



## **Breach Notification Compliance: The Feds are Watching.**

HCCA Managed Care Compliance Conference  
February 8, 2011



## **Today's Discussion**

- “Got Electronic?”
- What government is doing to ensure we're protecting data
- Why they're doing it
- How to prepare yourself for the New World

## Current Demands:

- For
    - Patient centered care
    - Outcome-focused care
    - Privacy & Security
    - Quality, safety, efficiency
    - Cost-effective care
    - Prospective v. Retrospective disease management
    - Transparency
  - From
    - Consumers
    - Regulatory forces
      - Federal
      - State
      - other
    - Market forces
- Patient Safety



## How Do We Address These?

- Health information technology
  - Electronic health records (EHRs)
  - Health information exchanges (HIEs)
  - Clinical decision support (CDS)
  - Computer physician order entry (CPOE)
  - Etc.



## For the “Doubters” ...

- *“There is no reason anyone would want a computer in their home.”*



- Ken Olson, founder and chairman of Digital Equipment Corp., 1977.

“Everything that can be invented has been invented.”

- Charles Duell, Commissioner of the US Office of Patents, 1899

- *“This ‘telephone’ has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us.”*

- According to an 1876 internal Western Union memo.



## Living in an Electronic Age



Our data is RICH and VALUABLE

- Increased availability of electronic data = increased access to it from afar
- More Americans worry about being a victim of identity theft than they do being a victim of terrorism
- Medical identity theft is the fastest growing category of identity theft in U.S.\*

## How Health Plans Stack Up

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>● Breaches over 500* involving <u>health plans</u></li> </ul> <p>Average # of records breached = 51,979</p> <p>Median = 2739</p> <p>Standard deviation = 208,311</p> | <ul style="list-style-type: none"> <li>● Breaches over 500* involving all <u>other covered entities</u></li> </ul> <p>Average # of records breached = 22,819</p> <p>Median = 2284</p> <p>Standard deviation = 709</p> |
|---|---|

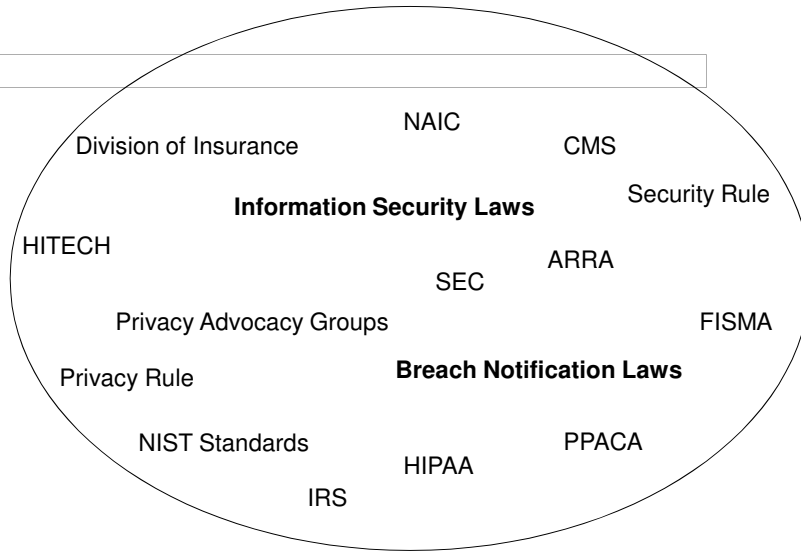
\*Reported to OCR since 9/23/09

## Largest Reported Breaches involving Health Plans

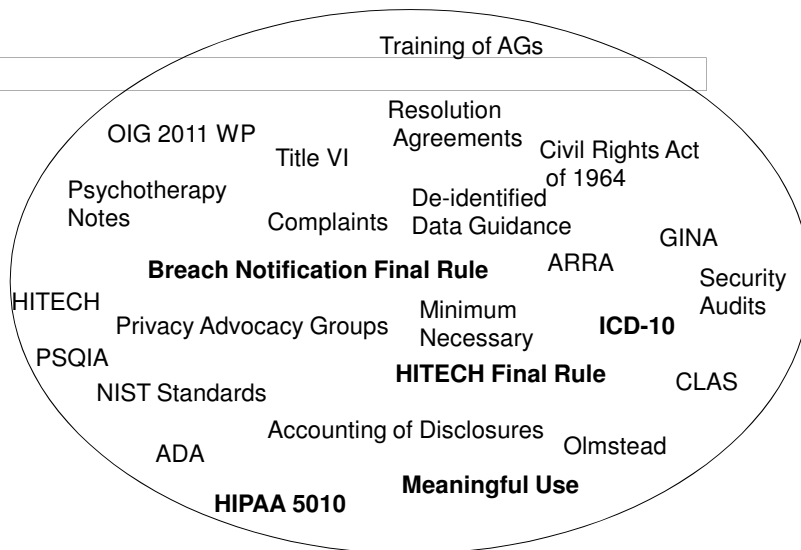
The screenshot shows a table with columns for 'Entity Name', 'Type of Breach', 'Number of Records Breached', and 'Date of Breach'. The data includes entries for AvMed, Inc., Blue Cross Blue Shield of Tennessee, Wellpoint, Inc., Affinity Health Plan, Inc., Keystone/AmeriHealth Mercy Health Plans PA, and Puerto Rico Department of Public Health.

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>● 1,220,000 – theft of laptop; AvMed, Inc.</li> <li>● 1,023,209 – theft of hard drive; Blue Cross Blue Shield of Tennessee</li> <li>● 480,000 - hacking/IT incident of network server; Wellpoint, Inc.</li> <li>● 400,000 – hacking incident, network server; Puerto Rico Department of Public Health</li> </ul> | <ul style="list-style-type: none"> <li>● 344,579 - type and location “other”; Affinity Health Plan, Inc.</li> <li>● 285,691 – loss of portable electronic device; Keystone/AmeriHealth Mercy Health Plans PA</li> <li>● 105,470 – theft of hard drive; Dept. of Health Care Policy &amp; Financing</li> </ul> |
|---|---|

## So, Here Is Our Plate...



## Here Is HHS' Plate...



## Don't be fooled...



- Enforcement will come
  - Already beginning
- OCR is logical
  - Security is relatively new to them
  - Still awaiting final rules from HHS
  - Hiring new FTEs; increasing budgets
- It never hurts to be conservative

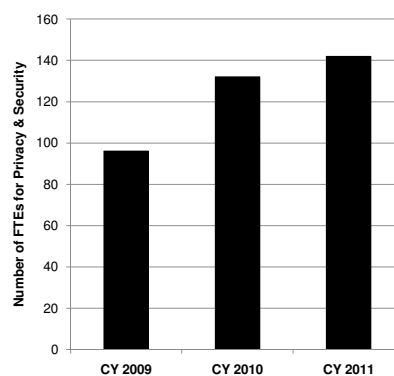
*Are You Ready?*

## OCR's FY 2011 Requested FTEs/ Budget

•Increasing FTEs devoted to Health information Privacy and Security Rule Compliance and Enforcement

•Budget increasing from \$19.9 million (2010) to \$22.8 million (2011)

•(if approved)



## Resolution through CIVIL MONETARY PENALTIES

- New Civil Monetary Penalties under HITECH
- Mandatory penalties for “willful neglect”

Level of Intent/Neglect	Each Violation	All Identical ViolationS per CY
Without Knowledge	\$100 - \$25,000	\$1,500,000
Based on reasonable cause	\$1000 – \$50,000	\$1,500,000
Willful neglect	\$10,000 – \$50,000	\$1,500,000
Willful neglect, not corrected	\$50,000	\$1,500,000

David Holtzman, OCR, HCCA Compliance  
Institute, April 2010

13

## Recent Enforcement


- 1<sup>st</sup> Criminal Conviction of individual for “snooping”
  - Houping Zhou, cardiothoracic surgeon
  - 4 months in prison
  - \$2000 fine
- FTC/OIG joint settlements with:
  - Rite Aid Corporation
    - \$1 million resolution & Corrective Action Plan
  - CVS Pharmacy Inc.
    - \$2.25 million resolution & Corrective Action Plan

Release No. 10-079 - Microsoft Internet Explorer provided by Health Care Policy and Financing

http://www.justice.gov/usao/cac/pressroom/pr2010/079.html

The United States Attorney's Office  
**Central District of California**

Home  
 About the USAO  
 How Can We Help?  
 Working With The Community  
 Press Room  
 Employment  
 En Español  
 Links



United States Attorney's Office  
 Central District of California  
 Thom Mrozek  
 Public Affairs Officer  
 (213) 894-6947  
 thom.mrozek@usdoj.gov

Return to the 2010 Press Release Index  
 Release No. 10-079

April 27, 2010

EX-UCLA HEALTHCARE EMPLOYEE SENTENCED TO FEDERAL PRISON FOR ILLEGALLY PEEKING AT PATIENT RECORDS


LOS ANGELES - A former UCLA Healthcare System employee who admitted to illegally reading private and confidential medical records, mostly from celebrities and other high-profile patients, was sentenced today to four months in federal prison.


Huping Zhou, 47, of Los Angeles, was sentenced this afternoon by United States Magistrate Judge Andrew J. Wistrich, who condemned Zhou for his lack of respect for patient privacy.

**“Zhou is the first person in the nation to be convicted and incarcerated for misdemeanor HIPAA offenses for merely accessing confidential records without a valid reason or authorization.”**

## Joint OCR/FTC investigations and settlements

- CVS Pharmacy (January 2009)
- Rite Aid (July 2010)





“The OCR opened its investigation...after media reports alleged that protected health information maintained by several retail pharmacy chains was being disposed of in dumpsters that were not secure.”

– “The OCR, ...opened its investigation...after television media videotaped incidents in which pharmacies were shown to have disposed of prescriptions and labeled pill bottles containing individuals’ identifiable information in industrial trash containers that were accessible to the public.”

## Georgina Verdugo, director of OCR, after the CVS Settlement:

- “It is critical that companies, large and small, build a *culture of compliance* to protect consumers’ right to privacy and safeguard health information. OCR is committed to strong enforcement of HIPAA. We hope that this agreement will spur other health organizations to examine and improve their policies and procedures for protecting patient information during the disposal process.”

## OCR Case Example

- Health Plan Corrects Computer Flaw that Caused Mailing of EOBs to Wrong Persons

A national health maintenance organization sent explanation of benefits (EOB) by mail to a complainant’s unauthorized family member. OCR’s investigation determined that a flaw in the health plan’s computer system...



## PCAST Report



*“Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward”*

Recommendations to the President (*December 2010*)

- Federal government to facilitate widespread adoption of a “universal exchange language”
- Recommendations for cultivating information technology (IT) ecosystem
  - “a more medically useful and secure system in which individual bits of healthcare data are tagged with privacy and security specifications”

## OIG Looking at HIPAA Compliance in 2011 Work Plan



- CMS’ policies and procedures on breaches/medical identity theft
- Actions CMS has taken in response to breaches
- Adequacy of OCR’s oversight of the HIPAA Privacy Rule
- Security controls implemented by Care/Caid contractors and hospitals to prevent loss of PHI stored on portable devices and media
  - laptops, jump drives, backup tapes, equipment considered for disposal
- Medicaid Management Information Systems (MMIS) Business Associate Agreements, Security Controls over state web-based applications, security controls at the mainframe data centers that process states’ claims data

## It's not just about getting in trouble with the feds...

- State Attorneys General enforcement
- State Breach Notification Laws
  - 46 states, the District of Columbia, Puerto Rico and the Virgin Islands so far
- “Your name in lights”
- Average cost of data loss per individual = \$204
  - 2009 Ponemon Institute/PGP Corporation study

## Connecticut Attorney General Reaches First State HIPAA Settlement with Health Net

- July 6, 2010
- Settlement with Health Net and its affiliates
- Failure to secure private patient medical records... on half million Connecticut enrollees and notify consumers ...
  1. Two years of consumer credit monitoring; \$1 million of identity theft insurance
  1. Reimbursement for costs of security freezes
  2. Corrective Action Plan
  3. \$250,000 payment to state for statutory damages
  4. Additional \$500,000 contingent payment to state if lost disk drive accessed and information used illegally

## What is a Data Breach?

- Now defined federally for health care
    - ARRA/HITECH
  - State's define it differently
    - Personal information + data element(s)= breach
- Often:
- Much stricter reporting timeframes
  - More requirements
  - Harm allowance?

## Section 13400 of Recovery Act

- Breach = an “unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the protected health information”
  - Effective September 23, 2009
  - You must notify:
    - Each affected individual (always)
    - The federal government (always)
    - The media (sometimes)

## Per the Regulations (Interim Final Rule)

- The unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which:
  - Compromises the security or privacy of PHI
  - Poses a significant risk of financial, reputational, or other harm to an individual (Risk Assessment)
  - Any form (i.e. verbal)
  - Exceptions for incidental uses or disclosures

## Safe Harbor

- Data that is encrypted or destroyed cannot be breached
  - Encryption = according to National Institute for Standards & Technology (NIST) standards
  - Destruction = shredded appropriately; cannot be reconstructed

## Risk Assessment

“Not a lot of Guidance?”

**Feds allowing for Flexibility?**

**Congress Upset!**

- Judged by the feds with a retroscope
- Documentation key
- Per HHS: reputational harm – “as cognizable a form of harm as physical or financial harm”

## Breach Case Study #1

- State going live with new online eligibility system for Medicaid
- Instructional video uploaded to website contained real client information, not “dummy”
- Information released
  - name, social security number, date of birth, address, children's names, children's dates of birth, husband's name, every state benefit they were receiving including welfare, Medicaid, etc.
- One individual (& her family) impacted.

## Case Study #1 (cont.)

- Investigation Begun
  - Video pulled immediately upon discovery (23 hrs later)
  - Forensics on internet clip
  - 86 people had accessed file
  - IT began analysis to determine if only state employees had accessed clip
- Didn't matter.
- We notified the client within 4 working days of discovery.

## Case Study #2

- Hard drive missing from computer placed in 'spare parts' cubicle at Business Associate's secured facility
- Used as server to run reports comparing patient systems to each other
- Contained 556,000+ patient records (all existing Medicaid & CHP+ patients)
- Information included (only):
  - Patient name
  - State ID
  - Program category (i.e. CHP+, Elderly, Blind & Disabled, Breast and Cervical Cancer, etc.)

## Case Study #2, cont.

- Facts gathered
- Colorado Bureau of Investigations called in to investigate
- Risk Assessment performed
- Based on “significant risk of reputational or other harm”.... we notified 105,432 individuals of the breach of their unsecured PHI

## Our Risk Assessment

Out of 566,523 total records:

111,513 fell in

455,016 fell out

Some duplicates =  
105,432 letters sent out to clients

Approximate cost to the state – tens of thousands

Category	#		Notify	No Notification
1931	124996	-		124996
4 month extended	1264	-		1264
Breast and Cervical Cancer PE	19	+	19	
Breast or Cervical Cancer	396	+	396	
CHP+	65808	-		65808
CHP+ Child PE	260	-		260
CHP+ Newborn	1918	-		1918
CHP+ Prenatal	1410	+	1410	
CHP+ Prenatal PE	155	+	155	
Eligible Needy Newborn	27872	-		27872
Expanded Child	56297	-		56297
Expanded Pregnant Women	8533	+	8533	
HCBS BI	206	+	206	
HCBS CDCE	1	+	1	
HCBS CES	384	+	384	
HCBS CHCBS	1230	+	1230	
HCBS CWA	64	+	64	
HCBS DD	4385	+	4385	
HCBS EBD	17270	+	17270	
HCBS MI	2026	+	2026	
HCBS PACE	1389	-		1389
HCBS PHW	91	+	91	
HCBS PLWA	38	+	38	
HCBS SLS	2269	+	2269	
Legal Immigrant Prenatal	541	+	541	
Medicaid Child PE	2483	-		2483
Medicaid Prenatal PE	1132	+	1132	
NF/30 Day Medicaid	10319	-		10319
OAP - A Med	6526	-		6526
OAP - A Med > 65 Psych	3	+	3	
OAP - B Med	512	+	512	
OAP - HCP (A)	1424	-		1424
OAP - HCP (B)	2815	+	2815	
Parents Plus	16125	-		16125
Pickle	245	-		245
Psych < 21	10	+	10	
QDWI	1	+	1	
QI-1	2782	-		2782
QMB	23105	-		23105
Qualified Child	7588	-		7588
Qualified Disabled Widow	1	-	1	
Qualified Pregnant Women	7144	+	7144	

## What Fell In?

- Obvious categories
  - Psych
  - Mental illness
  - Cancer
  - Old-age Pension
  - Refugee
  - Elderly, blind or disabled
- Anybody pregnant or prenatal
- All waiver programs
- Any category <30

## What Fell Out?

- Medicaid
- 1931
- Pickle
- CHP+

## Outcome

- Do you agree with our outcome?
- Do you disagree?
- Remember:
  - Risk assessment is fact-specific
  - Different covered entities will perform the RA differently, based on many factors (risk tolerance, etc.)
  - Do what you feel you can defend & what will enable you to sleep at night
  - DOCUMENT IT!

## Practical Advice – Risk Assessments

- Gather all the facts first
- Consider getting Legal Involved *early* – especially with the big breaches
- Take your time (but not too much)
- Use a tool or matrix
- Limit the people involved
  - Privacy, Security, Legal, Other?
- Know who is in charge

## Breach Learning Lessons

- Write a simple Notification Letter
  - Use bullets
  - Use boxes to highlight information
- Translate it into other languages – be generous (but use expertise)
- Inform everyone on your staff and all affected business entities before you send your Notice
- Have “live” people available to talk with affected individuals
- If business associate(s) involved, do not assume that they ‘have your back’
- Identify – up front – who will be involved in the process (& who won’t be)

## Practical Advice – Data Breaches

- Create/update policies and procedures
- Make sure everyone knows the importance of reporting actual or suspected breaches to the Privacy Officer ASAP
- Create a process for logging & reporting ALL breaches
- Encrypt everything that moves -- email? laptops? portable media?
- Lock down everything that doesn't (at least twice)
- Make sure you're correctly disposing of any discarded PHI

37

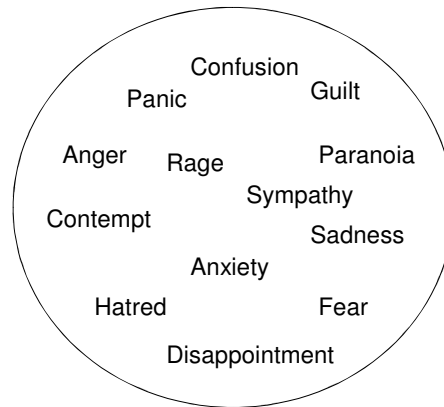
## Expect:

- Inner turmoil
- External turmoil
  - especially if BAs are involved
- To trigger Substitute Notification
- To be in multiple media outlets, multiple times, multiple ways
- The Unexpected

## And...be Ready for a Range of Human Emotions

Emotionality:

- a measure of a person's emotional reactivity to a stimulus.



## What's Could be Fixed with this Process?

- False Positives
- "Need for speed" drives the message
  - Governmental forces
  - Other
- Assumption that everyone should get the same message

### ***Quote of the Day***

"You can train, you can have seminars, do physical security surveys, but every once in a while people make mistakes, machines make mistakes, business associates make mistakes, people steal or lose hardware. Sometimes the disclosures are small and sometimes they are huge, but the bottom line is a privacy officer or organization can't plan for every eventuality. The most you can do is train, do risk assessments and when something unexpected happens, think on your feet and mitigate."

- An unidentified privacy officer

### **Top Predictions for Information Technology in 2011:**



1. Health information exchanges, many of which will be launched by inexperienced and understaffed organizations, will force more attention on security and privacy;
2. Increased fines and regulatory action by State Attorneys General and regulatory agencies;
3. Data breaches and associated costs will increase...
4. Hospital governing-boards will exert their power to manage data breach risks...
5. A significant "data spill" is inevitable and will bring national attention to the issue
6. Heightened patient awareness and concern over the security of their private medical data...

“2011 will be the year that Americans recognize they can’t control personal health information in health IT systems and data exchanges.”

*-- Dr. Deborah Peel, M.D., practicing physician and founder of Patient Privacy Rights*

## **On a Positive Note...**

“The best thing about the future is that it only comes one day at a time.”

Abraham Lincoln

**Thank you.**

Erika Bol  
[Erika.bol@state.co.us](mailto:Erika.bol@state.co.us)  
303-866-2958