Security numbers was stolen from the hospital.
- Stolen laptop contains medical information on 21,600 health plan beneficiaries.
- Stolen laptop had medical claims data on 230,000 people

ARRA Privacy/Security Changes - Breach of Information

- State attorneys general (AGs) will have the power to bring civil actions in federal court on behalf of state residents.
- Individuals may be the subject of prosecution - prior to ARRA, a breach of PHI (protected health information) constituted a violation of HIPAA; however, there was little recourse due to the fact that one could not sue under HIPAA.
- Some violations will be subject to criminal prosecution.

ARRA Privacy/Security - HIPAA Violations Tiered, Based on Severity

- Definitions provided based on entity knowledge:
 - Reasonable cause (RC)
 - Reasonable diligence (RD)
 - Willful neglect (WN)
- Secretary of HHS has some discretion in interpretation:
 - Your actions/policies/practices to ensure adherence or deal with violations can have bearing on decisions
 - Secretary required to investigate all complaints if preliminary investigation involves willful neglect

ARRA Privacy/Security - Penalties

- \$100 per violation, not > \$25K* (Reasonable Diligence)
- \$1000 per violation, not > \$100K* (RC, not WN)
- \$10,000 per violation, not > \$250K* (WN, corrected)
- \$50,000 per violation, not > \$1.5M* (WN, not corrected)
- Distribution of penalties or settlements to harmed individuals proposed for 2012

** All penalty limits listed are per calendar year and apply only to violations of an identical requirement or prohibition during a calendar year; additional penalties enforced may exceed the amount listed*

ARRA Privacy/Security - Business Associates Expansion

- Additional entities including vendors are subject to the same privacy and security rules as covered entities:
 - PHRs (Personal Health Records) hosted by vendors
 - Health Information Organizations (RHIOs and HIEs)
 - e-Prescribing gateways
 - Patient Safety organizations
- Will likely require new Business Associates contracts.

ARRA Privacy/Security - Notification of Breach Requirement

- If more than 500 records, breach must be reported to media within 60 days of occurrence and again annually.
- Patient may request an accounting of disclosures of PHI within the past 3 years even in the absence of a breach
 - If EHR in place on 1/2009, then compliance is 1/2014
 - If EHR purchased after 1/09, compliance is 1/11 or acquisition date
- Safe harbor for encrypted data
- Since release of NPRM, requirement to determine degree of harm has been rescinded.

ARRA Privacy/Security - Sales of Information, Marketing, and Foundation Activities

- Must clearly state that remuneration is associated with sale of information, marketing activity, and funds solicited
- Must make it easy for individual to opt out
- Foundations may view only demographics/dates of service
- Continues to exclude certain activities such as:
 - Public Health
 - Research subject to some limitations
 - Treatment and payment purposes
 - Others including the sale/purchase of a covered entity...

ARRA Privacy/Security - Disclosure and Accounting of PHI

- Patients can receive an electronic copy of EHR records, including external electronic transfer for a reasonable fee.
- Patient can request that no information be sent to their health plan if they pay for services in full out-of-pocket.
- Disclosures should be limited to minimum necessary or limited data sets. New definitions to be released 8/2010

ARRA Privacy/Security – Patient Consents and Hybrids

- Patient consents “may not be combined with any other document to create a compound authorization”
 - Some exceptions granted for research
 - Psych consent must always be separate
 - Need ability to opt out of HIEs
- Enhanced language for “hybrid” organizations - data may not be shared with portions of the organization not involved in direct health care delivery_simplly because they are members of the same organization.

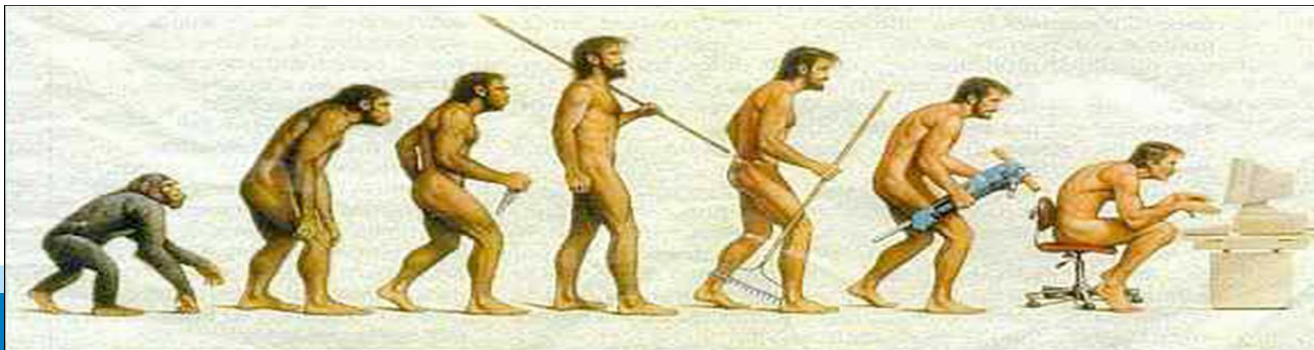
Issues Affecting Data Integrity, Security and Privacy :
How Risky Is Electronic Health Information?

Health Data Exchange Evolution

- *Paper*
- *Mail*
- *Fax*
- *Baby Books*

A short time

- *EMRs*
- *Health Information Exchanges*
- *E-prescribing*
- *Insurance and billing processes*
- *Public Health disease notification*
- *Telemedicine*
- *Personal Health Records*



Somewhere, something went terribly wrong

Paper Isn't Safe Either

How do you dispose of records? Janitor sells one hospital's for \$40

09/22/2010

A recent patient data breach at a California hospital highlights the importance of securely storing and properly disposing of paper patient records, *HealthLeaders Media* reports.

Investigators last week discovered that a janitor working at **Martin Luther King, Jr. Multi-Service Ambulatory Center** in Willowbrook sold 14 boxes containing 33,000 paper patient records to a recycling center for \$40. The hospital in July noticed the missing records, which listed patient addresses, phone numbers and other demographic information. The janitor was charged with felony commercial burglary, *HealthLeaders Media* reports.



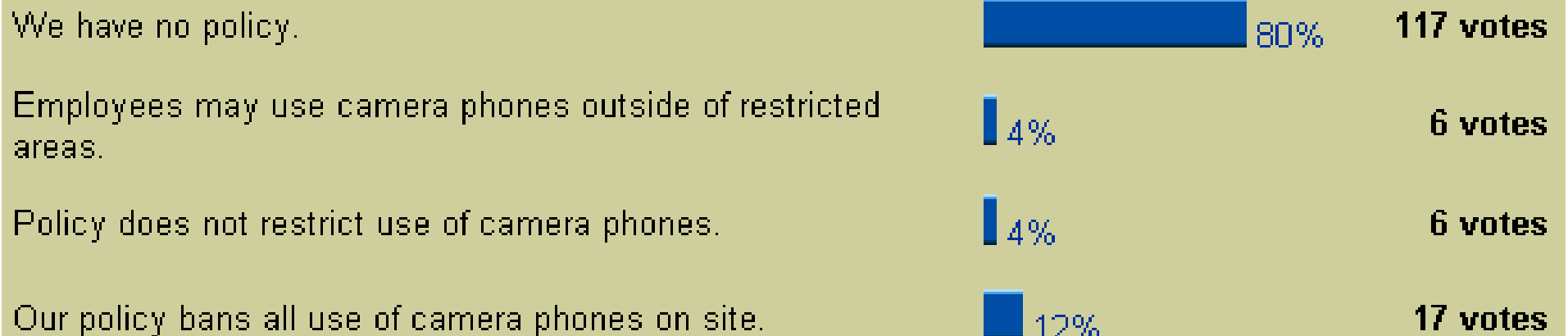
- **Proliferation of mobile devices and data**
- **Laptops, PDAs, Smart Phones, USB Memory Devices, Storage Cards, Blackberries, Converged Devices, Clinical Devices**

Data Loss Isn't Just From EMRs

SHRM HRTX Online Poll Results

What's your company policy on the use of camera-equipped cell phones?

146 total votes



In HIT, “Safe” Has Many Meanings

Some things to consider:

Is your data safe from:

- *loss of access (e.g., downtime)?*
- *deletion during downtime recovery?*
- *corruption during exchange?*
- *inappropriate viewing by others?*



Downtime – Loss of Access to Your Data



Squirrel Catches Fire, Brings Down Data Center

On an otherwise uneventful day a squirrel makes its way into a crevice that opens into the main power switches of a data center. It suddenly bursts into flames and triggers an emergency shutdown of the data center. Key systems are down for 6 hours plus time for data recovery.

Dr. Sue is treating a critical patient in the ICU. She clicks to check a blood gas level, but nothing happens. She suddenly has no idea how much fluid the patient has had or what their vital signs have been.

Sam, a young nurse, just entered his note on a complex patient. As he hits “save”, the system goes down. He realizes he is going to have to re-document their care entirely on paper, which he has never done.

Luckily no one died...

The above scenario is fictional, for instructional purposes only

Deletion Of Your Data During Downtime Recovery



Wrong Update File Applied, Restoration File Corrupt

On an otherwise uneventful day an analyst was upgrading a test file and accidentally applied the upgrade against the production system. For the next six hours, the system functioned erratically, eventually going down. Because of the problem existed over the time that a backup copy was taken, the data restoration had to go back to the previous backup, with a loss of over 6 hours of information.

Dr Sue went “blind” again regarding patient data for 20 minutes until a Downtime Viewer became available.

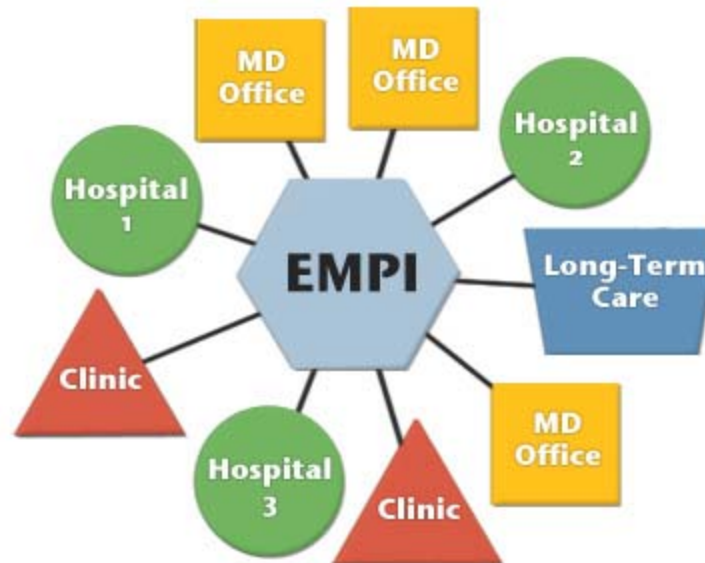
Sam the nurse knew how to work on paper...

Teams were emergently deployed to back enter all ADTs, lab and radiology orders and synchronize results, and back enter all clinical orders. It took months to get the financials cleaned up, but key clinical information was lost forever.

Again, no one died...

The above scenario is fictional, for instructional purposes only

Data Losses Through Corruption in Health Exchange



Wrong Identifiers Matched

On an otherwise uneventful morning Jo Smith felt right-sided abdominal pain. She ignored it as it increased in intensity because she didn't have the money for a doctor. She was found unresponsive by her roommate and was taken to the ER where her community records were matched through the Health Information Exchange.

Unfortunately another Jo Smith had records in the HIE and the physicians matched the two mistakenly. The other Jo had her appendix removed laproscopically. When the physicians saw her community record they focused on obstetrical/gynecological problems because the records showed that Jo didn't have an appendix. It was almost too late when they realized their error... *(the reverse of not matching your records is also possible and can lead to errors)*

The above scenario is fictional, for instructional purposes only

Data Loss Through Inappropriate Viewing







An All Too Common Occurrence

Kaiser fires workers for snooping in octuplet mom's records

By Jaikumar Vijayan, Computerworld

March 31, 2009 05:50 PM ET

 Share/Email  Tweet This  Comment  Print

 Newsletter Sign-Up

A Kaiser Permanente hospital located in a Los Angeles suburb has fired 15 employees and reprimanded eight others for improperly accessing the personal medical records of Nadya Suleman, the California woman who gave birth to octuplets in January.

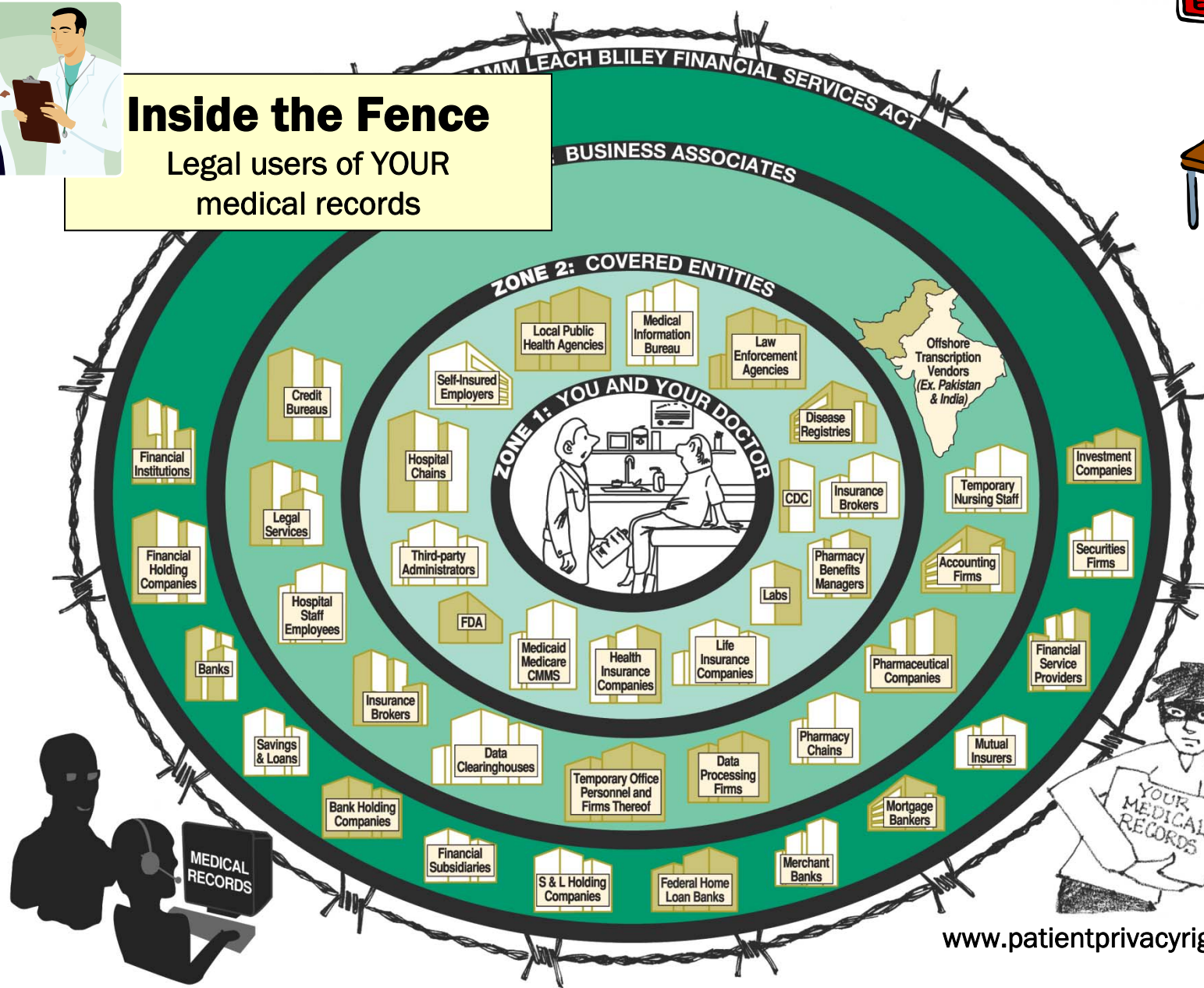
[Podcast: Who's Stealing Your Data?](#)

Inappropriate Viewing – Legal Versions



Inside the Fence

Legal users of YOUR medical records



www.patientprivacyrights.org

Personal health information is for sale

Table 1: Sample Data Elements for Commercial and Medicare Databases

Demographic	Medical Information (Inpatient and Outpatient)	Health Plan Features	Financial Information	Drug Information	Enrollment Information
Patient ID	Admission date and type	Coordination of benefits amount	Total payments	Generic product ID	Date of enrollment
Age	Principal diagnosis code	Deductible amount	Net payments	Average wholesale price	Member days
Gender	Discharge status	Copayment amount	Payments to physician	Prescription drug payment	Date of disenrollment
Employment status and classification (hourly, etc.)	Major diagnostic category	Plan type	Payment to hospital	Therapeutic class	
Relationship of patient to beneficiary	Principal procedure code		Payments—total admission	Days supplied	
Geographic location (state, ZIP Code)	Secondary diagnosis codes (up to 14)			National drug code	
Industry	Secondary procedure codes (up to 14)			Refill number	
	DRG			Therapeutic group	
	Length of stay				
	Place of service				
	Provider ID				
	Quantity of services				

Potential Future Directions

Security Issues in the Real World

- Networks not integrated necessitating data transfers
- Doctors' PCs largely uncontrolled and unprotected
- Workstations often shared among several people
- Data unencrypted and devices unsecured



Americans Want to Control Who Can See & Use Their Information

- “Researchers would be free to use my personal medical and health information without my consent at all” 1%
- 99% of the public want to be asked, even if it is for the “greater good.”

IOM Survey Findings on Health Research and Privacy, Dr. Alan F. Westin, October 2, 2007

Selected Physical Protection Mechanisms

- Locks
- Failed authentication data wipes
- Passwords vs Biometrics/Smart Cards
- Data encryption/VPNs

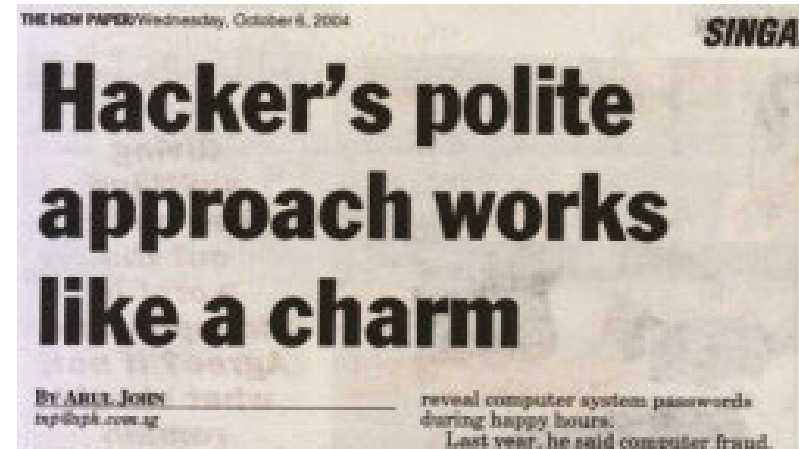


Selected Device Configuration Protection Mechanisms

- Turn off certain capabilities not required for use
- Implement all relevant security features available
- Disable discoverable and connectable options (e.g. Bluetooth)
- Do not store confidential information on devices unless necessary

Social Engineering

Do use your system access rights to let someone else on the system



Privacy: The Achilles Heel of Health Information Exchange

“Anyone today who thinks the privacy issue has peaked is greatly mistaken...we are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope.”

Forrester Research



Is HIE a Golden Apple?

The Privacy Answer: Personal Health Records

- PHRs managed by patients are the ultimate HIE
- Tools for data selection and transmission are needed:
 - Guidance from professional societies as to what info is needed – and not needed – for referrals and emergencies
 - The equivalent of “H&R Block” and “Quicken” for the PHR to help individuals manage their PHRs, including addressing inconsistencies and duplications
- With compensated primary care physician support, this could be in place quickly

*THSA: “Future EHRs will likely **separate data** (allowing input from registries and personal health records), **applications** (allowing calculations to be done by web services), **and presentation** (allowing physicians to customize their user interface much like customizing a homepage)”*

“Even if you're on the right track, you'll get run over if you just sit there”

-Will Rogers

Thank You

joseph.schneider@bhcs.com