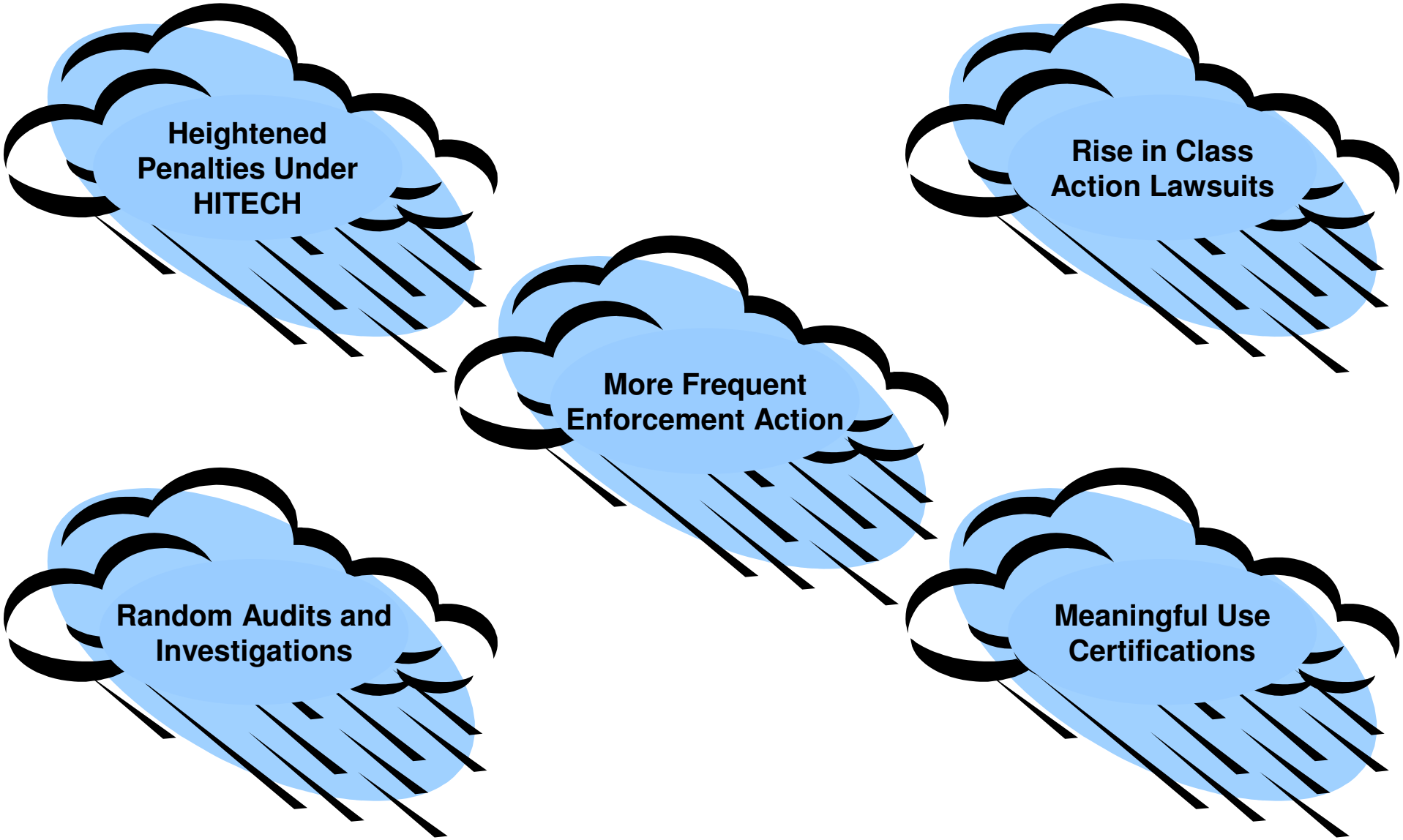
manatt Deloitte.

Managing Heightened Data Privacy Risks

June 11, 2013

Robert Belfort, Esq.
Manatt, Phelps & Phillips, LLP
212.830.7270
rbelfort@manatt.com

The Perfect Storm: Multiple Environmental Changes Heighten Data Privacy Risks



HIPAA Resolution Agreements and Civil Monetary Penalties

Covered Entity	Date	Incident	Penalty
Idaho State University	May 21, 2013	Firewall breach	$400,000
Hospice of Northern Idaho	December 31, 2012	Stolen laptop	$50,000
Massachusetts Eye & Ear	September 17, 2012	Theft of laptop	$1,500,000
Alaska DHSS	June 26, 2012	Stolen USB drive	$1,700,000
Phoenix Cardiac Surgery	April 17, 2012	Posting PHI on publicly accessible website	$100,000
UCLA Health System	July 7, 2011	Employee access to celebrity records	$865,000
Massachusetts General	February 24, 2011	Loss of paper records on train	$1,000,000
Cignet Health	February 22, 2011	Denial of patient access and failure to cooperate with OCR	$4,300,000
MSO Washington	December 13, 2010	Improper use of PHI for marketing purposes	$35,000
Rite Aid	July 27, 2010	Insecure disposal of prescription labels	$1,000,000
CVS	January 16, 2009	Insecure disposal of prescription labels	$2,225,000
Providence Health	July 16, 2008	Loss of backup tapes and laptops	$100,000

Increased HIPAA Civil Penalties Under HITECH

Level of Culpability	Minimum/Maximum Civil Penalty Per Violation	Maximum Annual Penalty for Type of Violation
Entity did not know and could not have reasonably known of the violation	$100/$50,000	$1,500,000
Violation due to reasonable cause but not willful neglect	$1,000/$50,000	$1,500,000
Violation based on willful neglect but corrected upon notice from HHS	$10,000/$50,000	$1,500,000
Violation based on willful neglect and not corrected upon notice from HHS	$50,000	$1,500,000

Breach Notification Routinely Triggers OCR Investigations

- All breaches involving 500 or more individuals must be reported to HHS and are posted on HHS website
- HHS requests information from covered entity after report filed
- If initial submission raises additional questions, further investigation may be conducted

OCR Random Audits Ramping Up

Pilot audit program of 115 covered entities	HHS solicits comments on audit protocol	OCR survey of pilot program experience	Expanded random audit program
November 2011	Early 2012	Spring 2013	Summer 2013	2014

Civil Enforcement Authority of State Attorneys General Under HITECH

- Damages are capped at $100 per violation/$25,000 for all identical violations per year
- Attorney fees may be payable
- AGs can request injunctive relief
- AGs must notify HHS, which has the right to take over prosecution of any case

Original HIPAA Statute

"(a) A person who knowingly and in violation of this part

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section."

42 U.S.C. § 1320d-6

HITECH Revision

"For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization."

HITECH, Section 13409

HIPAA Criminal Cases

Case	Alleged Facts	Disposition
U.S. v. Gibson	Employee of Seattle Cancer Care Alliance used PHI to fraudulently obtain credit cards	Guilty plea on August 19, 2004
U.S. v. Ramirez	Employee of medical practice sold PHI to FBI agents posing as drug traffickers	Guilty plea on March 6, 2006
U.S. v. Williams	Employee of billing company sold PHI to co-conspirator	Guilty plea on April 26, 2006
U.S. v. Ferrer and Machado	Employee of Cleveland Clinic (FL) gave PHI to co-defendant to submit fraudulent Medicare claims	Guilty verdict after trial on April 27, 2007

HIPAA Criminal Cases

Case	Alleged Facts	Disposition
U.S. v. Smith	Clinic nurse disclosed PHI to husband for use in legal proceeding against patient	Guilty plea on December 4, 2008
U.S. v. Howell	Employee of counseling center gave PHI to co-conspirators for credit card fraud	Guilty plea on August 22, 2008
U.S. v. Zhou	Former UCLA Medical Center researcher viewed PHI of celebrities without valid purpose	Guilty plea on January 13, 2010
U.S. v. Jackson	Administrative employee at UCLA Medical Center sold PHI about celebrities to *National Inquirer*	Defendant died before trial
U.S. v. Smith	Health plan employee stole PHI to obtain controlled substances for sale	Guilty plea on May 25, 2011

Lessons Learned From Criminal Cases

- No covered entities convicted
- Absence of criminal enforcement against institutions likely due to fact that:
  - Improper conduct was carried out by low-level personnel
  - Covered entities had reasonable policies and employee training in place
  - Covered entities did not benefit from improper conduct
- Risk of organizational criminal liability highest if disclosure occurs as part of authorized company activity

New Risks From Class Action Litigation

Covered Entity	Incident	Claim
UCLA Health System	Stolen hard drive containing PHI of 16,000 patients	$16 million
Emory Healthcare	Loss of disks of 315,000 patients	$200 million
Tricare	Lost back-up tapes of 4.9 million individuals	$4.9 billion

Risks Raised by Submissions for Meaningful Use Incentives: The False Claims Act

- The False Claims Act makes it illegal to:
  - Knowingly present, or cause to be presented, a false or fraudulent claim for payment to the federal government
  - Knowingly make, use, or cause to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the government
- "Knowingly" defined broadly to include acting with deliberate ignorance or reckless disregard of the facts
- Significant financial sanctions:
  - Damages of up to three times the amount of the false claim ("treble damages")
  - Penalties of up to $11,000 per claim

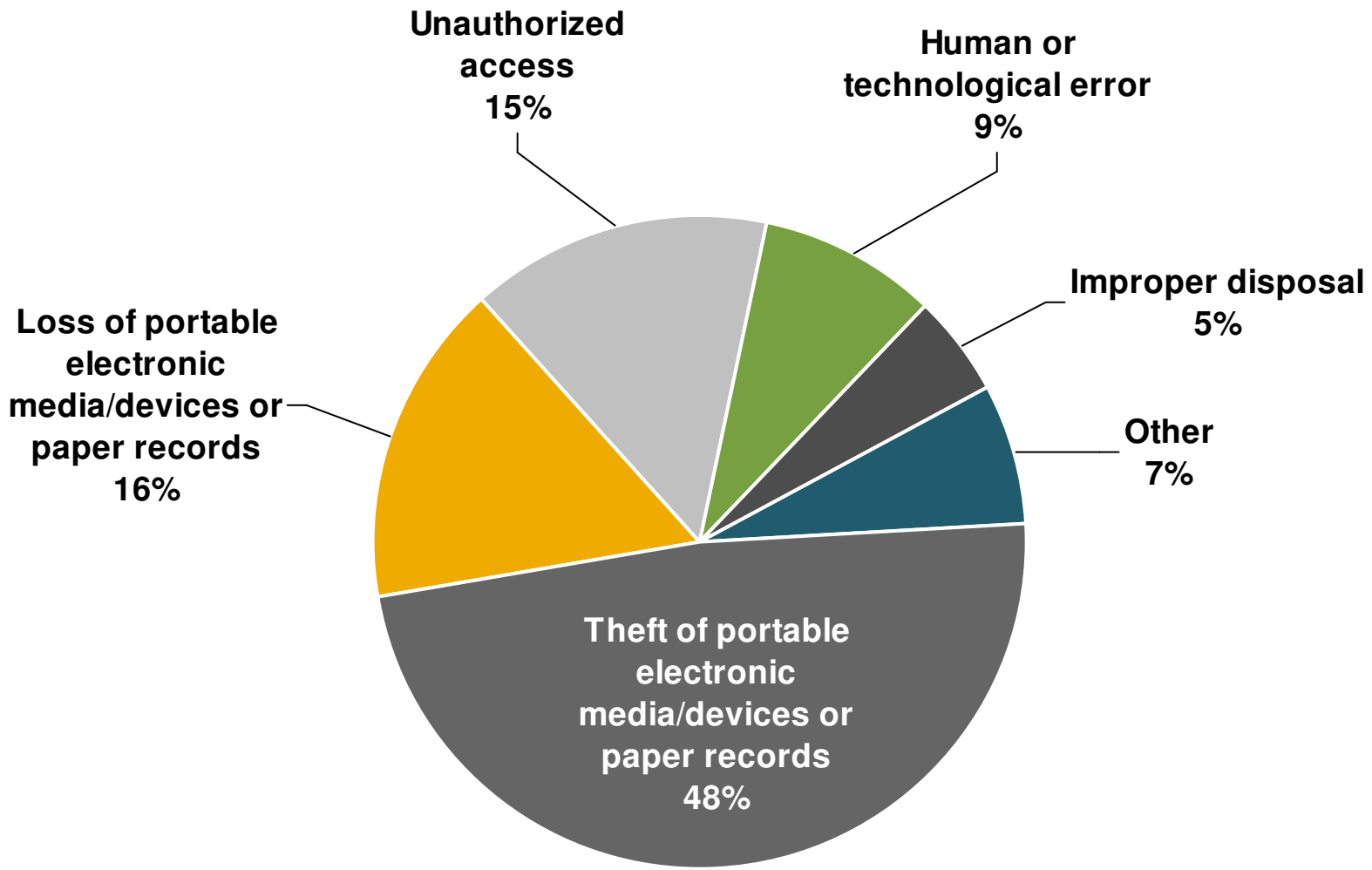
FCA Qui Tam Authority

- Private citizens with knowledge of fraud may serve as “relators”
- Relators may file suit under seal on behalf of the federal government
- The government may decide to intervene and take over prosecution of case
- Relators may receive 15 to 30 percent of recovery

Meaningful Use Payments Require Security Risk Analysis Provider Attestation

"Did you conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of its risk management process?"

Types of Breaches Triggering Notification



Source: OCR Report to Congress, 2011

Top Ten Risk Mitigation Steps

Mitigation Step	Why Is It Critical?
Perform risk analysis at least every two years	Key for MU compliance and foundational for security rule compliance
Encrypt PHI on portable media and devices	Huge portion of breaches fall into this category
Train all employees after hiring and on annual basis	Training supports “rogue employee” defense when violations occur
Minimize number of files/documents containing social security numbers	SSN’s raise heightened risk of fraud, class actions, credit monitoring, etc.
Develop business associate monitoring program	Reputational and other risks more important than absence of HIPAA liability

Top Ten Risk Mitigation Steps

Mitigation Step	Why Is It Critical?
Restrict removal of paper documents from facilities	Many breaches involve paper records lost in cars, trains, etc.
Employ special safeguards for PHI of employees and VIP's	Large percentage of snooping involves these individuals' records
Conduct regular audits of record access	Knowledge that audits conducted is deterrent
Regularly remind employees about dangers of social media	Growing number of privacy violations relating to Facebook, etc.
Discipline employees when appropriate	Sends message to entire organization that violations taken seriously

Thank You

Robert Belfort

Partner, Healthcare
Manatt, Phelps & Phillips, LLP

212.830.7270
rbelfort@manatt.com

Robert Belfort is a partner in the healthcare practice of Manatt, Phelps & Phillips, LLP, and has almost 20 years of experience representing healthcare organizations on regulatory compliance and transactional matters. Mr. Belfort has extensive experience advising a wide variety of healthcare clients, including hospitals, community health centers, medical groups, mental health providers, pharmacy chains, health insurers, managed care organizations, information technology vendors and healthcare industry trade associations.

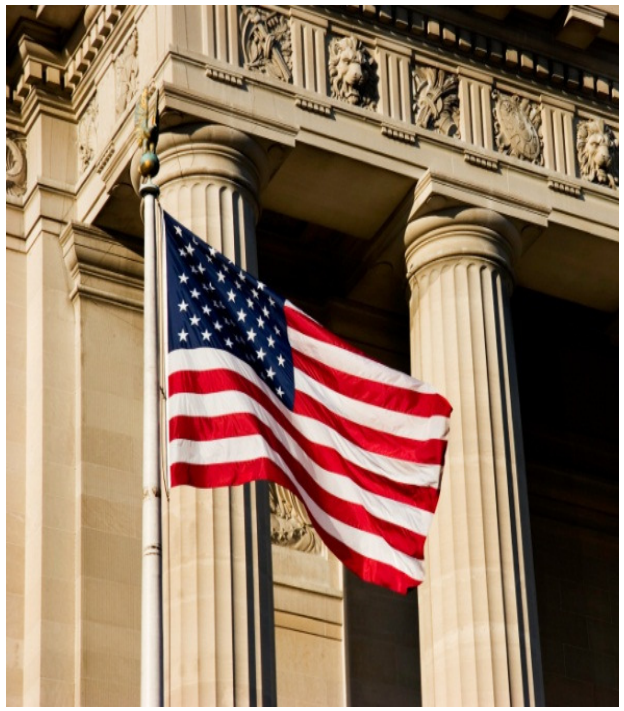
Deloitte.

manatt

Hot Topics in Security & Privacy

Program Highlights and Enforcement Trends

June 11, 2013



John Valenta, Director
Karolyn Woo, Senior Manager

Deloitte & Touche LLP

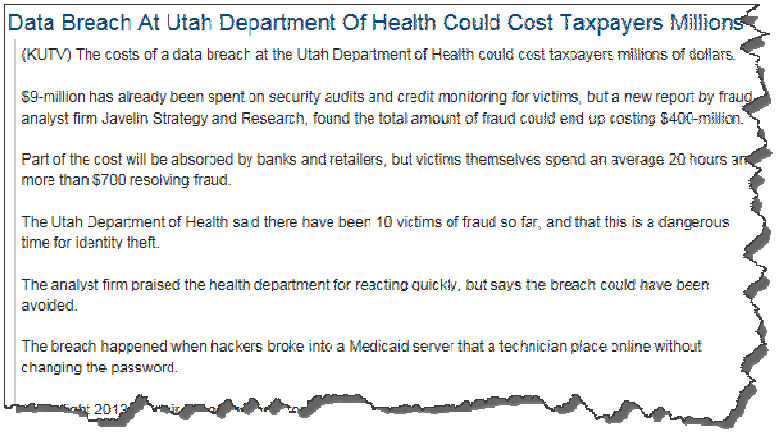
Agenda

- Compliance & security risks and challenges
- OCR audit protocol & enforcement trends
- Omnibus final rule

Compliance and Security Risks and Challenges

Organizations are challenged to address their compliance and security requirements while balancing business needs and the economic climate

Complex Compliance Landscape, Increased Scrutiny



Data Breach At Utah Department Of Health Could Cost Taxpayers Millions

(KUTV) The costs of a data breach at the Utah Department of Health could cost taxpayers millions of dollars.

$9-million has already been spent on security audits and credit monitoring for victims, but a new report by fraud analyst firm Javelin Strategy and Research, found the total amount of fraud could end up costing $400-million.

Part of the cost will be absorbed by banks and retailers, but victims themselves spend an average 20 hours and more than $700 resolving fraud.

The Utah Department of Health said there have been 10 victims of fraud so far, and that this is a dangerous time for identity theft.

The analyst firm praised the health department for reacting quickly, but says the breach could have been avoided.

The breach happened when hackers broke into a Medicaid server that a technician place online without changing the password.

Increasing Risks and Severity of Impact

Compliance obligations	An ever increasing amount of compliance requirements for organizations
Business requirements	There is immense competition for customers and pressure to continually grow the business
Economic climate	New laws and regulations have forced organizations to rethink their spending (e.g., HITECH, SOX, etc.)

Source: http://www.healthcareitnews.com/news/10-largest-data-breaches-2012-so-far

Emerging key health care security risk areas

Bio-Medical Devices	• Most newer bio-medical devices are networked, and some are connected wirelessly • Proof-of-concept hacks are in the wild • Rapidly becoming ingress points into EHRs
Mobile Devices	• Sharp increase in growth of mobile access to ePHI • Mobile devices are becoming gateway for patients to access ePHI • Mobile malware and hacking on the rise, increasing the risks to mobile access to ePHI
Third Parties	• Increased reliance on third parties to create, process, store and transmit ePHI • Enhanced breach notification laws for third parties in the HITECH Act • Business Associate Agreement compliance is often not monitored
End Users	• Many breaches are because of user error or neglect • User security training and awareness are sometimes not a focus for security programs • People will continue to be the weakest link in the security chain
Security Breaches	• Newer regulations require notification for even smaller breaches • DHS maintains a website tracking security breaches • 46 states now have breach notification laws in place

mHealth Spotlight

The health care and life sciences industry is recognized as one of the top three fields likely to propel mobile device growth in the next five years. By 2016 there will be a projected 10 billion mobile devices in use worldwide.

Mobile Devices	Mobile device sales in the U.S. are expected to grow from **172 million** in 2009 to **215 million** in 2016	↑ **25%**
Mobile Data Usage	Revenue from mobile data usage is expected to surge from **$35 billion** in 2008 to **$180 billion** in 2016	↑ **514%**
Global Mobile Traffic	Global mobile traffic has doubled for the fourth year in a row	↑ **100%**
Search Queries	Search queries have grown five times in the last two years	↑ **400%**

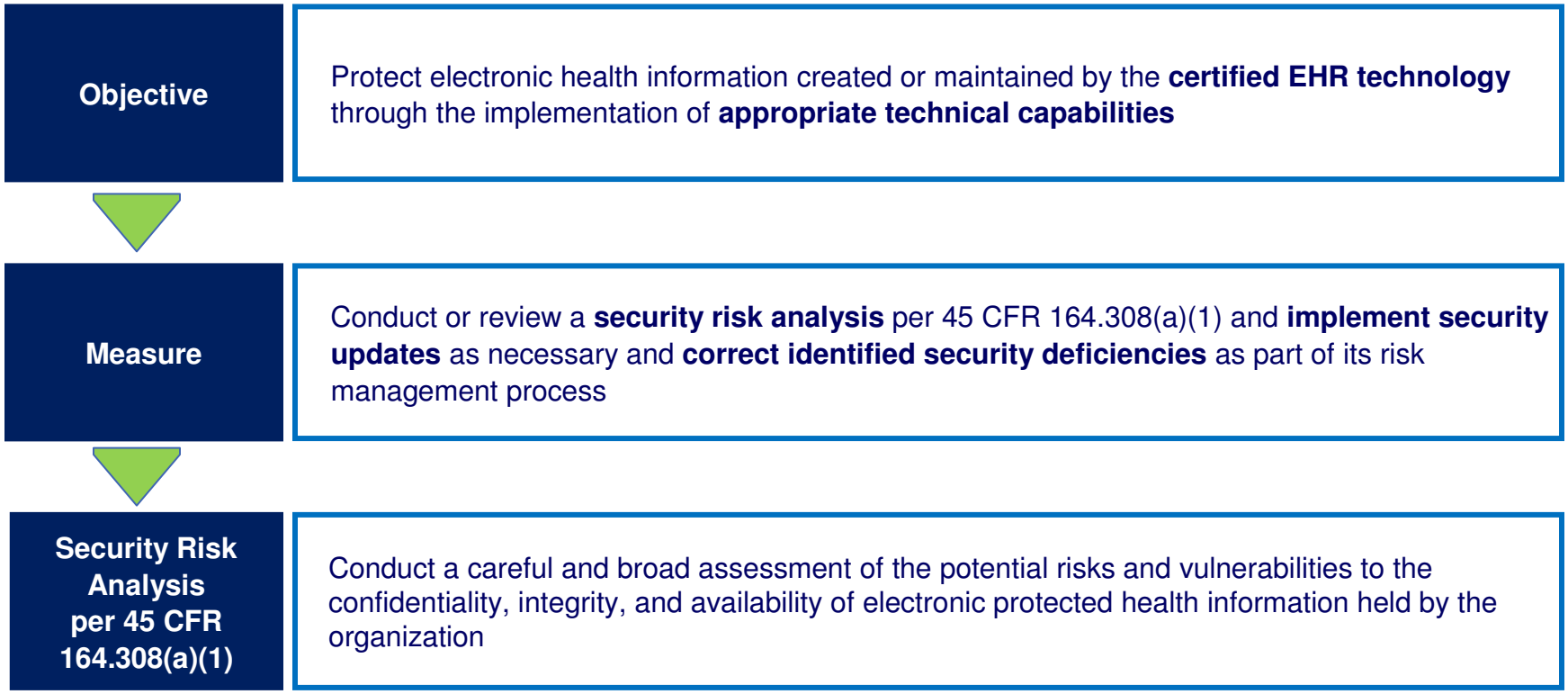
An integrated mobile risk mitigation strategy should be a key component of any compliance and risk strategies for the public sector, providers, health plans and biopharma and med-device companies.

Source: Deloitte Center for Health Solutions, "mHealth in an mWorld: How mobile technology is transforming health care", 2012, www.deloitte.com/centerforhealthsolutions

Meaningful Use (MU) Background

Sections of the HITECH Act provide grant and payment incentives for certain health care entities to adopt and make meaningful use of technology. Along with the grants and payment incentives, the legislation includes provisions intended to shore up public confidence in the use of EHRs and personal health records (PHRs) by enhancing the enforcement of and expanding the scope of activities covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

With respect to security and privacy, the following criteria must be met by covered entities to be considered eligible for Stage 1 Meaningful Use incentives:



Source: http://www.healthcareitnews.com/news/10-largest-data-breaches-2012-so-far

Meaningful Use: What's new for Stage 2?

While the total number of measures has decreased, the complexity and considerations associated with Stage 2 are significantly higher. The top challenges the industry is facing as they prepare are:

Vendor Dependency	Only a handful of EHRs are currently "Stage 2 Certified," and most organizations are waiting to see what the technology will look like before making decisions on how to prepare
Patient Engagement	Some measures require action from the patient in order to meet the associated objectives
Increased Information Exchange	Providers are required to exchange patient information electronically for 10% of transitions of care
3-Month Reporting Period	Due to the need to upgrade to the 2014 version of Certified EHR Technology, Eligible Professionals and Eligible Hospitals can attest to any 3-month quarter in calendar or federal fiscal year 2014, respectively
Stage 1 Changes	The Stage 2 Final Rule also includes changes to select Stage 1 measures

Source: http://www.healthcareitnews.com/news/10-largest-data-breaches-2012-so-far

Office for Civil Rights (OCR) Audit Protocol

The OCR has established a comprehensive audit protocol that contains the requirements to be assessed through the HIPAA Audit Program. In total, **169 modules** have been developed as part of the entire audit protocol.

81 Privacy Modules	78 Security Modules	10 Breach Notification Modules
The audit protocol covers Privacy Rule requirements for: (1) notice of privacy practices for PHI (2) rights to request privacy protection (3) access of individuals to PHI (4) administrative requirements (5) uses and disclosures of PHI (6) amendment of PHI (7) accounting of disclosures	The protocol covers Security Rule requirements for administrative, physical, and technical safeguards.	The protocol covers requirements for the Breach Notification Rule.
Common Findings: •**PHI Disclosures:** impermissible uses and disclosures of PHI •**Access to PHI: f**ailure to provide appropriate patient access to records •**Minimum Necessary:** lack of policies and procedures in place to limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of disclosure	**Common Findings:** •**Risk Assessment:** an accurate and thorough risk assessment was not conducted •**Security Incidents Response and Reporting:** policies and/or procedures not in place for identifying, responding to, reporting, and mitigating security incidents. •**Access Controls:** ineffective security measures relating to access controls	**Common Findings:** •**Risk Assessment:** lack of a risk assessment process to determine significant harm in a breach •**Notification to Individuals:** lack of process for notifying individuals within the required time period •**Burden of Proof:** insufficient process to determine threshold for breach notification

Source: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

Office for Civil Rights Enforcement

Enforcement highlights (as of April 30, 2013)

Complaints filed	80,836
Cases resolved	73,676
Cases with corrective action	19,726

Issues most frequently reviewed

Privacy Rule

- Impermissible uses & disclosures of PHI
- Safeguards to protect health information
- Access to health records
- Minimum necessary
- Notice of privacy practices

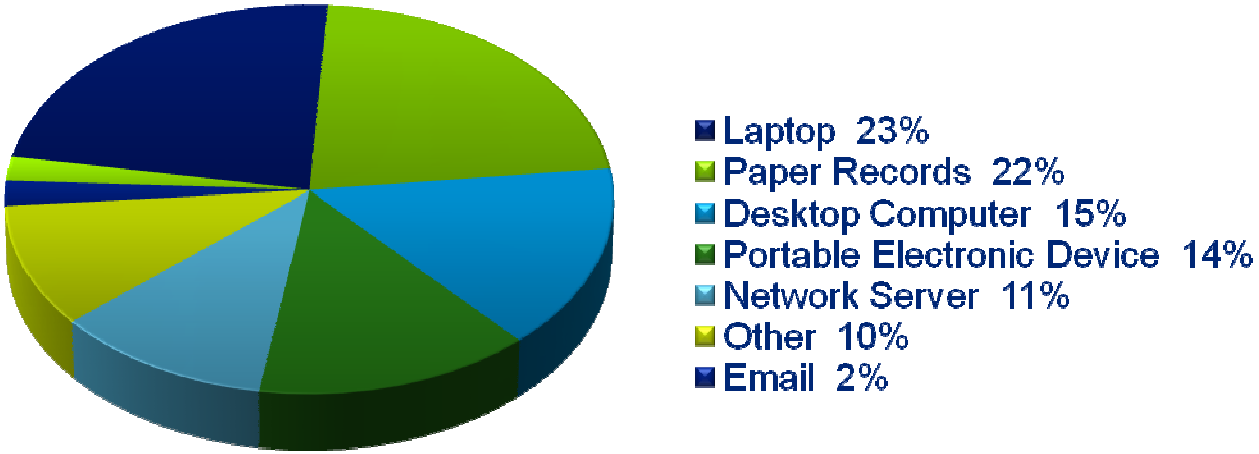
Security Rule

- Risk analysis
- Security incident response & reporting
- Security awareness & training
- Access controls
- Encryption & decryption (data storage)

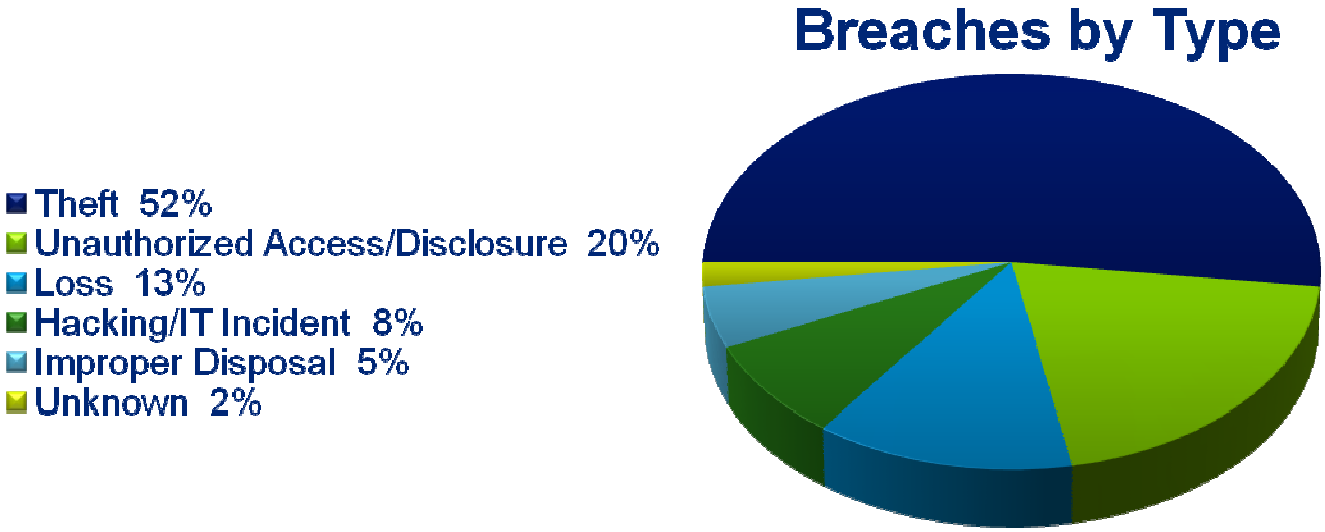
Source: The Department of Health and Human Services, Office for Civil Rights
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html

Office for Civil Rights (OCR) Enforcement

Breaches by Location



Breaches by Type



Source: The Department of Health and Human Services, Office for Civil Rights
"OCR Reports on the Enforcement of the HIPAA Rules", HCCA 2013 Compliance Institute

Omnibus Final Rule

HIPAA and HITECH

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) announced a Final Rule (the "omnibus final rule") finalizing modifications to HIPAA. The omnibus final rule makes modifications to the Privacy Rule, the Security Rule, and implements many provisions of the HITECH Act. It represents the first major set of updates to HIPAA since its enactment 15 years ago. The omnibus final rule is an outcome of Executive Order 13563 (2011), which resulted in the HHS facilitation of a retrospective review of existing regulations for the purpose of identifying ways to reduce costs and increase flexibilities of current regulations.

Key Questions

- What should a Security Officer or Privacy Officer do as part of these changes?
- Have scope and procedures for a Risk Assessment been performed?
- Have HIPAA policies and procedures, BAA and HIPAA authorization forms been updated?
- Have breach notification policies, procedures and training been updated?

Omnibus Final Rule

What's new in the Omnibus Final Rule?

- Business Associates (BA) of Covered Entities (CE) are both directly liable for compliance with technical, physical, and administrative safeguard requirements under the HIPAA Security Rule
- Strengthens limitations on the use and disclosure of protected health information (PHI) for marketing and fundraising purposes
- Prohibits the sale of PHI without individual authorization
- Expands individuals' rights to receive electronic copies of their health information
- Replaces "harm to individual" with more objective measure of compromise to the data as threshold for breach notification
- Adopts increased CMP amounts and tiered levels of culpability from 2009 Interim Final Rule

Important Dates

January 17, 2013	Public Display at *Federal Register*
January 25, 2013	Published in *Federal Register*
March 26, 2013	Effective Date
September 23, 2013	Compliance Date
September 22, 2014	Conform Business Associate Contracts

Source: The Department of Health and Human Services, Office for Civil Rights
"OCR Reports on the Enforcement of the HIPAA Rules", HCCA 2013 Compliance Institute

Contact Information and Speaker Biographies

Contact Information and Bios

John Valenta, Director jvalenta@deloitte.com **+1 714 436 7296**
Deloitte & Touche LLP

John has over 24 years of experience in the healthcare and life sciences industries and advises clients on regulatory and compliance issues as well as financial, risk management, and other operational issues. He has extensive consulting experience on issues related to compliance, government regulations, government program reimbursement, enterprise risk management, internal controls and other financial and operational issues. John has assisted organizations with performing risk assessments, compliance program effectiveness assessments, developing policies and procedures, providing education and evaluating the organizational structure of the compliance and internal audit functions. He has led numerous compliance reviews of areas including physician contracting/compensation, RAC Audit preparedness, coding for short stays and various HIPAA Privacy issues.

Karolyn Woo-Miles, Senior Manager kwoo@deloitte.com **+1 714 436 7886**
Deloitte & Touche LLP

Karolyn has over 13 years of experience working with healthcare clients in California, Arizona and New Mexico on a number of compliance and operations related engagements. She has extensive audit and compliance experience working with large hospital systems, individual community hospitals, payors and physician groups. Her consulting career has been specialized in compliance auditing and monitoring activities, conducting gap assessments, and process re-design and improvement. Her advisory services are focused on regulatory compliance matters such as Medicare billing compliance, physician arrangements, compliance program requirements, financial and compliance acquisition due diligence.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.