


**The House Always Wins –
How Recent HIPAA Privacy and Security
Enforcement Efforts Can be used to stack the
deck in your favor.**


Darrell Contreras,
Chief Compliance Officer,
Lakeland Regional Medical Center



www.hcca-info.org | 888-580-8373

HIPAA Enforcement

- Regulatory Enforcement
- Criminal Enforcement
- Civil Lawsuits




www.hcca-info.org | 888-580-8373

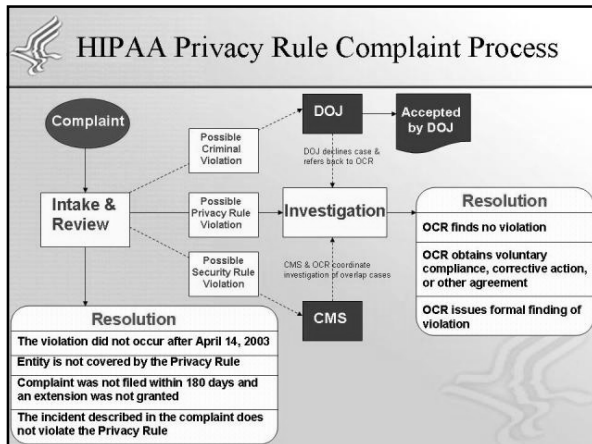
Regulatory Enforcement - Overview

Which agencies are involved?

- _____
- _____
- _____



www.hcca-info.org | 888-580-8373



Regulatory Enforcement - Let's Look at the Numbers

From April 2003

- Total number of Privacy Complaints received by OCR:

- Of that number, 80%, or _____ have been resolved.
- Of that number, 23,466 were not eligible for enforcement.
- That leaves approximately _____ that were eligible for enforcement.

HCCA HEALTH CARE COMPLIANCE ASSOCIATION www.hcca-info.org | 888-580-8373

Regulatory Enforcement - Violation or No Violation

<p>CASE INVESTIGATED – SOME VIOLATION FOUND:</p> <p>_____</p>	<p>CASE INVESTIGATED – NO VIOLATION FOUND:</p> <p>_____</p>
--------------------------------------------------------------------------	------------------------------------------------------------------------

HCCA HEALTH CARE COMPLIANCE ASSOCIATION www.hcca-info.org | 888-580-8373

Piedmont Hospital – HIPAA Audit

- March 2007 Audit

Providence Resolution Agreement

- Facts
 - December of 2005
 - Four backup tapes and two optical disks were stolen from an employee's van that was parked overnight.
 - The data was not encrypted
 - The practice was followed and known by staff of Providence Home and Community Services.
 - Unencrypted laptops containing ePHI were stolen on 4 separate occasions from September 29, 2005 – March 3, 2006.
 - Information for 365,000 people was compromised.

So what did it cost?

- \$100,000 to settle the case
- Attorneys fees to defend against the class-action lawsuit
- The cost of one year of credit protection services for the 365,000 patients
- The cost to implement the resolution agreement
- Time and expense to immediately upgrade security/encryption measures

What had to be done?

- Within 90 days - Policies approved by HHS to support the privacy and security rule
- Within 30 days of HHS approval of policies – Distribute and evidence distribution of all policies to **ALL** members of the workforce who have access to ePHI.
- Within 60 days of HHS approval of policies – Implement the policies.
- Within 90 days of HHS approval of policies – Provide training to **ALL** workforce members, with a written or electronic certification of attendance.
- Within 120 days of HHS approval of policies – submit an implementation report summarizing the efforts to complete the Corrective Action Plan.
- **ALL** workforce members who receive the policies must attest that they have read, understand and will abide by the Policies and Procedures.
- Report any violation of the policies to HHS in writing within 30 days.
- Quarterly – Conduct and document monitoring reviews to ensure compliance through unannounced site visits, interviews, random audits of portable devices.
- Submit Annual Reports summarizing the efforts of the Corrective Action Plan for 3 years.



www.hcca-info.org | 888-580-8373

10

Criminal Enforcement

- OCR has referred _____ cases to the DOJ
- Of those cases, _____ have been prosecuted
- Highlights:
 - October 2006 – Cleveland Clinic, Weston, Florida
 - July 2008 – Northeast Arkansas Clinic
 - November 2008 – UCLA Medical Center



www.hcca-info.org | 888-580-8373

11

Civil Litigation

- 5th U.S. Circuit Court Appeal decision from 2006
 - “HIPAA has no express provision creating a private cause of action.”
- *Sorensen, et al v. Barbuto, et al*, 143 P. 3rd, 295 (Utah Ct. App. 2006) – footnoted reference to HIPAA, but overturned a dismissal on the basis that the confidentiality of the physician-patient relationship creates a legal duty.
- *Acosta v. Byrum*, 638 S.E.2d 246 (N.C. Ct. App. 2006) – overturned a dismissal at the trial court level asserting that HIPAA establishes the standard of care for a negligence claim.
- Providence lawsuit related to Resolution Agreement and Settlement dismissed by Oregon Court.



www.hcca-info.org | 888-580-8373

12

Identifying the Risk Universe

- Start with 3 main categories:
 - Criminal
 - Regulatory
 - Civil

Risk Assessment – Criminal

- **Criminal Risk**
 - **Intentional Malfeasance by Employees**
 - **Impact**
 - **Financial** - How much would it cost the organization?
 - **Reputation** – How will it hurt the organization's standing in the community?
 - **Patient Satisfaction** – How are patients going to view us or evaluate us on surveys after this event?

Risk Assessment – Criminal

- **Likelihood**
 - **Regulatory response** – what is the likelihood of a government investigation?
 - **Public response** – what is the likelihood that the public or patients will care or respond?
 - **Motive** – Does our location, workforce, or culture have a history or tendency to have something like this occur?
- **Mitigation**
 - **Training Efforts**
 - **Audits**
 - **How much have you done to reduce this risk?**

Regulatory Enforcement

- _____
- _____
- _____
- _____
- _____



www.hcca-info.org | 888-580-8373

16

Civil Liability

- Cause of Action—Negligence
 - Duty
 - Breach of Duty
 - Causation
 - Damages



www.hcca-info.org | 888-580-8373

17

HIPAA Regulatory Audit

- Piedmont Hospital – Atlanta, GA.
 - 1st HIPAA Audit
 - Conducted by the OIG of the Department of Health and Human Services (DHHS)
 - Data request for 42 items
 - Production timeframe: **10 DAYS!**

Here is the link:

<http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9025253>

(last tested 1/29/09)

Google Search Phrase: "42 Questions HHS"



www.hcca-info.org | 888-580-8373

18

Providence Health Services

- Causes:

- Four backup tapes and two optical disks were stolen from an employee's van that was parked overnight.
- The data was not encrypted.
- The practice was followed and known by staff of Providence Home and Community Services.
- Unencrypted laptops containing ePHI were stolen on 4 separate occasions from September 29, 2005 – March 3, 2006.
- Information for 365,000 people was compromised.



www.hcca-info.org | 888-580-8373

19

NEWS

Millions Believe Personal Medical Information Has Been Lost or Stolen

Issue a Roadblock to Acceptance of Electronic Health Record Systems

Last update: 5:01 a.m. EDT July 15, 2008

ROCHESTER, N.Y., Jul 15, 2008 (BUSINESS WIRE) -- According to The Harris Poll(R), four percent or an estimated nine million American adults believe that they or a family member have had confidential personal medical information either lost or stolen. Results of the poll of 2,454 adults surveyed online between June 9 and 16, 2008 by Harris Interactive(R), which was designed in collaboration with Dr. Alan F. Westin, Professor of Public Law and Government Emeritus at Columbia University.



www.hcca-info.org | 888-580-8373

20

Portable PHI

Intended

Incidental

_____	_____
_____	_____
_____	_____
_____	_____



www.hcca-info.org | 888-580-8373

21

A Note on Off-Site Record Storage

- Limitation of Liability:
 - Company shall exercise such care in storing Customer's goods, including files, records, and electronic media and in providing services in connection therewith as a reasonably careful person would under similar circumstances. Company shall not be liable for any loss or damage, however caused, unless such loss or damage results from a failure of Company to exercise such a level of care.
 - If Company becomes liable to Customer for failing to exercise such level of care in storing Customer's goods, including files, records, and electronic media and/ or in providing services to Customer hereunder, Company's liability to Customer shall be limited to \$2.00 per cubic foot of material, beyond which value per unit Company shall not be liable, including for consequential, punitive, incidental or exemplary damages.
 - Customer acknowledges that it is customer's responsibility to obtain its own insurance for any loss or damage beyond the scope of company's agreed limited liability hereunder if, in Customer's judgment, there exists a potential for loss or damage in excess of such limitation.



www.hcca-info.org | 888-580-8373

22

How to mitigate HIPAA exposure in an expanding regulatory environment

- New issues and stories will come up
 - Look at the causes
 - Why did this hit the newspaper?
 - Add it to your risk assessment matrix.
- “Best Practices” may not be best for your organization
 - Are they required?
 - Are they realistic?



www.hcca-info.org | 888-580-8373

23

Wrapping Up



www.hcca-info.org | 888-580-8373

24
