

Indiana Health Industry Forum
Health IT Seminar Series
Privacy and Security

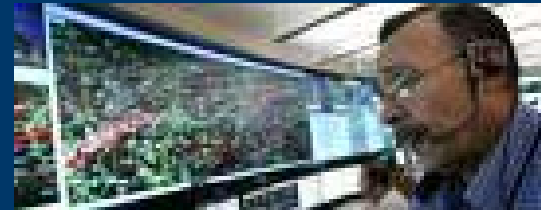
November 10, 2009

*Joan Antokol, Esq.
Partner, Baker & Daniels LLP
Head, Privacy and Information Management Subgroup*

Privacy and Security Affect All of Us

Cyberspies penetrate US electrical grid

Wed Apr 8, 2009

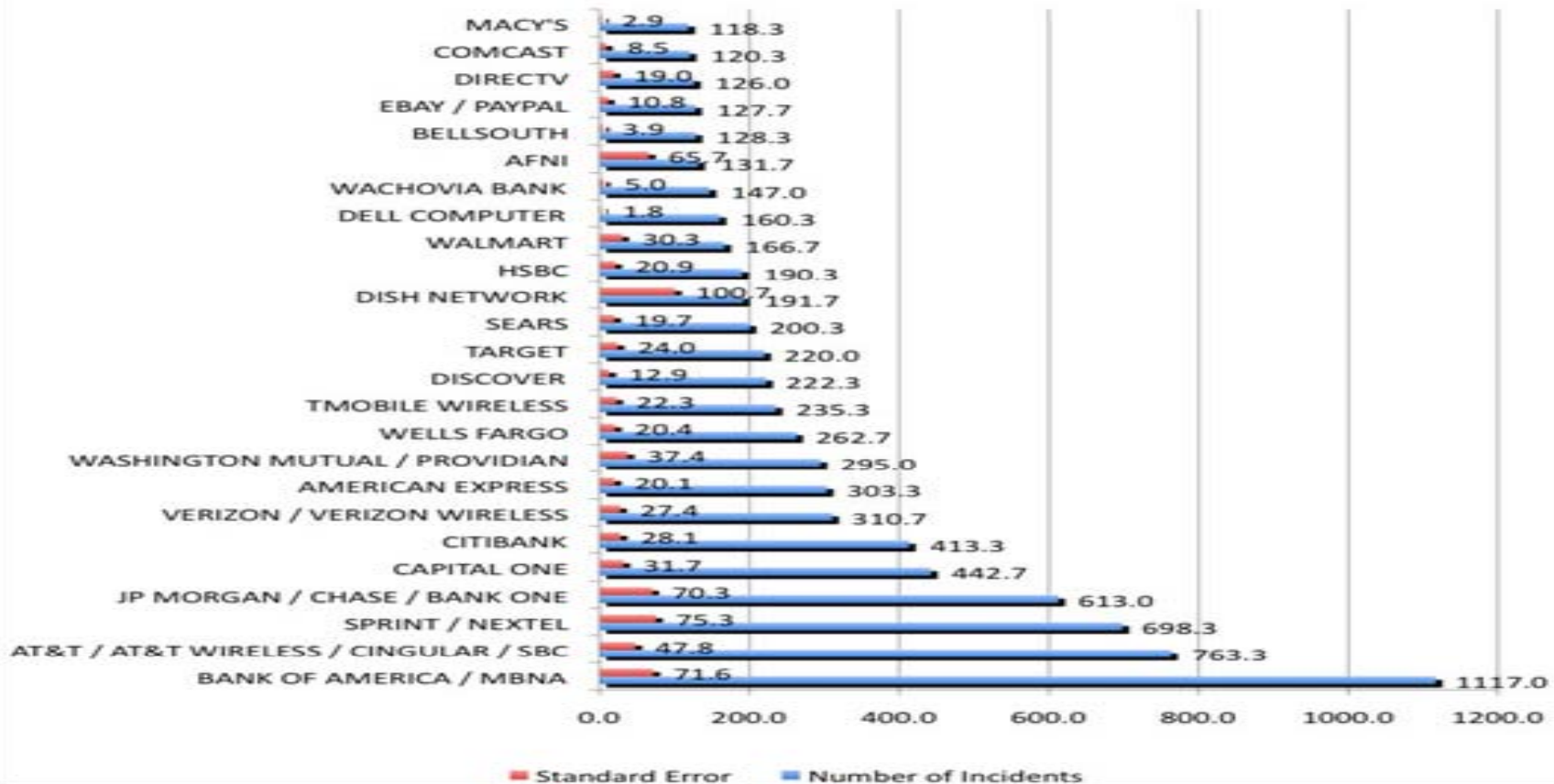


WASHINGTON (Reuters) - Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, the Wall Street Journal reported on Wednesday.

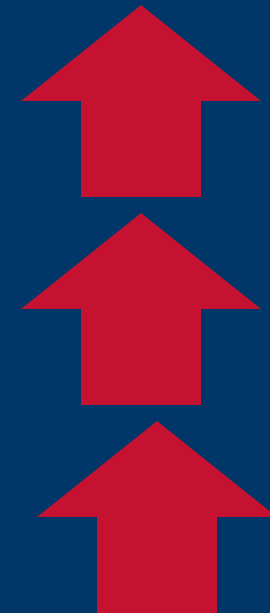
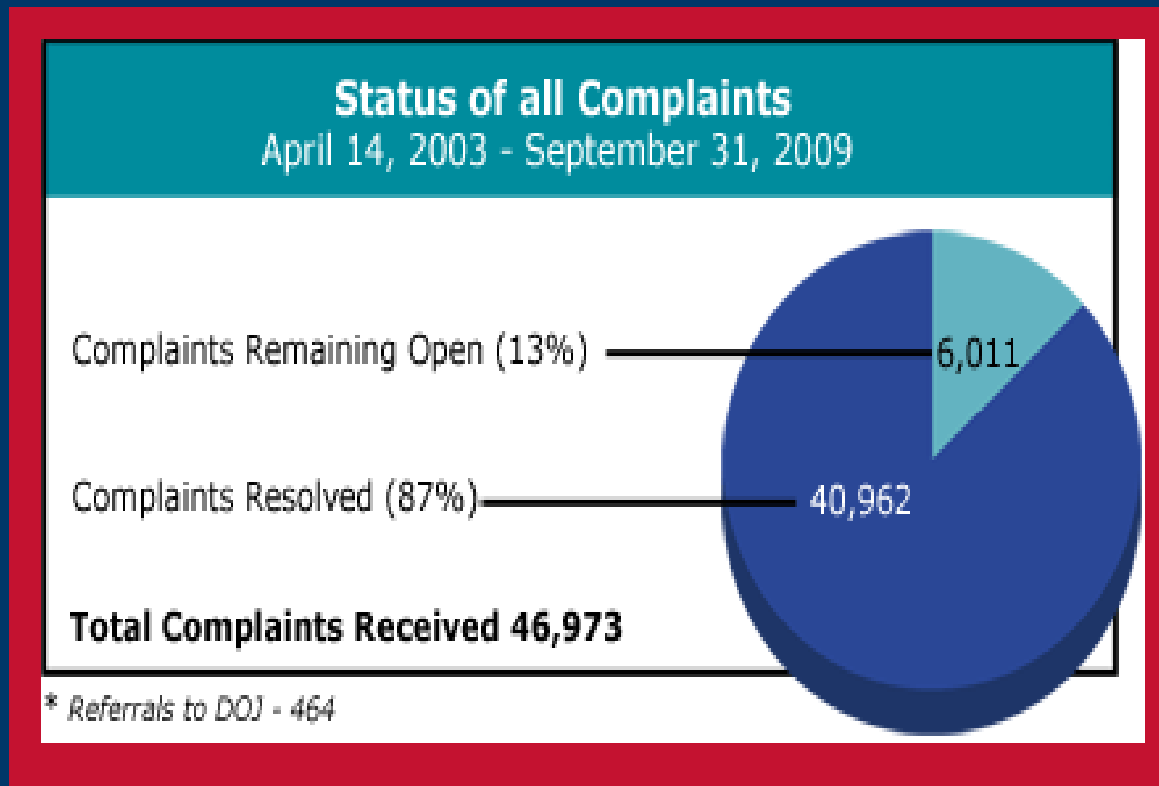
China, Russia and other countries were believed to be on a mission to navigate the U.S. electrical system and its controls, the newspaper said, citing current and former U.S. national security officials.

The Risks You Face with Popular US Retailers

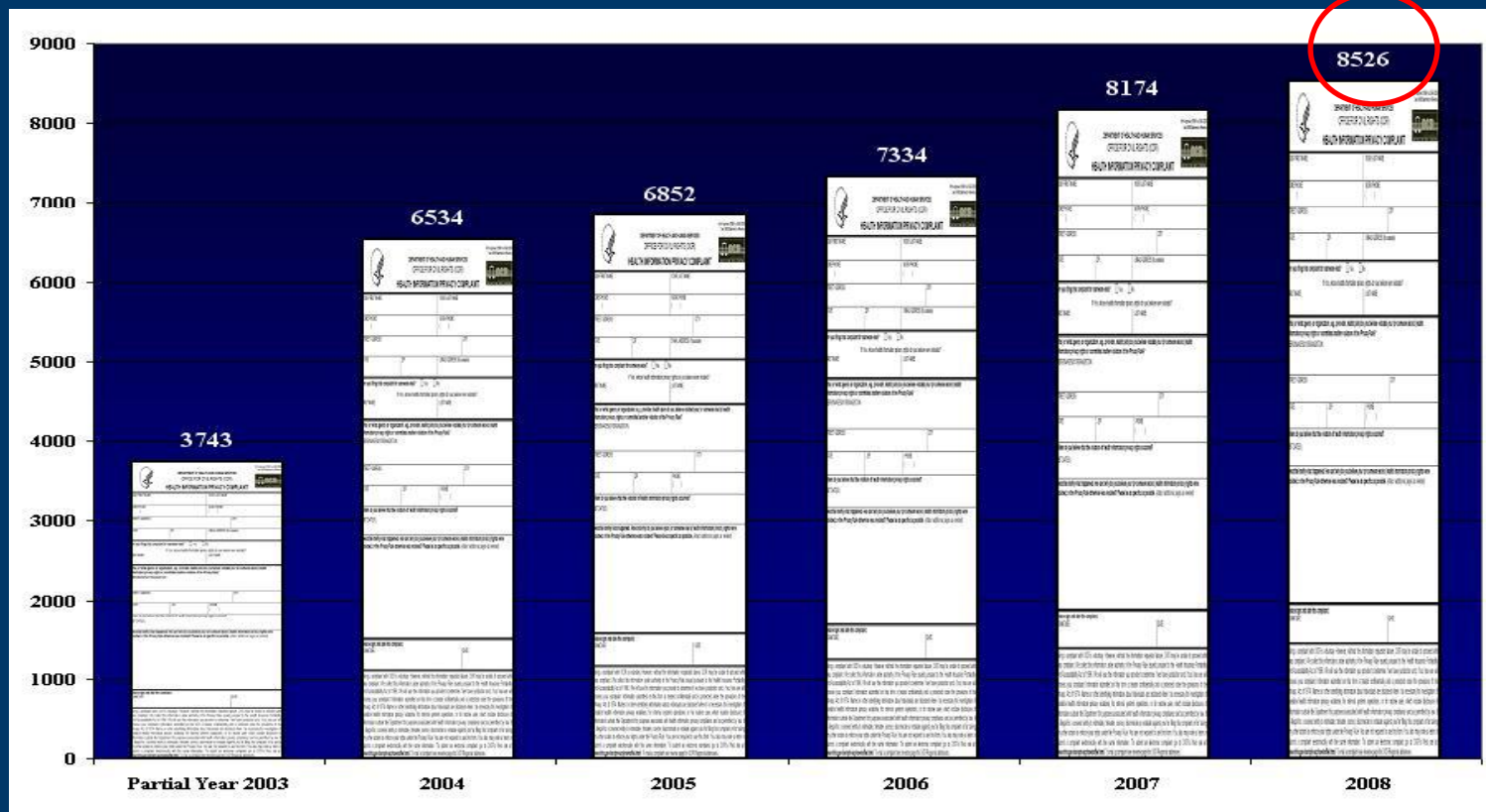
**Incidents Per Month (Average of Jan., Mar., Sept. 2006)
Among Institutions With High Frequency of Complaints**



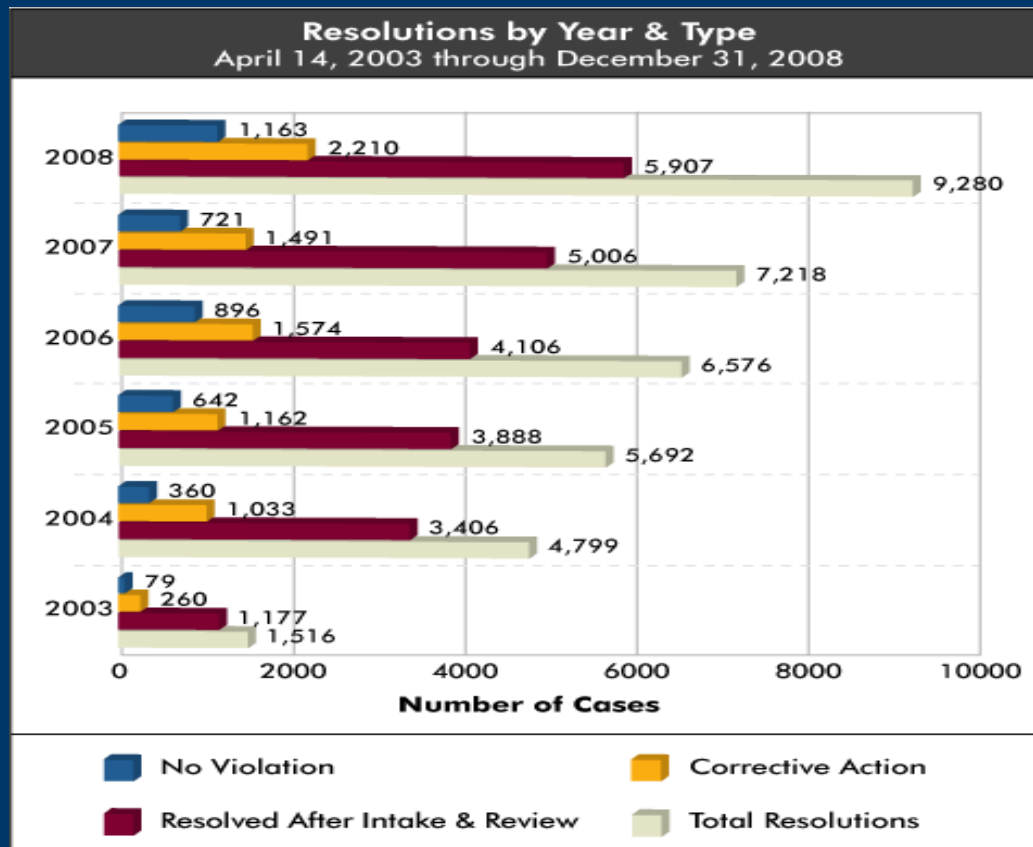
HIPAA Privacy Rule Complaints



HIPAA Privacy Rule Complaints By Year



HIPAA Privacy Rule Resolutions By Year and Type



Top Five Allegations in HIPAA Privacy Rule Complaints

- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access to their protected health information;
- Uses or disclosures of more than the Minimum Necessary; and
- Lack of or invalid authorizations for uses and disclosures of protected health information

Top Targets for HIPAA Privacy Rule Complaints

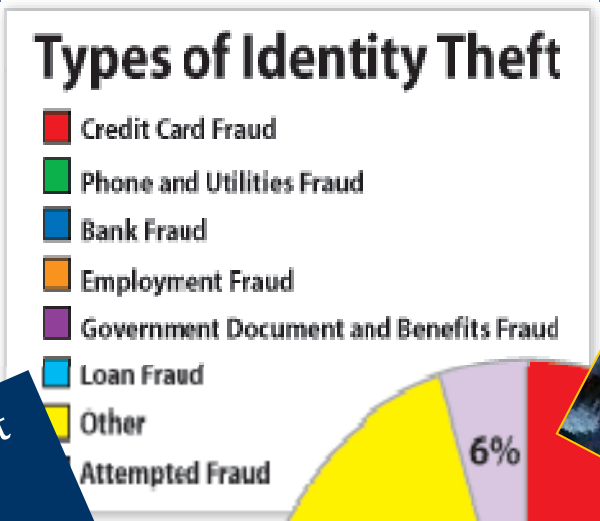
- Private Practices
- General Hospitals
- Outpatient Facilities
- Health Plans (group health plans and health insurance issuers)
- Pharmacies

Public Enforcement



and many smaller ones.....

The Current Landscape



1 out of 700 hackers are caught and prosecuted

Data Hijacking On the Rise-Is Your Business Next??

Citibank Hackers Blamed for Alleged ATM Crime Spree



Key Pieces of Information Involved in Identity Theft



A US resident's identity is stolen at least every two minutes.
 One in seven hundred identity thieves are caught and prosecuted.

Medical Records Are a Key Target

Insiders and External Thieves



UCLA's medical record spying problem worse than thought

Medical Record Breaches on the Rise

Google Health Goes Live
May 19, 2008 At a press-packed, early morning event, Google launched its long anticipated health initiative, Google Health today.

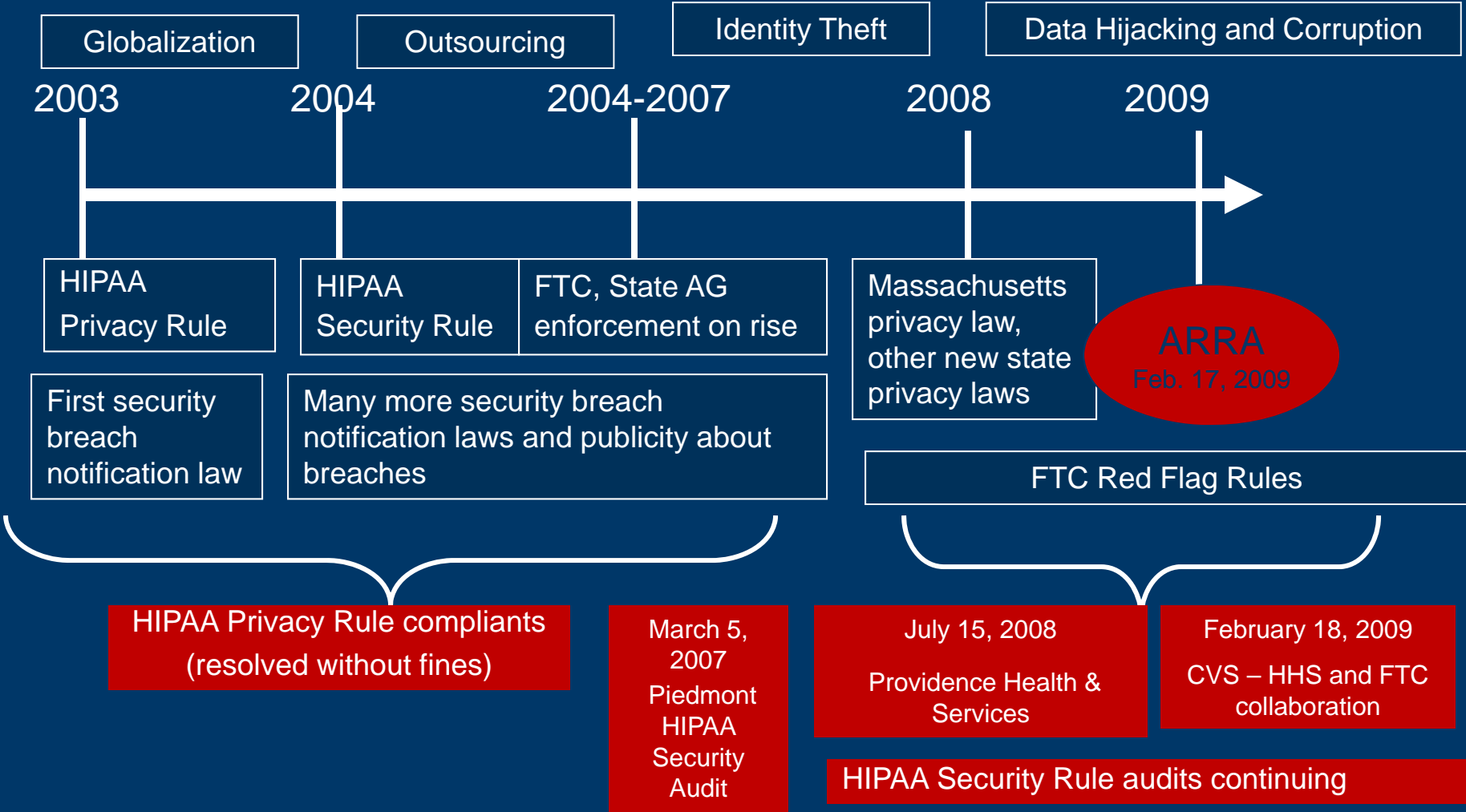
IDENTITY THIEVES TARGETING MEDICAL INFORMATION

California's breach disclosure law now covers medical records

University of Florida said to be a 'natural target' for ID theft

Proliferating HIPAA complaints and medical record breaches

Pre-ARRA – Legal Framework



Pre-ARRA HIPAA Security Rule Complaints

- Complaint-driven enforcement
- Very few complaints filed through 2006
- CMS criticized by OIG for lax compliance, insufficient enforcement
- OIG found significant violations at 8 hospitals that it audited
- March 5, 2007 – first CMS audit (Piedmont Hospital)
- Reportedly auditing 50 hospitals per year – via unannounced audits

Pre-ARRA Security Breach Notification Requirements

- State security breach notification laws
- Varying requirements
- No federal security breach law
- HIPAA Privacy Rule – disclosure log only



ARRA – Overview

- Significant changes to the US privacy and security landscape
- Increasing scrutiny, enforcement on the way (federal and state)
- Expect great deal of uncertainty – as with HIPAA

ARRA—Key Changes

“Improved Privacy Provisions and Security Provisions”

- Security breach notifications
- Broader HIPAA scope of coverage (and enforcement)
- Additions and modifications to certain HIPAA requirements
- New HHS inspection and enforcement framework
- New tiered penalties for federal *and* state regulators
- Varying effective dates for different sections

Security Breach Notifications

- First federal security breach notification requirements
- Expanded scope of when notification is triggered for covered entities
- Business associates required to notify covered entities about breaches
- Third parties involved with personal health records also *temporarily* covered
- Breach: An individual's protected health information [in "unsecured" form] that has been, or is reasonably believed by the covered entity to have been accessed, used, acquired or disclosed to an unauthorized person, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
- Exception for unintentional access by employees or individuals acting under authority of covered entity or business associate if information is not used or disclosed by recipient or anyone else.
- "Unsecured" form [forthcoming Guidance]
- Includes information in any format – ePHI, paper, tapes, etc.

Security Breach Notifications, Continued

- Notify without unreasonable delay and at least within 60 day timeframe
- 60 days begins to run from the date the covered entity or business associate or any employee, officer or other agent of the covered entity or business associate knew or reasonably should have known about the breach
- Very limited law enforcement exception to 60-day timeframe
- Method of notice (new obligations):
 - Content of notification
 - Transmission requirements
 - HHS notification
 - Publication obligations (homepage of website, media, HHS website)
 - Disclosure log
- Temporary notification requirements for non-HIPAA covered entities (vendors of personal health records)—notify FTC in place of HHS. Provision will sunset if FTC enacts other regulation that applies.

Broader HIPAA Scope of Coverage

- Business associates
- Other third parties (who are now clearly business associates)
- Another category of third parties who are not business associates under ARRA, but may be considered business associates under a forthcoming evaluation (before February 17, 2010)

Business Associates

Pre-ARRA	ARRA	Comments
BA's contractually bound to certain HIPAA requirements.	Statutorily bound to all HIPAA Privacy and Security Rule requirements, including new requirements in ARRA.	Some BA's might not be able to comply. HIPAA Security Rule obligations will be a challenge.
Covered entity legally responsible for ensuring appropriate BA agreement. No requirement for BA agreements between covered entities.	BA and covered entity both responsible for ensuring appropriate BA agreement. Specific requirement to update all BA's, consistent with new ARRA obligations.	Recommend evaluation of BA for ability to comply too.
HIPAA enforcement and penalties do not apply directly to BA's.	HIPAA enforcement and penalties apply directly to BA's.	Unclear whether violations by BA will be applied to covered entities.
No right for HHS to audit BA's.	HHS has the right to audit BA's and must publish results.	Much greater scrutiny of BA's.

Additions and Modifications to Certain HIPAA Requirements

- Disclosure log – now includes treatment, payment, healthcare operations
- Patient access rights – electronic records, 3 years for accounting (not 6)
- Patient access rights to information from BA's (two options)
- Minimum necessary – applies to treatment disclosures too, new guidance
- Additional restrictions on use of PHI without a valid authorization

New Inspection and Public Posting Requirements

- HHS required to conduct inspections of covered entities
- Inspections of business associates
- Publication of inspections, general findings
- Publication of security breaches on HHS website

New Security Breach Enforcement Requirements

- Attorney Generals can bring state actions for violations under ARRA
- However, cannot bring an action while an HHS action is pending
- Individual right to a percentage of the government's fine – forthcoming guidance

New Enforcement Requirements

- As noted previously, business associates now fall directly under HIPAA enforcement
- ARRA makes clear that HIPAA enforcement applies to *individuals* as well as organizations that are covered
- New tiered enforcement – willful violations result in highest penalties

Effective Dates

- Vary by section
- Many sections effective on February 17, 2010
- Some contingent on passage of additional guidance documents
- Penalty section (including state enforcement) effective immediately

Tips and Recommendations

- Increasingly complex legal requirements – state, federal, global
- Recommend overall risk management approach
- Specific individuals for privacy and security (two roles)
- Written policies and procedures for privacy and security
- Policies should be approved by senior management, consistent, accurate. Do not make promises that you cannot keep.
- Ongoing vigilance required – changing threats, new laws, new guidances

Tips and Recommendations, Continued Business Associates

- Overall vendor management approach
- Pre-screening of vendors including business associates
- Proper agreements – ensure that you have a final copy in place

Tips and Recommendations, Continued Some Key Areas of Consideration

- Security assessments
- Security breach notification process
- Policies and procedures (including Notice of Privacy Practices)
- Training
- Auditing/compliance monitoring
- Litigation risk reduction – proper recordkeeping

Conclusion

- Don't become the next CVS.
- Or the next security breach poster child
- Or the target of state attorneys general
- Don't be fooled into buying things that you don't need (remember the HIPAA scams, like HIPAA-compliant cabinets?)
- Prepare procedures and training programs that are employee-friendly and not overwhelming. The goal is results, not reams of paper.
- Security experts can differ greatly in terms of cost and expertise. Don't be fooled.
- Ensure proper documentation and recordkeeping practices.

Contact Information

Joan Antokol

Partner, Baker & Daniels LLP

Head, Privacy and Information Management Practice Subgroup

600 E. 96th St., Suite 600

Indianapolis, IN 46042

(317) 569-4665 (office)

(317) 937-6903 (mobile)

Joan.antokol@bakerd.com