Becky Williams
Chair, HIT/HIPAA Practice

Edwin Rauzi
Partner

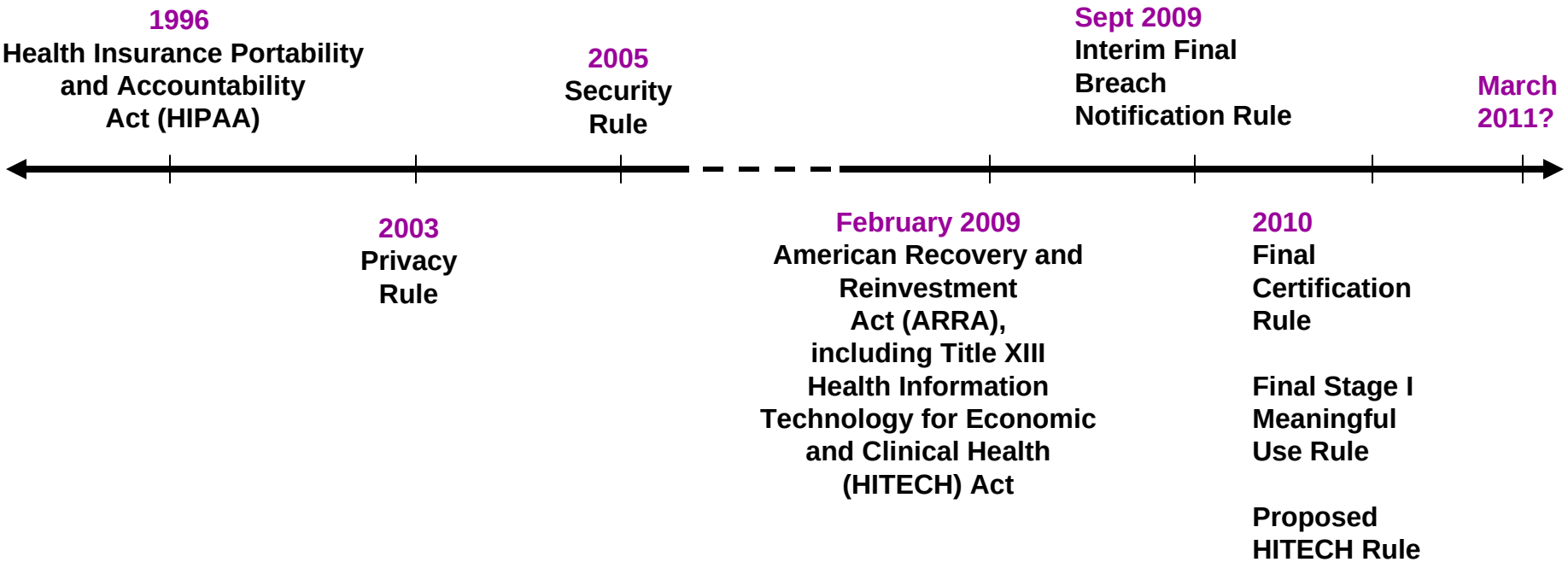
Randy Gainer
Partner

Techno-News

all the acronyms that fit

Health Information and Technology Update

The New ARRA Reality (Or ARRA You Ready)



What Hath ARRA Wrought?

- Carrots and Sticks – Meaningful Use
  - Incentives to become meaningful users of certified interoperable EHR technology
  - Eventual penalties for those who resist
  - Much to do in a little time
- Breach Notification
  - First Federal breach notification law
  - Joining the vast majority of states that require breach notification
  - Granddaddy of breach laws - California
  - HHS published interim final regulations

What Hath ARRA Wrought?

- Big changes for Business Associates
  - Direct obligations to comply with most of the Security Rule
  - Direct obligations to comply with privacy requirements under business associate contract
  - Clarification of who is considered a business associate (e.g., HIEs, HIOs, certain PHRs)

What Hath ARRA Wrought?

- Expanded access requirements
- More disclosures to include in accountings
- Prohibition on the “sale” of PHI
- Changes to marketing restrictions – remuneration changes the game
- Increased penalties and expanded enforcement approaches

Around the Next Corner

- Final rule to bring HIPAA into conformity with ARRA
- Potential implications for covered entities:
  - Revise business associate contract templates
  - Amend all existing business associate contracts
  - Update HIPAA policies and procedures
  - Revise notices of privacy practices
  - Revisit breach notification policies and procedures
- For business associates:
  - Risk analysis/risk management
  - Policies and procedures: security, breach notification, privacy
  - Potential expansion of who is a business associate (subcontractor)
  - Business associate contracts/Subcontractor agreements

Meaningful Use

- Facts
- Figures &
- ***Relevant Ratios***

Facts

- Checks are being mailed, direct deposits are being made, but only for--
  - Certified software
  - Used in ways that are “meaningful”
- Two sovereigns must be obeyed
  - ONC certifies the software
  - CMS defines the meaningful use of that software

Facts

- Certified software comes in two types
  - All the data that's fit to capture
  - Specific modules for specific tasks
  - The tale of the TA (Troubling Answer) to the FAQ
- Applicants come in two types
  - Eligible Hospitals
  - Eligible Professionals
- Payments originate from two accounts
  - Medicare
  - Medicaid

Facts

- EHR Goals come in two flavors
  - Objective
  - Measure

- ***Objective***. Maintain an up-to-date problem list of current and active diagnoses.

- ***Measure***. More than 80 percent of all unique patients admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have at least one entry or an indication that no problems are known for the patient recorded as structured data.

- If one person is thinking “objective” when conversing with another, and the other is thinking “measure,” opportunities for misunderstanding abound.

Facts

- In terms of performance, the final deal from the Hospital/EP side is unknown
  - Viewed in the abstract, the Stage 1 measures don't seem all that meaningful
  - Hospital software rollouts don't occur in the abstract, and—in most parts of the country—it's not clear that EP rollouts have a precedent
  - Stage 2 measures are being defined so that they can be proposed and elicit comments
- The federal government can't spend billions in response to a glorified e-mail without an excruciating amount of detail.

Figures

TABLE 17: Payment Scenarios For Medicaid EPs Who Begin Adoption in the First Year

Calendar Year	Medicaid EPs who begin adoption in					
	2011	2012	2013	2014	2015	2016
2011	$21,250	----------	----------	----------	----------	----------
2012	$8,500	$21,250	----------	----------	----------	----------
2013	$8,500	$8,500	$21,250	----------	----------	----------
2014	$8,500	$8,500	$8,500	$21,250	----------	----------
2015	$8,500	$8,500	$8,500	$8,500	$21,250	----------
2016	$8,500	$8,500	$8,500	$8,500	$8,500	$21,250
2017	----------	$8,500	$8,500	$8,500	$8,500	$8,500
2018	----------	----------	$8,500	$8,500	$8,500	$8,500
2019	----------	----------	----------	$8,500	$8,500	$8,500
2020	----------	----------	----------	----------	$8,500	$8,500
2021	----------	----------	----------	----------	----------	$8,500
TOTAL	$63,750	$63,750	$63,750	$63,750	$63,750	$63,750

Figures

Figure 1--Incentive Payment Calculation for Subsection D Hospitals

Incentive Amount = [Initial Amount] x [Medicare Share] x [Transition Factor]

Initial Amount = $2,000,000 + [$200 per discharge for the 1,150th – 23,000th discharge]

Medicare Share = *Medicare*/(*Total*Charity Care) = [M/(T*C)]*
M = [# of Inpatient Bed Days for Part A Beneficiaries] + [# of Inpatient Bed Days for MA Beneficiaries]
T = [# of Total Inpatient Bed Days]
C = [Total Charges – Charges for Charity Care*]/[Total Charges]
*If data on charity care is not available, then the Secretary would use data on uncompensated care as a proxy. If the proxy data is not also available, then "*C*" would be equal to 1.

Table13: Transition Factor

Consecutive Payment Year	Transition Factor
1	1
2	¾
3	½
4	¼

Relevant Ratios

(Where do they come up with these numbers?)

"For situations in which there is an existing standard of practice and complying is fundamentally within the provider's control and where the objective relies solely on a capability included as part of certified EHR technology and is not, for purposes of Stage 1 criteria, reliant on the electronic exchange of information, for the final rule, we adopt, the reasonably high threshold of 80 percent."

Relevant Ratios

(Where do they come up with these numbers?)

"For other situations, where the objective may not be fundamentally within the provider's control and is not an existing standard of practice, but where objective continues to rely solely on a capability that is included as part of certified EHR technology and is not reliant on electronic exchange of information, we are setting the percentage at 50 percent. This was the most commonly recommended percentage for these objectives that rely solely on a capability included as part of certified EHR technology and do not rely on the electronic exchange of information."

Relevant Ratios

- *Denominator:* Number of unique patients seen by the EP or admitted to an eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) during the EHR reporting period.

- *Numerator:* The number of patients in the denominator who have at least one entry or an indication that no problems are known for the patient recorded as structured data in their problem list.

- *Threshold:* The resulting percentage must be more than 80 percent in order for an EP, eligible hospital, or CAH to meet this measure.

Breach Notification

Costs and How to Avoid Them

California data breach notice requirements

- Cal. Civ. Code § 1798.82 (2003 SB 1386)
- Cal. Health & Safety Code § 1280.15 (2008 SB 541)

Purposes of notice requirements

- To protect individuals from fraud
  - 11.4 million Americans were victims of identity theft in 2010
  - Identity theft cost consumers and businesses more than $54 billion in 2009 (Javelin)
  - Identity theft is the fastest growing white collar crime in America
  - It takes a person an average 150 hours and $900 to resolve fraudulent charges

Purposes for notices (cont'd)

- To encourage businesses to improve their information security practices by mandating disclosure of data thefts.

Types of fraud

- Common types of fraud:
  - Current account fraud – credit card, debit card, phone card
  - Identity theft using an individual's name and SSN:
    - To establish new credit
    - To commit other crimes

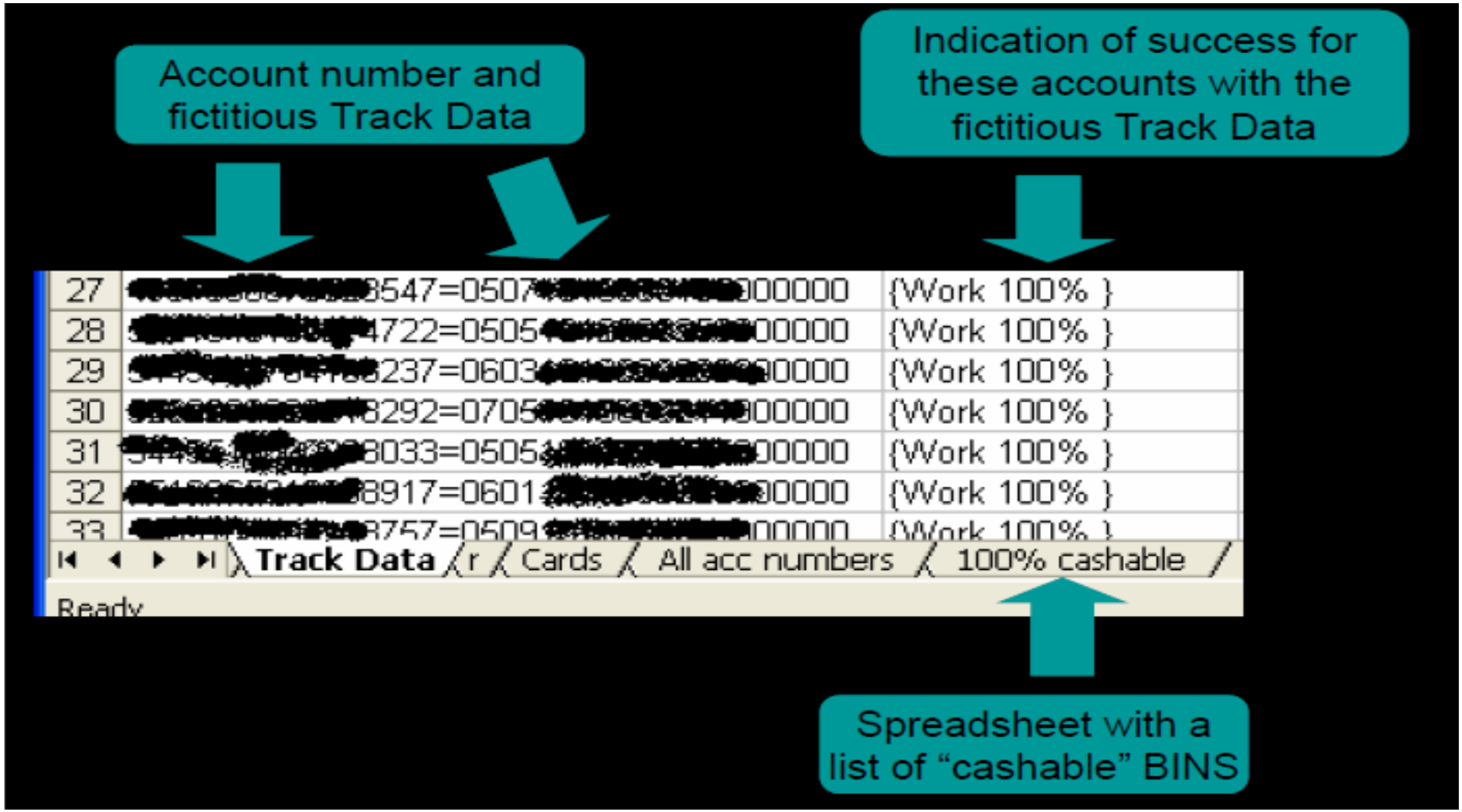
Types of fraud (cont'd)

- Other types of fraud:
  - Driver's licenses
  - Health benefits
  - Insurance fraud
  - Rental housing
  - Utilities
  - Government benefits
  - Fraudulent W-2s
- These may not show up on credit reports for years

Types of fraud (cont'd)

- Targets include anyone with a SSN or payment card
- The thieves' modus operandi:
  - Gain access to large numbers of potential victims
  - Keep a low profile
  - Victimize average consumers over long periods
  - Sell victims' personal information

File Recovered From a Hacker's Computer



Cal. Civ. Code § 1798.82

- Defines “personal information” as a person’s first name or initial, plus last name, plus
  - SSN,
  - Driver’s license or state ID card number, or
  - Financial account number.
  - Medical information (added 2007).
  - Health insurance information (added 2007).

Cal. Civ. Code § 1798.82 (cont'd)

- Became national and international model.
- As of February 15, 2011, 46 states, Washington, D.C., and Puerto Rico have data breach notification laws.
  - Alabama, Kentucky, New Mexico, and South Dakota have not yet enacted data breach notice laws.
- The EU is considering a data breach notice requirements.

Examples of costs incurred

- Online theft of 35,000 payment card datasets (2010):

Additional employee wages	$94,893
Temp. staffing	$82,773
Forensic investigation	$93,020
PCI DSS compliance review	$22,200
New hosting service	$185,880
Network redesign	$17,000
New hardware	$65,460
New software	$27,241
Legal	$30,000
Customer notices, call center, credit restoration services ($6.25/customer)	$218,750
Lost business during temporary shutdown	$159,784
Visa/merchant bank fines	$5,000
Total	**$1,002,001**

Examples of costs incurred

- In December 2005, a thief stole backup discs and tapes from the vehicle of an employee of Providence Health & Services.
- The tapes and discs contained unencrypted information about 365,000 patients.

Examples of costs incurred (cont'd)

- A few patients filed a putative class action case against Providence in Oregon state court.
- The trial court dismissed the case because the patients could not show they incurred any damages.
- An appeal is pending.

Examples of costs incurred (cont'd)

- HHS investigated the backup disc and tape theft, as well as several incidents in which Providence laptops were stolen.
  - HHS investigators sent document requests and interviewed witnesses.
  - HHS officials negotiated a Resolution Agreement in 2008.

Examples of costs incurred (cont'd)

- The Resolution Agreement included a three-year Corrective Action Plan ("CAP") that requires Providence to
  - improve its information security practices,
  - train its workforce,
  - monitor compliance with the CAP, and
  - report any additional breaches.

Examples of costs incurred (cont'd)

- Providence backup theft costs 2006-08: approximately $7 million.

Examples of costs incurred (cont'd)

- Providence is meeting its responsibilities under the CAP.
- The key to Providence's success was management's decision to plan, build, and operate first-class information security practices across the five-state, 50,000-employee organization.

Examples of costs incurred (cont'd)

- That led to
  - Hiring a CISO,
  - Creating a new information security management structure,
  - Increasing the number of its info. security employees from five to 18,
  - Rewriting info sec. policies and procedures, and
  - Deploying and managing state-of-the-art info. sec. software.

Examples of costs incurred (cont'd)

- Providence's annual information security costs increased by more than 800% from 2005 to 2009.

Examples of costs incurred (cont'd)

- These cost examples amounted to $28.49 and $18.94 per customer or patient.
- That's less than reported average costs --
  - E.g., Ponemon Institute, for records stolen in 2008:
    - direct costs per record: $50;
    - indirect costs per record (lost productivity, stock price decrease, etc.): $152.

Health & Safety Code § 1280.15

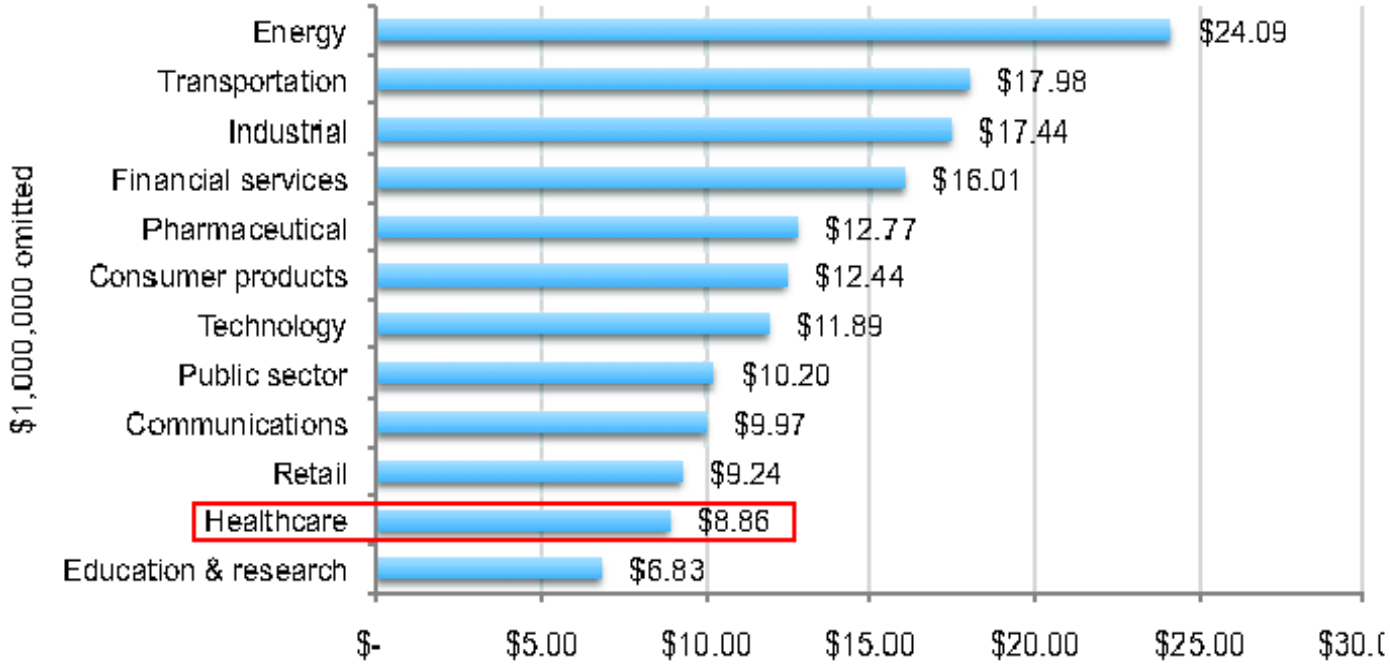
- Applies to hospitals, skilled-nursing facilities, psychiatric health facilities, clinics, home health agencies, and hospices licensed under Ca. laws.
- Covers individually-identifiable information, in electronic or physical form.
- Pertains to any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information.

H & S Code § 1280.15 (cont'd)

- "Unauthorized" means the inappropriate access, review, or viewing of medical information without a direct need for medical diagnosis, treatment, or other lawful purpose under any state or federal law.
- Requires notice to patient and Ca. Dept. of Public Health within five business days after detection.
- H & S Code § 1280.15 is a "hard trigger" statute.

Healthcare providers spend less than other industries to comply with data security requirements

Figure 10: Total compliance cost by industry
Computed from 46 benchmarked companies

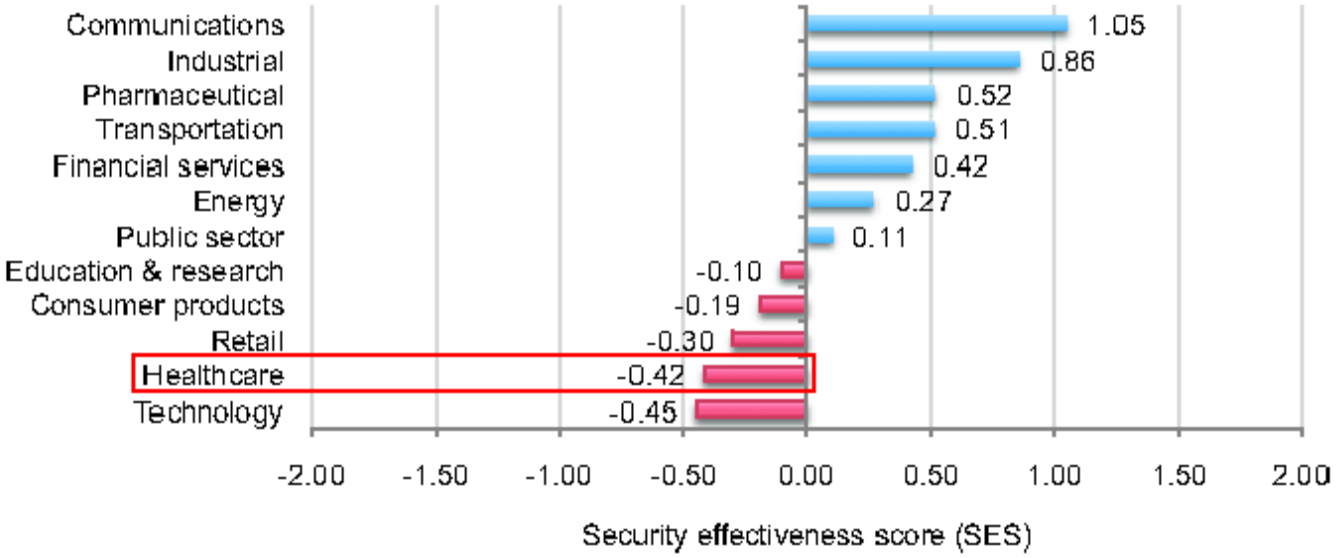


Ponemon Institute, "Cost of Compliance," BNA Vol. 10, No. 6 *Privacy & Security Law Report* 217 (Feb.7, 2011)

Davis Wright Tremaine LLP

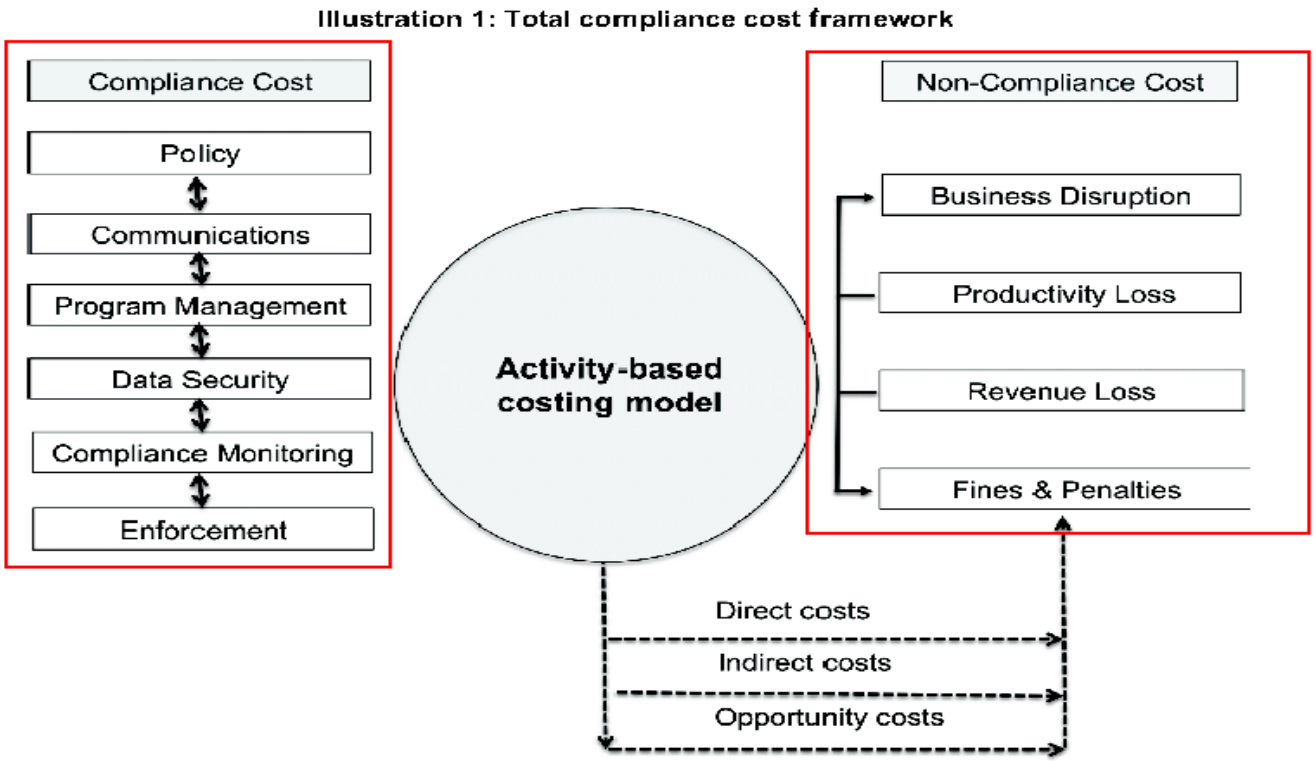
The Security Effectiveness Score for healthcare is lower than for other industries

Figure 16: Security effectiveness score for 12 industry segments
Computed from 46 benchmarked organizations



Ponemon Institute initially developed the Security Effectiveness Score in its 2005 Encryption Trends Study. The purpose of the SES is to define the security posture of responding organizations. The SES is derived from the rating of 25 leading information security and data protection practices. This indexing method has been validated from more than 30 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). An index value above zero is net favorable.

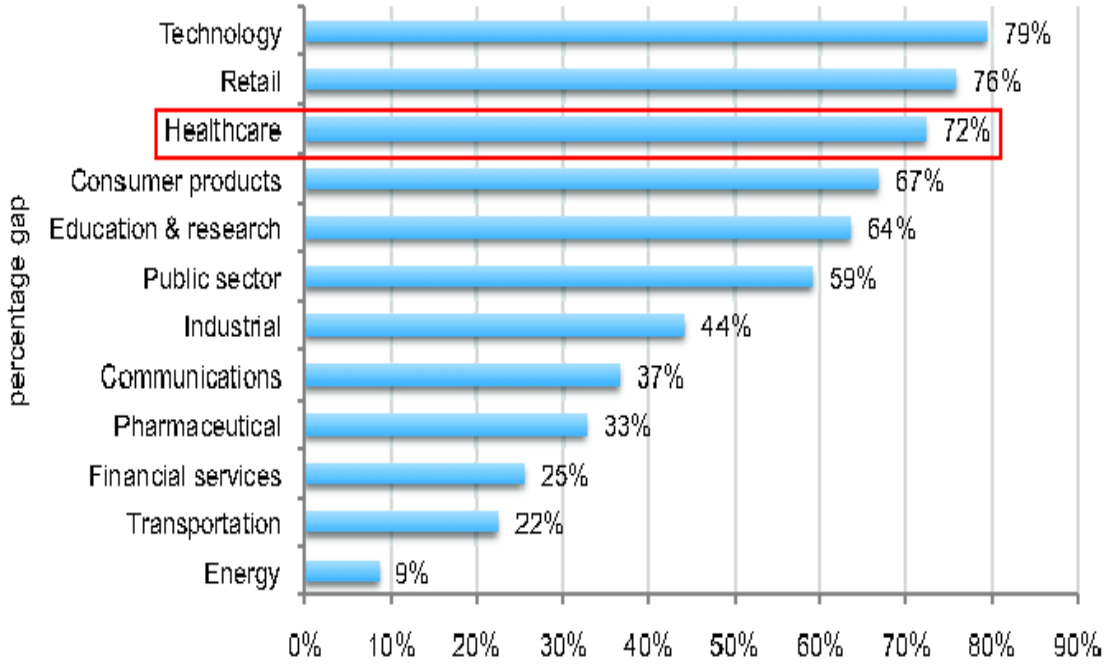
Failure to invest in security measures saves compliance costs but increases non-compliance



Davis Wright Tremaine LLP

Healthcare's percentage of non-compliance costs as a per cent of total costs is high.

Figure 11: Percentage gap between non-compliance and compliance cost by industry
Computed from 46 benchmarked companies

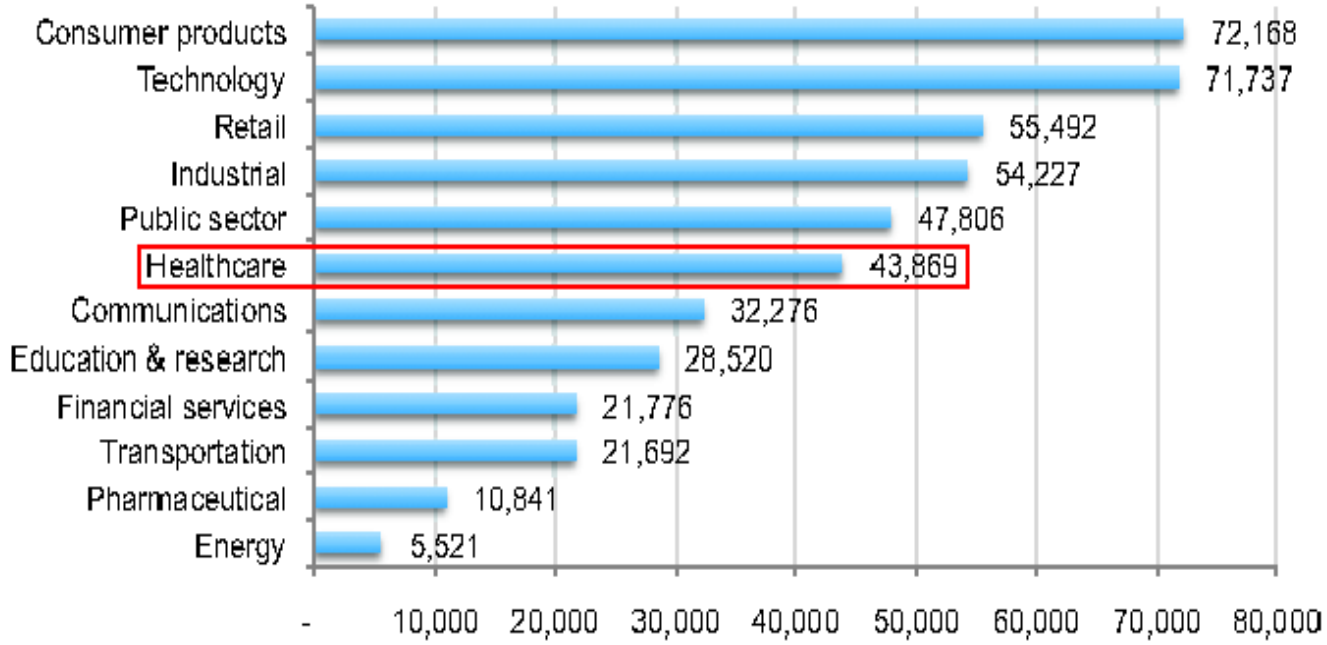


Pct% gap = [NC – CC]/TC, where NC = non-compliance cost,
CC = compliance cost and TC = [NC + CC] = total compliance cost.

Davis Wright Tremaine LLP

Healthcare providers experience more compromised records than other industries.

Figure 12: Average number of compromised records by industry
Computed from 46 benchmarked companies



Proactive steps to avoid breaches

Educate all staff that may access medical information only if they have a direct need

- to make a medical diagnosis,
- for treatment, or
- for another lawful purpose.

Correct all security vulnerabilities, e.g.,

- institute secure transport and storage of backup tapes;
- encrypt personal information on all portable devices;
- install “lojack” (“call home”) software on laptops;
- deploy software to prevent data leakage through outgoing emails;
- ensure that audit logs are retained;
- implement automated auditing of logs;

Steps to avoid breaches (cont'd)

- Correct all vulnerabilities, e.g. (cont'd):
  - ensure that video surveillance of areas where info. is stored is functioning;
  - hire staff to implement and monitor firewalls or outsource that work;
  - install and monitor intrusion detection and prevention systems;
  - ensure that anti-virus software is consistently maintained and patches are always installed; and
  - harden servers and operating system software by turning off unneeded features.

. . . so, stay tuned!

Becky Williams
206.757.8171
beckywilliams@dwt.com

Edwin Rauzi
206.757.8127
edrauzi@dwt.com

Randy Gainer
206.757.8047
randygainer@dwt.com

Davis Wright Tremaine LLP