

INNOVATION. IMPACT. OUTCOMES.

ONWARD

Identity Fraud and Data Breaches: Criminal and Civil Enforcement Efforts

Feb. 24, 2014

James Robnett
Special Agent in Charge for the
Tampa Field Office
IRS – Criminal Investigations

Tatiana Melnik
Attorney
Melnik Legal PLLC

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS. www.himss-conference.org


Conflict of Interest Disclosure

James Robnett

Has no real or apparent conflicts of interest to report.


Tatiana Melnik, J.D.

Has no real or apparent conflicts of interest to report.

 © 2014 HIMSS

Learning Objectives

- Identify corporate risk factors for identity theft
- Discuss a typical identity theft criminal investigation
- Discuss data breach civil enforcement efforts
- Describe best practices to minimize identity theft and data breach risks




An Introduction to the Benefits Realized for the Value of Health IT

S T E P S


S Increased satisfaction from workforce members due to increased training.

S Long-term savings from on-going compliance efforts, leading to a reduction in data breach incidents. Growth of goodwill among staff and community.

 <http://www.himss.org/ValueSuite>

Outline

- I. Why is the IRS at HIMSS?
- II. Identity Theft and Healthcare
 - Why Identity Theft?
 - What is Identity Theft?
 - How Do Identity Theft/Tax Fraud Schemes Work?
 - Why Does Identity Theft Matter in Healthcare?
- III. An Update on Civil Enforcement
 - Private Plaintiffs
 - Office of Civil Rights
 - States' Attorney General
 - Federal Trade Commission
- IV. Best Practices



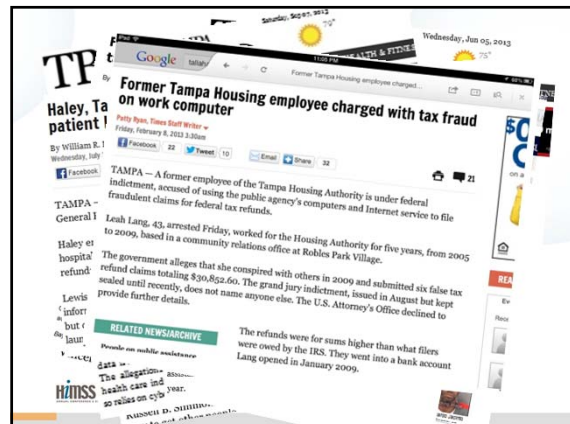
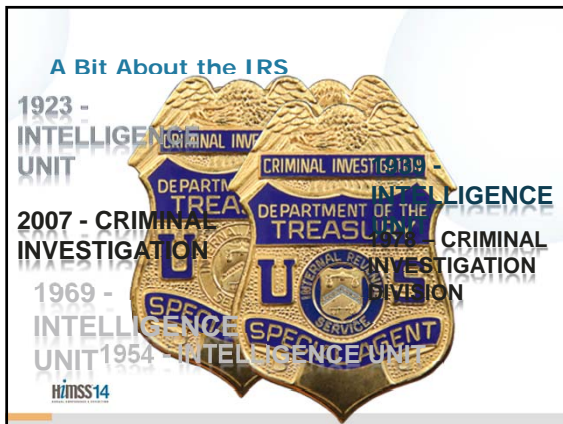
A Bit About the IRS



IRS

Department of the Treasury
Internal Revenue Service





Why is the IRS at HIMSS?

December 18, 2013
HUFF POST TECH

Identity Theft: ID Theft Is Here Today, Here to Stay

Posted: 10/22/2013 3:45 pm

THE TIME 113 people like this. Sign Up to see what your friends like.

The time to have persistent monitoring of your personal identity assets has arrived. We now must monitor our fiscal engagements (credit card, bank accounts, loans, etc.) for ourselves and parents, for your children as well. Monitor, our health insurance for medical identity theft (think of going into the hospital and their records have you as O- and you are AB+ due to someone having stolen your healthcare identity?) and even our Social Security records.

ACQUAINTANCE OR WARNING:
The time to have persistent monitoring of your personal identity assets has arrived. We now must monitor our fiscal engagements (credit card, bank accounts, loans, etc.) for ourselves and parents, for your children as well. Monitor, our health insurance for medical identity theft (think of going into the hospital and their records have you as O- and you are AB+ due to someone having stolen your healthcare identity?) and even our Social Security records.

HIMSS14

Why is the IRS at HIMSS?

Stealing from the government: SIRF's up | The Economist

Facebook page, above) who, along with her eager associates, claimed bogus rebates of more than \$11m.

A degree in computer science is not needed to steal personal data. Names, addresses and Social Security numbers can be nicked from doctor's surgeries, nursing homes and hospitals, either by insiders (a medical assistant was indicted in June for allegedly selling hundreds of names to feed his crack habit) or outsiders (who may distract secretaries an grab patient logs). Swindlers commonly prise information from the unsuspecting over the phone by posing as, say, Medicare reps. Some use the identities of dead people after trawling genealogical or family-support web sites. The Affordable Care Act is a gift: complaints about phone calls and visits from bogus Obamacare "navigators" are on the rise.

HIMSS14

Why is the IRS at HIMSS?

THE TRIFECTA

HIMSS14

Why is the IRS at HIMSS?

- Disclosure Pilot Program
 - The IRS has implemented a Disclosure Process with Local Law Enforcement Officers (LEO), now is available to all states.
 - Process assists local LEOs who are investigating identity theft schemes, related to false tax returns, within their jurisdictions
 - A process and forms were developed for ID theft victims to allow LEOs to retrieve tax return information from the IRS on their behalf (*Forms 14039 ID Theft Affidavit & 8821A IRS Disclosure Auth for Victims of ID Theft*).

HIMSS14

Why is the IRS at HIMSS?

- Formation of a Collaborative Working Group - The Tampa Bay ID Theft "Alliance"

The Charge

The "Alliance" is charged with the protection of both its citizens and government treasuries. With more than 15 participating law enforcement agencies and a single mission, agency names are dropped in favor of the Alliance banner.

HIMSS14

Why is the IRS at HIMSS?

The Alliance Mission

The primary purpose of The Alliance is to coordinate police efforts to prosecute individuals that target citizens for criminal financial gain, through the theft of personal identifying information (PII).

HIMSS14

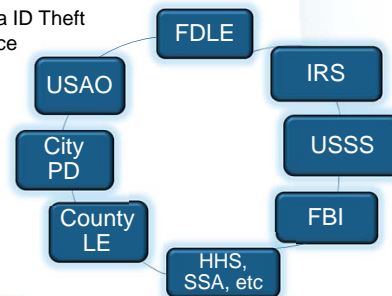
Why is the IRS at HIMSS?



HIMSS14

Why is the IRS at HIMSS?

Tampa ID Theft Alliance



HIMSS14

Why is the IRS at HIMSS?



HIMSS14

Outline

- I. Why is the IRS at HIMSS?
- II. **Identity Theft and Healthcare**
 - Why Identity Theft?
 - What is Identity Theft?
 - How Do Identity Theft/Tax Fraud Schemes Work?
 - Why Does Identity Theft Matter in Healthcare?
- III. An Update on Civil Enforcement
 - Private Plaintiffs
 - Office of Civil Rights
 - States' Attorney General
 - Federal Trade Commission
- IV. Best Practices

HIMSS14

Why Identity Theft?

THE TAMPA TRIBUNE, TBOCOM NEWS CHANNEL 8: INFORMING 2.1 MILLION ADULTS EVERY WEEK

THE TAMPA TRIBUNE
August 3, 2011

Nationwide, IRS issued more than \$5 billion in potentially fraudulent refunds last year

Tampa is No. 1 in tax fraud

Nationwide, IRS issued more than \$5 billion in potentially fraudulent refunds last year, according to a new report by a federal watchdog agency.

The study by the Internal Revenue Service's Inspector General, released last April, found that in 2010, the IRS issued more than \$5 billion in potentially fraudulent refunds last year, and that Tampa was the city with the highest number of fraudulent refunds.

The report identified the five cities with the highest number of fraudulent refunds last year, and by Tampa, with more than 100,000 fraudulent refunds, was the city with the highest number of fraudulent refunds.

The report also found that the IRS issued more than \$5 billion in potentially fraudulent refunds last year, and that Tampa was the city with the highest number of fraudulent refunds.

Tampa's Tax Fraud

Category	Amount
Refunds	\$1.5B
Income Tax	\$1.2B
Charitable Deductions	\$1.0B
State Tax	\$0.8B
Other	\$0.5B

What is Identity Theft?

- **Identity Theft and Identity Fraud**
 - Terms used to refer to all types of crime in which someone
 - wrongfully obtains and uses
 - another person's personal data
 - in some way that involves
 - fraud or deception
 - typically for economic gain
- **Identity Theft Used to Achieve Many Types of Fraud**
 - Credit card fraud
 - Healthcare fraud
 - Mortgage fraud
 - Tax fraud

HIMSS14

Why is ID Theft/Refund Fraud Possible?

- IRS is presently a customer service oriented U.S. government agency
- Filing System is designed around taxpayers who provide truthful & accurate information
- Mandate to quickly process tax returns and pay out tax refunds
- Presently, there is limited but not instant matching or authentication of information submitted to IRS

HIMSS14

Solutions to ID Theft and SIRF

- Match Info Docs to Tax Filings before issuing refunds.
- Delay Refund Issuances until after April 15th.
- Require Filer to know last 2 yrs AGI.
- Require Out of Wallet Questions before processing.
- Improve Filters and Technology.
- Use Finger Print technology.
- Roll tax refund over to the next filing period.
- Simplify Tax Code and minimize tax credits.

HIMSS14

Processing Challenges

- January 15th Thru April 15 (61 business days)
- Approx. 160 Million Tax Returns Submitted
- 2.6 Million Per Day
- Turn Around Processing in 2 days
- Error Correction
- Information Document Matching
- Use of Pre-Paid Cards

HIMSS14

How Do Identity Theft/Tax Fraud Schemes Work?

- **Criminals steal personal identifying information**
 - Name, date of birth, social security number
 - Hospitals, Universities, prisons, insurance companies, large apartment complexes, etc.
- **Create fraudulent email addresses for correspondence with IRS and banks**
- **Electronically file fraudulent tax returns**
 - False W-2 wages and withholdings
 - False interest income and withholding
 - False other income or Schedule C income targeted to the EIC
- **Refunds in the form of direct deposit, debit cards, and Treasury checks**

HIMSS14

How Do Identity Theft/Tax Fraud Schemes Work?

```

graph TD
    A[Person] -- "Transmits ID information to IRS" --> B[IRS]
    B -- "Mailed Checks" --> C[Mailbox]
    B -- "Mailed DEBIT Card" --> D[Mailbox]
    C --> E[Corrupt Check Casher]
    D --> E
    E --> F[Corrupt Business Owner]
    B -- "Wire Transfer" --> G[Bank]
    G -- "2nd Transfer" --> H[Bank]
    H --> I[Bank]
  
```

The diagram illustrates the flow of funds in a tax fraud scheme:

- Transmits ID information to IRS:** A person provides stolen identity information to the Internal Revenue Service (IRS).
- Mailed Checks:** The IRS mails checks to a mailbox.
- Mailed DEBIT Card:** The IRS mails a debit card to a mailbox.
- Corrupt Check Casher:** A person cashes the mailed checks.
- Corrupt Business Owner:** A person cashes the mailed debit card.
- Wire Transfer:** The IRS initiates a wire transfer to a bank.
- 2nd Transfer:** A second transfer is made from the bank to another bank.
- Bank:** The final destination for the funds.

How Do Identity Theft/Tax Fraud Schemes Work?

Perpetrator purchases or obtains stolen identities

Fraudulent tax returns are filed utilizing the stolen identities

Refunds are issued to locations perpetrator can obtain mail

Refunds are direct deposited into bank accounts or pre-purchased prepaid cards controlled by perpetrators

Corrupt Mail Carrier

Mail Theft from Boxes

Mail delivered to addresses controlled by perpetrators or associates

Funds are withdrawn from the bank accounts or transferred


```
graph TD; A[Perpetrator purchases or obtains stolen identities] --> B[Fraudulent tax returns are filed utilizing the stolen identities]; B --> C[Refunds are issued to locations perpetrator can obtain mail]; B --> D[Refunds are direct deposited into bank accounts or pre-purchased prepaid cards controlled by perpetrators]; C --> E[Corrupt Mail Carrier]; C --> F[Mail Theft from Boxes]; C --> G[Mail delivered to addresses controlled by perpetrators or associates]; D --> H[Funds are withdrawn from the bank accounts or transferred];
```

Making The Case for Successful Prosecution

- Communication between Alliance Agencies
- Sharing of Talent and Resources
- Analyzing Evidence, Serving Subpoenas, Contacting Witnesses
- Conducting Joint Undercover Operations
- Conducting Joint Enforcement Operations
- Evidence and Writing Prosecution Reports
- Testifying in the Grand Jury
- Indict, Arrest, Plea, Trial Sentence – Truth in Federal Sentencing

SIRF Evidence

- **Financial Institution Records**
 - Application or signature cards with supporting documents
 - Bank or Debit Card Statements
 - Details of specific transaction
 - ATM or branch video
- **Internet Service Provider (ISP) Records**
 - Need to ID and Preserve the Digital Trail
- **IRS Records**
 - U.S. Income Tax Returns
 - Transcripts of Account
 - Information Documents reported to IRS



The Refund Check

The easiest way to identify a tax refund check is the 12/XX on the check next to the dollar amount. This is the tax period indicator. Current year will be 12/13. The check also indicates tax refund under the check number.

H&MSS14

[illegible]

Evidence of ID Theft Occurring?

Notebook Entries



HIMSS14

Evidence of ID Theft Occurring?

High Volume Prepaid Card



HIMSS14

Evidence of ID Theft Seized by Law Enforcement

- Car Stops, Informants, Search Warrants
 - List of personal identifiers (Names, SSN, DOB's)
 - List of multiple bank accounts
 - Multiple paper returns (to include electronic transmissions)
 - Multiple paper U.S. Treasury Refund Checks
 - Multiple reloadable debit/prepaid cards
 - Multiple forms of ID's (driver's license, Birth Cert, SSN Cards)
 - Notes on how to prepare/transmit returns
 - IRS, SSA, Local Government Notices for multiple individuals, duplicate addresses related to tax returns and/or benefits



HIMSS14

Evidence of ID Theft Seized by Law Enforcement



HIMSS14

Evidence of ID Theft Seized by Law Enforcement

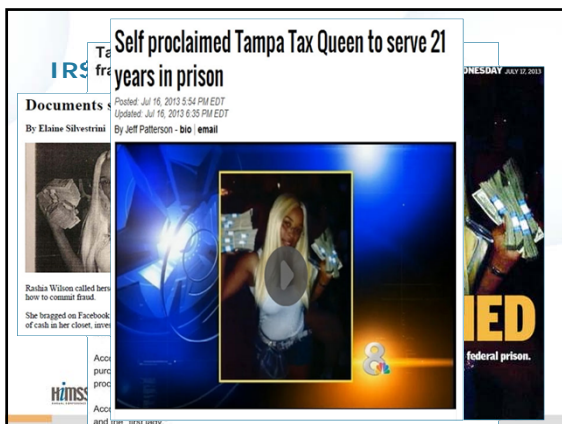
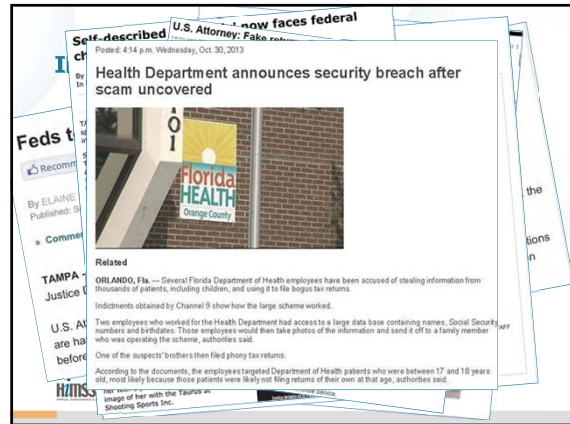


HIMSS14

Evidence of ID Theft Seized by Law Enforcement



HIMSS14





Outline

- I. Why is the IRS at HIMSS?
- II. Identity Theft and Healthcare
 - Why Identity Theft?
 - What is Identity Theft?
 - How Do Identity Theft/Tax Fraud Schemes Work?
 - Why Does Identity Theft Matter in Healthcare?
- III. An Update on Civil Enforcement
 - Private Plaintiffs
 - Office of Civil Rights
 - States' Attorney General
 - Federal Trade Commission
- IV. Best Practices

HIMSS14

Data Breach Statistics

Healthcare Data Breach Reports Submitted to the Office of Civil Rights for Breaches Impacting 500+ Individuals

Year	Number of Breaches Reported to OCR ^{1,2}	No. of Breaches Listing "Theft" of Laptop, Desktop, Server, or Portable Device	Number of Patients Impacted
2013	182	68 (37% to total breaches)	6,971,141
2012	212	93 (44%)	2,276,248
2011	179	72 (40%)	11,180,673
2010	221	100 (45%)	5,512,852

¹ Count based on breach date and not posted date as of Jan. 12, 2014. Count may change with new reports.
² Breach counted for each year occurred. For example, the Duke University Health System reported a breach that took place from 4/21/2004 - 2/16/2012. This breach is counted once for each of 2010, 2011, and 2012.

HIMSS14

Data Breach Statistics

Healthcare Data Breach Reports Submitted to the Office of Civil Rights for Breaches Impacting Fewer Than 500 Individuals

Year	Number of Breaches Reported to OCR	Number of Patients Impacted
2010	25,000+	50,000+
2009 (9/23/2009 – 12/31/2009)	5,521	approx. 12,000

- Majority of small breach reports in 2009 and 2010 involved misdirected communications and affected just one individual each:
 - clinical or claims record mistakenly mailed or faxed to wrong individual
 - test results sent to the wrong patient
 - files attached to the wrong patient record
 - emails sent to the wrong addresses
 - member ID cards mailed to the wrong individuals

Source: OCR Annual Report to Congress, Aug. 15, 2011

HIMSS14

Costs to Repair Data Breaches

Globally data breaches cost more per record

Cost of Repair:
 2011: \$194/record
 2012: \$188/record

Average per capita cost of data breach over two years
 Measured in US\$

HIMSS14 2013 Annual Study: Global Cost of a Data Breach - June 5, 2013 Symantec

Costs to Repair Data Breaches

Source: 2013 Annual Study: Global Cost of a Data Breach (Ponemon Institute, Sponsored by Symantec)

Average Notification Costs
 (measured in US \$)

Country	Cost
US	565,020
DE	353,927
UK	
AU	
FR	
IT	73

Average Ex-Post Response Cost
 (measured in US \$)

Country	Cost
US	1,412,548
DE	1,406,663

Average Lost Business Costs
 (measured in US \$)

Country	Cost
US	3,030,814
AU	1,957,966
DE	1,746,467
FR	1,569,953
UK	1,417,116
IT	790,899

Private Plaintiffs

- Most actions are class actions

- Difficult to win
 - Article III Standing
 - an injury-in-fact

Identity theft shows money damages....

How did me losing your information hurt you?
How much **money** did you lose?

HIMSS14

Private Plaintiffs

- AvMed Health Plan

- In 2009, **unencrypted** computers were broken into
- Class action filed in Florida
 - Theory: Some portion of the problem was caused by the company's failure to implement adequate security measures
 - Was dismissed in July 2011 and then reinstated by the 11th Circuit in Sept. 2012
- Settled in October 2013 for \$3M, and included:
 - mandatory security training for employees
 - mandatory training on appropriate use of company computers
 - updating company computers and security mechanisms, including GPS tracking of company vehicles
 - new password protocols and full disk encryption on all company computers
 - physical security upgrades
 - review and revision of written policies and procedures for information security

Why this Case Matters:

- Some class members suffered identity theft while others did not
- But, all class members can collect from the Settlement Fund - \$10 for every year they were customers (up to \$30)
- AvMed chose to settle rather than investigate harm done to other class members

HIMSS14

Private Plaintiffs

- UCLA

- In Sept. 2011, an **encrypted** external hard drive was stolen during a home invasion. The drive contained an index card by the drive and could have been used to access the drive's contents.
- Class action filed in California (O'Connell v. UCLA)
 - Grounded in California's Confidential Information Act, which permits plaintiffs to seek actual damages, nominal damages, or both
 - **Damages would have been \$50,000 per plaintiff**
- Cali. Appeal Court ruled for UCLA – "private right of action for negligent mismanagement of individual's medical information) **only if the mismanagement results in unauthorized or wrongful access to the information**"
- Plaintiff must show **more than** a loss of possession by Defendant

Why this Case Matters:

- Ruling was a huge relief to other California health systems currently being sued on similar grounds
- If class members can show a "breach," then case goes on → breach does not require money damages, just simply for someone to "look" at the PHI without authorization
- Recall this case was brought under State law

HIMSS14

Private Plaintiffs

- R.K. v. St. Mary's Medical Center (West Virginia)

- Patient was admitted to St. Mary's as a psychiatric patient in March 2010
 - Hospital's employees accessed his records and disclosed PHI to his estranged wife and her divorce lawyer
- RK sued asserting claims for (1) negligence, (2) outrageous conduct, (3) intentional infliction of emotional distress, (4) negligent infliction of emotional distress, (5) negligent entrustment, (6) breach of confidentiality, (7) invasion of privacy, and (8) punitive damages
- No HIPAA claim asserted
- St. Mary's filed a motion to dismiss arguing that claims were preempted by HIPAA
 - St. Mary's motion was granted and RK appealed

HIMSS14

Private Plaintiffs

- R.K. v. St. Mary's Medical Center (West Virginia)

- In reversing the lower court, the West Virginia Court of Appeal noted:

Finally, we note that, contrary to finding state common-law claims preempted by HIPAA, several courts have found that a HIPAA violation may be used either as the basis for a claim of negligence *per se*, or that HIPAA may be used to supply the standard of care for other tort claims.
- Citing decisions from Connecticut, Missouri, North Carolina, and Tennessee

Why this Case Matters:

- Consider your organization's current state of compliance. What would happen if the HIPAA Rules were used as the "standard of care" in the case of a breach?

HIMSS14

Office of Civil Rights

- Since April 2003 (the initial compliance date)

- Received over 89,045 HIPAA complaints
- Resolved complaints through -
 - investigation and enforcement (over 21,942)
 - investigation and finding no violation (9,869)
 - closure of cases that were not eligible for enforcement (51,910)
- Compliance issues investigated most:
 - impermissible uses and disclosures of PHI
 - lack of safeguards of PHI
 - lack of patient access to their PHI
 - uses or disclosures of more than the minimum necessary PHI
 - lack of administrative safeguards of ePHI

HIMSS14

Office of Civil Rights

OCR has taken action against:

Entity	Amount	Rules	Breach	Incident	Settlement
Cignet Health	\$4.3M	Privacy Rule, \$3M for willful neglect per HITECH	Denying patients access to medical records	Prior to 3/1/2009	2/4/2011 (this was <i>not</i> a settlement)
General Hospital Corp. & Physicians Org.	\$1M	Privacy Rule	Left documents on subway	3/9/2009	2/14/2011
UCLA Health System	\$865,500	Privacy & Security Rules	Workers snooping on celebrity patients	Prior to 6/5/2009	7/5/2011

HIMSS14

Office of Civil Rights

OCR has taken action against:

Entity	Amount	Rules	Breach	Incident	Settlement
Blue Cross Blue Shield of TN	\$1.5M	Privacy & Security Rules	unencrypted hard drives stolen from a leased facility	Prior to 11/3/2009 (self reported)	3/13/2012
Phoenix Cardiac Surgery	\$100K	Privacy & Security Rules	posting appt. on an online, publicly accessible calendar	Prior to 2/19/2009	4/11/2012
Alaska Dept. of Health & Human Services	\$1.7M	Privacy & Security Rules	unencrypted portable media device stolen from car of employee	10/12/09 (self reported)	6/25/2012

HIMSS14

Office of Civil Rights

OCR has taken action against:

Entity	Amount	Rules	Breach	Incident	Settlement
Massachusetts Eye and Ear Infirmary	\$1.5M	Privacy & Security Rules	theft of unencrypted personal laptop while at conference	Prior to 4/21/10 (self reported)	9/13/2012
Hospice of Northern Idaho	\$50K	Security Rule	theft of unencrypted laptop (less than 500 patients)	Prior to 2/16/11 (self reported)	12/17/2012
Idaho State University	\$400K	Security Rule	disabled server firewall for ~ 10 mo. resulting in a breach	Prior to 8/9/2011 (self reported)	5/10/2013

HIMSS14

Office of Civil Rights

OCR has taken action against:

Entity	Amount	Rules	Breach	Incident	Settlement
Shasta Regional Medical Center -	\$275K	Privacy Rule	senior leaders at co. met w/media to discuss medical services provided to a patient w/o a valid written authorization	1/4/2012 (read article in LA Times)	6/3/2013
WellPoint	\$1.7	Privacy & Security Rules	software update to web-based database left ePHI publicly accessible	Prior to 6/18/10 (self reported)	7/8/2013

HIMSS14

Office of Civil Rights

OCR has taken action against:

Entity	Amount	Rules	Breach	Incident	Settlement
Affinity Health Plan	\$1,215,780	Privacy and Security Rules	returned copiers to a leasing agent w/o erasing the copier hard drives	Prior to 4/15/10 (self reported)	8/7/2013
Adult & Pediatric Dermatology	\$150K	Privacy, Security & Breach Notification Rules	theft of unencrypted personal thumb drive from employee vehicle	Prior to 10/7/11 (self reported)	12/24/2013

HIMSS14

Office of Civil Rights

• A Few Identified Problems

- Failure to conduct a Risk Analysis in response to new environment
 - BCBSTN – Changed offices
 - WellPoint – Installed software upgrade
 - Alaska DHHS – Never conducted a risk analysis
- Workforce members
 - Failure to train and train on an on-going basis
 - Failure to “apply appropriate sanctions”
 - Failure to install security measures to monitor unauthorized access
 - UCLA case – workforce members repeatedly snooping on patients between 2005 – 08

HIMSS14

Office of Civil Rights

• A Few Identified Problems

- **Portable devices**
 - Lack of encryption/security measures
- Lack of policies and procedures to address
 - Incident identification, reporting, and response
 - Restricting access to authorized users
 - "To provide [CE] with a reasonable means of knowing whether or what type of portable devices were being used to access its network"

Settlement Agr. with Massachusetts Eye and Ear Infirmary



Office of Civil Rights

• OCR Corrective Action Plans

- Comprehensive Risk Analysis
- A written implementation report describing how entity will achieve compliance
- Revised policies and procedures
- Additional employee training
- Monitoring – Internal and 3rd Party
- Term is 1 – 3 years, with document retention period of 6 years



Office of Civil Rights



• HITECH includes a sort of whistleblower provision

- Not a true whistleblower provision because the statute does not authorize a lawsuit to recover payments
- Permits "an individual who is harmed by an act that constitutes an offense [in violation of HIPAA to] receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense"

• Waiting on regulations

- HITECH requires that the GAO recommend to the Secretary a methodology under which individuals harmed as a result of a HIPAA violation would receive a percentage of any CMP or monetary settlement collected with respect to the HIPAA violation
- HHS Secretary is required to issue regulations (w/in 3 years of ARRA enactment) implementing the recommended methodology



States' Attorney General

- HITECH granted State AG's power to enforce HIPAA
- OCR offers training and technical assistance on enforcement to AGs throughout the US
 - Want to know what they learned?
 - Videos available:
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/sagmoreinfo.html>
- AGs sue as *parens patriae* to recover on behalf of residents



States' Attorney General

• Actions Based on HIPAA



- Connecticut AG first to file
 - Sued HealthNet for a breach that spanned multiple states
 - Settled with HealthNet for \$250,000 + compliance



- Vermont AG also sued HealthNet
 - Entered into a consent decree, which required
 - payment of \$55,000
 - submit to a data-security audit
 - file reports with Vermont regarding information security programs for 2 years



States' Attorney General

• Actions Based on HIPAA



- Minnesota AG is the first to take action against a **business associate**, Accretive Health, Inc.
- Action filed in 2012, after an unencrypted laptop containing PHI was stolen out of an Accretive employee's car
 - Laptop contained sensitive (name, address, etc.) and highly sensitive information (mental health, STDs)
- Accretive settled with Minnesota AG
 - Accretive agreed to cease all operations in Minnesota within ... 90 days, or by November 1, 2012
 - Company is subject to an **outright ban on operating in Minnesota for 2 years**, after which, for the next 4 years, it can only reenter the State if the Attorney General agrees to a Consent Order regarding its business practices in the State



States' Attorney General

• Actions Based on State Law



- Indiana AG sued WellPoint under Indiana state law which requires notification "without unreasonable delay"
- WellPoint had a breach in its online application tracker website
 - impacted approx. 32,000 Indiana residents
 - social security numbers, financial information, health records
- Breach span: October 2009 to March 2010
 - WellPoint notified as early as Feb. 22, 2010 and again on March 8, 2010 that PHI publicly available online
 - Began notifying customers on June 18, 2010
 - Notified AG's office on July 30, 2010, after the AG's office reached out to WellPoint – BUT, state law requires notification to both consumers and AG

HIMSS14

States' Attorney General

• Actions Based on State Law



- Indiana sued WellPoint on Oct. 29, 2010 seeking \$300K in civil penalties
- Case settled in June 2011
 - \$100K to the AG's Consumer Assistance Fund
 - Agree to comply with Indiana's Disclosure of Security Breach Act
 - **Admit** that WellPoint had a security breach and failed to properly notify the AG as required by law
 - Up to 2 years of credit monitoring and identity-theft protection services to affected Indiana consumers
 - Reimburse any WellPoint consumer up to \$50K for any losses that result from identity theft due to the breach
- **Did it cost WellPoint more than the \$300K initially sought by the AG? (consider legal fees, employee time)**

HIMSS14

States' Attorney General

• Indiana has been active in enforcing Indiana's Disclosure of Security Breach Act



- Failure to comply with the notification requirement can result in a lawsuit by the AG and an order to pay civil penalties of up to \$150K
- As of July 5, 2011, the AG's Office
 - Issued warning letters to 47 companies that delayed in issuing notice of security breaches
 - Of the 47,
 - 39 issued to companies for delays in notifying both consumers and the AG's Office (**Q. How did AG find out?**)
 - 5 sent to companies for delays in notifying the AG's Office only
 - 3 sent to companies for delays in notifying consumers only

HIMSS14

Federal Trade Commission



- FTC "works for consumers to prevent fraudulent, deceptive, and unfair business practices"
- Has authority to pursue **any company** that has engaged in "**unfair or deceptive acts or practices**" in or affecting commerce"
- Has pursued companies across a number of industries
 - Hotels
 - Mobile apps
 - Rental services
 - Healthcare

HIMSS14

Federal Trade Commission



• Recent privacy related settlements

– Accretive Health

- Action based on the **same theft** of unencrypted laptop that triggered the Minnesota AG action
 - Theft happened in July 2011
 - Minnesota settled in July 2013
 - FTC settled (proposed) in December 2013

• FTC:

Until at least July 2011, Accretive failed to provide reasonable and appropriate security for consumers' personal information it collected and maintained **by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access.** Among other things, Accretive Health created unnecessary risks of unauthorized access or theft of PI by [a number of actions].

HIMSS14

Federal Trade Commission



• Recent privacy related settlements

– Goldenshores Technologies, LLC and company's founder **individually**

- FTC settled (proposed) in Dec. 5, 2013
- Mobile app development company - "Brightest Flashlight Free" app
- App transmitted geolocation with persistent device identifiers to third parties, including advertising networks
- Problems
 - Privacy Policy failed to tell users that geolocation and persistent device identifiers transmitted
 - Consumers do not have a "true" opportunity to decline terms – app installs and starts transmitting before EULA appears

HIMSS14

Federal Trade Commission



- What does the FTC require for remediation?
 - Consent order calls for a **20 year compliance period**, generally with 3rd party audits every 2 years
 - In Goldenshores, **the owner** is required:
 - “for a period of ten (10) years after the date of issuance of this order, shall notify the Commission of the discontinuance of his current business or employment, or of his affiliation with any new business or employment”
 - In Accretive Health, the FTC order mirrored some of the HIPAA requirements (e.g., undertaking a risk assessment, taking remediation steps, etc.)
 - But, also required that Accretive “development and use of reasonable steps to *select and retain service providers capable of appropriately safeguarding personal information* they receive from” Accretive

HIMSS14

Outline

- I. Why is the IRS at HIMSS?
- II. Identity Theft and Healthcare
 - Why Identity Theft?
 - What is Identity Theft?
 - How Do Identity Theft/Tax Fraud Schemes Work?
 - Why Does Identity Theft Matter in Healthcare?
- III. An Update on Civil Enforcement
 - Private Plaintiffs
 - Office of Civil Rights
 - States' Attorney General
 - Federal Trade Commission

IV. Best Practices

HIMSS14

Best Practices to Protecting Clients' Personal Data

Five Principles To Safe Guard Personal Information

- 1 Take Stock
- 2 Scale Down
- 3 Lock It
- 4 Pitch It
- 5 Plan Ahead

HIMSS14

Take Stock

- KNOW WHAT PERSONAL INFORMATION YOU HAVE IN YOUR FILES.



HIMSS14

Scale Down

- Keep only what you need for your business
- Develop a written records retention policy
- Truncate the account information on electronically printed credit and debit card receipts



HIMSS14

Lock It

- PROTECT THE INFORMATION THAT YOU KEEP.

- Employee/Contract Security
- Physical Security
- Electronic Security
- Employee Training



HIMSS14

Pitch It

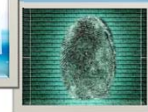
- ❑ Properly dispose of what you no longer need
- ❑ Use wipe utility programs on old computers
- ❑ Home employees must follow same procedure.



HIMSS14

Plan Ahead

- ❑ Create a plan to respond to security incidents
- ❑ Investigate security incidents immediately
- ❑ Take steps to close off existing threats to personal information



HIMSS14

Report Identity Theft

- Report Stolen Identities to
 - Local Law Enforcement
 - IRS – Criminal Investigations

HIMSS14

Victim/Witness Assistance

- ID Theft Victim/Witness Assistance
 - Refer victim to the following websites.
 - www.irs.gov, www.ssa.gov,
 - www.ic3.gov Internet Crime Complaint Center,
 - FTC www.idtheft.gov or 1-877-IDTHEFT (1-877-438-4338).
 - Recommend the victim file a police report.
 - Recommend the victim notify the 3 major credit bureaus.
- Victim should contact the ID Theft Protection Specialized Unit (IPSU) at (800) 908-4490
 - IRS will place an ID Tracking indicator on the account
 - By mail:
 - Internal Revenue Service
 - P.O. Box 9039
 - Andover, MA 01810-0939

HIMSS14

Best Practices for Compliance

- Default position under the HIPAA Final Rule is that there was a "breach"
 - Go through the analysis carefully and document
 - But, don't forget to review state law requirements as well
 - Are all of the impacted individuals residents of the same state?
- When was the last time your organization conducted a Risk Analysis?
 - Has the company opened a new office?
 - Upgraded software?
- Are the laptops and other portable devices encrypted?
 - Why not? Should desktops be encrypted?
- Is a BYOD policy in place?
 - Does it align with existing policies (e.g., Remote Access Policy, Acceptable Use Policy, Litigation Hold Policy, etc.)
 - Patients texting doctors? Is texting a 'secure' form of communication? Is an authorization in place?

HIMSS14

Best Practices for Compliance

- Choose vendors carefully
 - Business Associate/Subcontractor Agreements should be tailored to the situation
 - "Standard" agreement may give too much leeway to BA/Sub
 - Does the breach notification provision provide enough time for compliance? Require cooperation?
 - Is each party bearing a "fair" amount of risk?
- Breaches happen to every organization... Buy insurance
 - Policy and coverage should be reviewed carefully
 - Some policies exclude coverage for incidents that are against your organization's "Privacy Policy"
 - How much coverage do you need? Recall that in 2012, cost of remediation was \$188/record (188 * 500 patients = \$94K)

HIMSS14

On the Lookout for 2014

- Office of Civil Rights will continue to take enforcement actions
 - Will likely be targeting business associates
- "Big Data" is coming to healthcare
 - Many opportunities (reduce readmissions, population health management, clinical research, improved point of care decisions)
 - Privacy and security concerns? Yes, BUT, can be addressed with advanced planning, on-going compliance efforts and contracts
 - Choose partners wisely...

"The general counsel for the company that maintains the health insurance quote website, when contacted by [the Senate] Committee majority staff, said the company had no information sharing agreement with Axiom, and that the entities that contract to receive the website's information are contractually prohibited from sharing that data with third parties such as Axiom. Axiom represented that this website data source was provided by one of Axiom's data aggregators."

Source: A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Senate Committee on Commerce, Science, and Transportation, Dec. 18, 2013



An Introduction to the Benefits Realized for the Value of Health IT



Increased satisfaction from workforce members due to increased training.



Long-term savings from on-going compliance efforts, leading to a reduction in data breach incidents. Growth of goodwill among staff and community.



<http://www.himss.org/ValueSuite>

Questions?

Thank You!

James (Jim) Robnett
James.Robnett@ci.irs.gov
727-568-2552

Tatiana Melnik
tatiana@melniklegal.com
734-358-4201

