HIPAA 102a
What You Don’t Know About HIPAA Privacy and Security Can Really Hurt You! Revision 2015
Presented by
Jack Kolk President
ACR 2 Solutions, Inc.
Todays Agenda:

1) About Myself - Jack Kolk, CEO of ACR 2 Solutions a information security and privacy compliance software and consulting company. We are the Compliance Partner for 211 LA County.

2) Overview of the changes in the Omnibus law

3) Penalties and Fines

4) Examples of HHS Audit Findings and thought leader Recommendations

5) Examples of Audits Fines and Enforcement

6) Lessons Learned and what should we be doing?

7) Questions and answers
The Omnibus Rule and What has changed!

HITEC Major Changes to HIPAA Privacy and Security Rules:

Business Associates and Subcontractors liability
  – Wellpoint $1.7 Million fine and Sutter Health 11 class-action lawsuits

Breach Notification
  – Letter to a doctor after reporting a breach
  – Affinity Health Plan’s Photocopier Settlement

Civil and Willful Neglect Penalties
  – Up to $1.5 Million

Private Right to Sue
  – Notice to a Physician
  – July 2013 Privacy violation $1.44M Walgreen

And More…
  – Cardiac Phoenix Healthcare $100 K and the:
  – 3/3 “failure to obtain reasonable assurance”
  – NSF media and 2 Doctors for posting Pictures of a rhinoplasty
Getting to know you.

1. Who here is a “Covered Entity”?  
2. Who here is a “Business Associate”?  
3. Have attested for Meaningful use funds?  
4. Who has read the HIPAA Security Rule?  
5. Who has read the HIPAA Privacy Rule?  
6. Who has read the “Omnibus Rule”?  
7. Who thinks they would pass a HIPAA Audit?  
8. Who has attended one of my presentations before?
Why did I call it HIPAA 102a?

Hint: (I assuming that you are familiar with … )

Health Insurance Portability and Accountability Act of 1996
- HIPAA 1a - Privacy Rule – in place since 2003
- HIPAA 1b - Security Rule – in place since 2005
  • was adopted to address the implementation provisions of HIPAA

HIPAA 101
- HITECH Act 2010
  • Meaningful Use
  • Changes to the law

HIPAA 102
- Omnibus Rule and beyond with recent enforcement examples
There 2 Major Parts to HIPAA

HIPAA Security Rule covers several areas:

- Rules regarding health coverage qualification
- Rules regarding data interchange
- Regulations protecting security of ePHI

HIPAA Privacy Rule focuses on:

- Privacy of Protected Health Information (PHI)
Acronyms and Abbreviations

1) Health Information Technology for Economic and Clinical Health Act - “the HITECH Act”
2) HIPAA Privacy Rule - HIPAA Security Rule
3) ONC – the Office of the National Coordinator for Healthcare
4) OIG – Office of the Inspector General
5) PHI – Protected Health Information
6) ePHI – electronic Protected Health Information
7) BA - Business Associate
8) CE – Covered Entity
9) Breach Notification,
10) Reasonable Assurance, Justifiable Assurance
11) Willful Neglect and Reasonable diligence
PHI what is it?, what isn’t it?

HIPAA PHI: List of 18 Identifiers

1. Names;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code…
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; etc.
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or ..
HIPAA Omnibus Rule
Summary of Major Provisions
This omnibus final rule is comprised of the following four final rules:

1. **Final modifications to the HIPAA Privacy and Security and Enforcement Rules mandated by HITECH**
   1. Make business associates (BA’s) of Covered Entities directly liable for compliance with certain of the HIPAA requirements.
   2. Strengthen the limitations on the use and disclosure of PHI for marketing and fundraising and resale of PHI
   3. Expand individual right of ownership and disclosure
HIPAA Omnibus Rule
Summary of Major Provisions
This omnibus final rule is comprised of the following four final rules:

Final modifications HIPAA Privacy and Security and Enforcement Rules mandated by HITECH
(continued)

4. Require modifications to, and redistribution of, a covered entity’s notice of privacy practices.

5. Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof.

6. Adopt additional HITECH Act enhancements to the Enforcement Rule. Such as the enforcement of noncompliance with the HIPAA Rules due to “willful neglect”.
HIPAA Omnibus Rule

Summary of Major Provisions

This omnibus final rule is comprised of the following four final rules:

2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure. More on this later

3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule’s “harm” threshold with a more measurable standard.

4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information.
Important Dates are here now!

1. Rules went into effect **March 26, 2013**
2. Compliance Deadline **Sept 23th, 2013** for HIPAA Privacy and Security
3. BA Agreements, updated and renewal
   1. BA Agreements in place by **Sept 2013**
   2. Auto-renewing Agreements updated at time of renewal
   3. Full BA Agreements updated by no later than **Sept 2014**
Penalties and Fines

What has Changed??
How does or could it affect me?
Risk Assessment puts you firmly on the path to “Reasonable Diligence” for HIPAA Security and Privacy

Table 3: Tiered Civil Monetary Penalties

<table>
<thead>
<tr>
<th>Standard of Culpability</th>
<th>Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know of the violation and by exercising reasonable diligence would not have known of violation</td>
<td>Corrective action without penalty</td>
<td>No penalty--however, subject to discretion of Secretary.</td>
</tr>
<tr>
<td>Unknowing Violations</td>
<td>At least $100 per violation</td>
<td>Not to exceed $1,500,000</td>
</tr>
<tr>
<td>Violation due to reasonable cause, not willful neglect</td>
<td>At least $1000 per violation</td>
<td>Not to exceed $1,500,000</td>
</tr>
<tr>
<td>Violation due to willful neglect</td>
<td>At least $10,000 per violation</td>
<td>Not to exceed $1,500,000</td>
</tr>
<tr>
<td>Violation is due to willful neglect and the violation is not corrected within 30 days of the first date the person liable for the penalty knew or should have known that the violation occurred.</td>
<td>At least $50,000 per violation</td>
<td>Not to exceed $1,500,000</td>
</tr>
</tbody>
</table>
New Definition of what constitutes a Breach!

(2) Except as provided in paragraph (1) of this definition,
“an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health information was actually acquired or viewed; and
(iv) The extent to which the risk to the protected health information has been mitigated.”
Recent fines for Breach

Affinity Health Plan - $1.2M for photocopier
  - > 344K records on copier drive, but units returned, some unknown. 2010

Goldthwait Assoc. and 4 clients $140,000
  - Improper disposal of paper records. 2010

Anthem Blue Cross Fined $150,000 for 34K letters
  - Printed with some SS#’s viewable through the envelope window. Oct. 2012

Alaska Medicaid pays HHS $1.7M
  - USB drive stolen, no policies, no training, etc..
New HIPAA Privacy and Security Rules for Covered Entities and Their Business Associates

Federal Register at Vol. 78, No. 17, Friday January 23, 2013, starting at page 5566.

Major Changes from 2003 HIPAA Regulations –

1. New definition of “Business Associate” covers any person or organization that “creates, receives, maintains or transmits protected health information…” (page 5688)

2. Business Associates are directly responsible for HIPAA privacy and security compliance (page 5589).

3. HIPAA non-compliance by Business Associates can create up to $1.5 million in liability for Covered Entities (page 5691).
HIPAA/HITECH
Business Associate Decision Tree

1. Is Protected Health Information (PHI) being disclosed to a person or entity other than in the capacity as a member of the covered entity's workforce?
   - Yes
   - No

2. Is the PHI being disclosed to a healthcare provider for treatment purposes (e.g., primary/referring physician, contract physicians or specialists, contract nursing staff, contract rehab staff, ambulance, home health, dentist, etc.)?
   - Yes
   - No

3. Is the PHI being disclosed to a health plan for payment purposes, or to a health plan sponsor with respect to disclosures by a group health plan?
   - Yes
   - No

4. Is the PHI being disclosed to a government agency pursuant to an official investigation (e.g., CMS, OCR, OSHA, FDA, Health Department, etc.)?
   - Yes
   - No

5. Is the PHI being disclosed to another covered entity that is part of an organized healthcare arrangement in which the originating covered entity participates?
   - Yes
   - No

Business Associate Agreement is NOT needed.
HIPAA/HITECH
Business Associate Decision Tree

6. Does the other person or entity create, receive, maintain or transmit PHI for a function or activity regulated by HIPAA, including: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefits management, practice management, and repricing?

7. Does the other person or entity provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services where the provision of such services involves disclosure of PHI to the person or entity?

8. Will the other person or entity be able to access PHI on a routine basis, AND/OR is there a possibility that the PHI in the person or entity’s custody or control could be compromised (e.g., data storage vendor, document shredding company, or other, etc.)?

Business Associate Agreement IS needed.
Entities specifically included under HITECH:
- Health Information Organizations
- E-prescribing Gateways
- Data transmission vendors with routine access to PHI
- Personal Health Record vendors that offer a PHR to individuals on behalf of a covered entity
- Subcontractors that create, receive, maintain, or transmit PHI for or on behalf of a business associate

2nd Section continued
Omnibus Law effective as of Mar 26 2013
What are BA’s required to do?

What are HIPAA Business Associates required to do?

- Comply with HIPAA’s Security Rule – Implement specific policies & procedures; and implement physical, administrative, and technical safeguards to protect medical data.
- Follow HIPAA’s Privacy Rule – Protect medical data from misuse; and follow the terms of new or existing Business Associate contracts.
- Train All Employees on HIPAA and the Business Associate Requirements – Employees must be trained to provide the strongest protections to medical data.
- Provide “Breach Notifications” if Medical Data is Compromised or Lost – Business Associates must promptly notify their medical entity partners – and in some cases, patients – if medical data in the Business Associates possession is compromised or lost.
- Other Requirements Also Apply – This is not a comprehensive list. These items are only a portion
Business Associates and Security Breach Notification

1) **Subcontractor** “any person to whom a BA delegates a function, activity or service, other than a member of BA’s workforce”

2) Subcontractor is a BA if they “create, receive, maintain or transmit” PHI on behalf of a business associate

3) Status of a business associate flows down the chain of custody of ePHI
Business Associates Agreement per the AMA Agreement

1) **Reasonable Assurance** is driving new BA agreements

2) AMA Business Associate Agreement – Sample Notice

   - **Section** - 2.26 Implement Information Security Program. Upon request, Contractor shall make available Contractor’s security program, including the most recent electronic Protected Health Information risk analysis, policies, procedures, security incidents and responses and evidence of training.

3) Subcontractors of BA’s must do the same!
Liability of Covered Entities and Business Associates for Violations by Their Business Associates and Sub-Contractors

**Old standard:** CE not liable for violations of BA if

- Compliant BA Agreement in place
- CE did not know of pattern or practice by BA in violation of BA Agreement
- If CE knew of pattern or practice, took reasonable steps to cure or terminate if feasible or, if termination not feasible, reported to HHS

**New standard:**

- CE liable for acts of BA that is its agent under federal common law
- BA liable for acts of subcontractor that is its agent under federal common law
- Where BA or subcontractor not agent, old standard applies
Lesson Learned:

Don’t call it a “Breach”, call it an incident or an event, until you do your assessment.

*Document* your reasons for not reporting it as a breach

Transition to encryption of data at rest. It’s a requirement of Stage 2 meaningful use starting in 2014.
The Audits are here!

CMS TO BEGIN AUDITS OF ATTESTING PROVIDERS

The Centers for Medicare and Medicaid Services (CMS) has begun audits of attesting providers (those stating they have met “Meaningful Use” requirements) under the HITECH Act. CMS announced its plan to audit 10% of attesting providers and “...being found deficient on any one measure, will cause a provider to be out of compliance. In this case, CMS will recoup the provider’s entire stimulus.” In addition, the first issue to be addressed in an audit will be the medical practice’s IT security risk assessment.
HIPAA Compliance Vs. Security

- **Compliance** involves meeting the “standard of care” by whatever regulatory authority overseeing them. OCR is the enforcer and HIPAA is the standard.

- **Security** is keeping unauthorized persons away from accessing, corrupting or destroying sensitive data.

- **HIPAA** does not require that you be perfectly secure, it requires you to be compliant “as reasonable and appropriate’..

- **Your Organizations** (CE’s and BA’s and their subcontractors) are required to be compliant with the law!
HHS Audits 2013 Results - OCR

Security Results

58 of 59 providers had at least one Security finding or observation

No complete & accurate risk assessment in two thirds of entities
- 47 of 59 providers,
- 20 out of 35 health plans and
- 2 out of 7 clearinghouses

Security addressable implementation specifications: Almost every entity without a finding or observation met by fully implementing the addressable specification.
they're liable for HIPAA compliance under the HIPAA Omnibus Rule.

In OCR's audits and breach investigations, "we will really look at the level of compliance at both covered entities and business associates," Rodriguez stressed in his Sept. 23 presentation.

Under the permanent program, audits will focus on vulnerabilities that might change year to year as new issues come into focus, Rodriguez said.

A major weakness found during the pilot audit program, as well as through OCR breach investigations, has been a lack of thorough risk analysis, he added.
HIPAA Audits: A Preliminary Analysis

Security a Bigger Challenge Than Privacy

By Marianne Kolbasuk McGee, June 20, 2012. ★ Credit Eligible

The initial 20 HIPAA compliance audits found that more organizations had trouble with security compliance than privacy compliance, and smaller organizations had more difficulties than larger ones, a preliminary analysis by federal officials shows.

Many of the audited organizations hadn't been conducting regular risk assessments, says Linda Sanches, a federal official involved in supervising the audits. For some of the organizations audited, "HIPAA hasn't been a priority for several years. ... Risk assessments were done six years ago and haven't been looked at since," she says.
Security Issues

Top Security Issues
The top HIPAA Security Rule compliance issues identified in the first round of audits, Sanches says, included:

- User activity monitoring;
- Contingency planning;
- Authentication and integrity;
- Media reuse and destruction;
- Risk assessments;
- Granting or modifying user access.

Many smaller entities, in particular, are having trouble setting up HIPAA compliance programs and implementing them, Sanches says. "Larger institutions are getting better at that," she adds.

The first round of audits also showed that many organizations aren't paying enough attention to managing third-party risks, including monitoring whether there have been issues with business associates that need to be addressed, Sanches adds.

RELATED WHITEPAPERS
- Guide to Mapping Splunk Enterprise to PCI Requirements
- Using Healthcare Machine Data for Operational Intelligence
- Achieving Compliance in Digital Investigations
- 5 Ways to Use Security Intelligence to Pass Your HIPAA Audit
BA are the Biggest Security Risk

The 2015 Healthcare Information Security Today survey found that business associates taking inadequate security precautions is perceived to be the biggest security threat facing healthcare organizations today. Nevertheless, many covered entities aren't taking steps needed to help reduce the risks posed by business associates, says privacy and security attorney David Holtzman.
Meaningful Use
Audit Determination Letter

Your practice has not met the meaningful use requirement!

(Once they received this, they have signed up with us!)
Dear Dr. [Redacted]

We have completed our meaningful use audit of the certified Electronic Health Record (EHR) technology utilized in your practice in accordance with Section 13411 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), as included in Title XIII, Division A, Health Information Technology and in Title IV of Division B, Medicare and Medicaid Health Information Technology of the American Recovery and Reinvestment Act of 2009. The HITECH Act provides the Secretary, or any person or organization designated by the Secretary, the right to audit and inspect any books and records of any organization receiving an incentive payment.

We performed a review of your practice’s meaningful use attestation for the Program Year 2012 and Payment Year 1. Based on our review of the supporting documentation furnished by you, we have determined that your practice has **not met the meaningful use criteria** for the following reasons:

- Failed Eligible Professional Meaningful Use Core Measure 15 – Protect Electronic Health Information
Incentive Payments are being recouped – the total payment!

Since you did not meet the meaningful use criteria, the incentive payment will be recouped. You will receive a demand for your total Medicare EHR incentive payment shortly from the EHR HITECH Incentive Payment Center. The demand letter will include all information regarding the repayment process, and will also include your appeal rights.

This audit does not preclude your practice from future, prior or subsequent year audits.

Sincerely,

[Signature]

Peter Figliozi, CPA, CFF, FCPA
Early 2011 Audits

1) Thinking about the numbers
   - Illinois – 821
   - Georgia – 1036
   - Missouri – 1265
   - Wisconsin – 1033

2) Everyone involved in healthcare will soon know a Covered Entity that has been audited!
November 12, 2010

Transaction Number: [REDACTED]

Dear Dr. [REDACTED],

This correspondence follows the November 12, 2010 letter acknowledging your October 5, 2010 reported breach of the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, D and E, the Privacy and Security Rules) to the Department of Health and Human Services (HHS), Office for Civil Rights (OCR). Specifically, you reported the breach of the Protected Health Information of approximately 4700 individuals when a laptop and an out of service server were stolen from your office during a burglary. This allegation could reflect violations of 45 C.F.R. §§ 164.502(a), 164.530(c), 164.308(a)(1)(ii)(A), 164.308(a)(5)(i), 164.308(a)(6)(ii), 164.310(a)(2)(ii), 164.310(c) and 164.312(a)(2)(iv). Additionally, OCR will be reviewing your compliance with 45 C.F.R. §§ 164.404 and 164.406.

Texas
The Privacy and Security Rules provide that, to the extent practicable, OCR will seek the cooperation of covered entities to informally resolve complaints; therefore, we are requesting that you submit your response to OCR no later than close of business December 2, 2010:

1. Documentation of the covered entity’s admission, denial, or a statement indicating that the covered entity has obtained insufficient evidence to make a determination regarding the allegations;

2. Documentation of an internal investigation conducted by the covered entity in response to the allegations including a copy of the incident report prepared as a result of the laptop and server theft;

3. Documentation of the covered entity’s corrective action taken or plan for actions the covered entity will take to prevent this type of incident from happening in the future, including documentation specifically addressing, if applicable:
   a. sanctioning of the workforce member(s) who violated the Privacy and Security Rules, in accordance with the covered entity’s current policies and procedures, and as required by the Privacy Rule;
   b. re-training of appropriate workforce members;
Your responsibility to keep and submit the data and information requested is found at:

45 C.F.R. § 160.310(a) Provide records and compliance reports. A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of this part 160 and the Privacy and Security Rules.

45 C.F.R. §164.502(a)(2) Required disclosures. A covered entity is required to disclose protected health information: ...(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity’s compliance with this subpart.

Your responsibility to cooperate with this investigation is found at:

45 C.F.R. §160.310(b) Cooperate with complaint investigations and compliance reviews. A covered entity must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of a covered entity to determine whether it is complying with the Privacy and Security Rules.

It is very important that you provide the information and data requested on the attached list within the time frame specified above. Failure to do so may result in enforcement efforts to obtain the information. This may include the issuance of a subpoena (see 45 C.F.R. § 160.314) and/or an on-site inspection of your facility, books, records, accounts, or other sources of information, including interviews of workforce members (see 45 C.F.R. § 160.310(c)). Furthermore, failure to provide the requested information in a timely fashion may constitute a violation of the above regulatory provisions and is punishable by a fine of $100 to $50,000 per day.
Resolution Agreement
Fined $100K and references 3 items.
1 was – Reasonable Assurance

RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement ("Agreement") are the United States Department of Health and Human Services ("HHS"). Office for Civil Rights ("OCR") and Phoenix Cardiac Surgery, P.C. ("PCS"), an Arizona for-profit corporation. PCS is hereinafter referred to in this Agreement as "Covered Entity."
Cost of a Audit - Meaningful Use

Comments and Lesson to be Learned:

Don’t file unless you are sure you meet all the requirements!

Have all your paperwork available and printed out. Switching systems has created major issues with attesters when they are audited!

The requirement of Stage 2 meaningful use for 2014 is for 90 days of use, so plan accordingly.
Georgia hospice group sees data breach

ROME, GA | February 22, 2013

Officials at a northwest Georgia hospice group have notified patients of a data breach after an unencrypted company laptop containing personal health information was stolen from an employee’s car in January.

Heyman HospiceCare, part of the 304-bed Floyd Medical Center in Rome, Ga., began mailing letters Feb. 15 to nearly 2,000 patients affected by the breach. Officials say the laptop contained patient names, addresses, phone numbers, dates of birth, Social Security numbers, insurance numbers, clinical diagnoses and provider names.

[See also: 43K affected in Wisconsin data breach.]

"Heyman HospiceCare deeply regrets any inconvenience or concern this may cause patients," a company notice reads. "To help prevent something like this from happening in the future, Heyman HospiceCare is implementing a more disciplined approach to its encryption for all laptop computers and re-educating staff on policies and procedures for securing such mobile devices."

1,828 patients seen at Heyman HospiceCare from July 2006 to January 2013 were affected by the incident.

According to data from the Department of Health and Human Services, some 452,185 patient records in Georgia have been compromised in a breach since the August 2009 Breach Notification rule. The lion’s share of that comes from the Emory Healthcare data breach in 2012, when backup tapes containing personal health information on some 315,000 patients went missing.
Jail time in a federal prison for a misdemeanor HIPAA offense and fined!

• Last year, a former UCLA Health System employee became the first person in the United States to receive jail time in a federal prison for a misdemeanor HIPAA offense. The employee used his employee access to the University’s electronic medical records system to view the medical records of his supervisors, co-workers, and high-profile patients. While none of the information was “used” or sold, the access was nonetheless illegal because the employee lacked a valid reason for looking at the records.

• The ex-employee pled guilty to four misdemeanor counts of violating HIPAA.
• His sentence was four months in prison and a $2,000 fine.
Jail time in a federal prison for a misdemeanor HIPAA offense and fined!

**Hospital Employee Gets Jail Time For HIPAA Violation**

Hospital employee sentenced to federal prison for 3-week long medical records spree.
Published Apr 29, 2010

A Chinese trained surgeon who formerly worked at the UCLA medical center as a researcher was sentenced this week to 4 months in a federal prison following a guilty plea to 4 counts of HIPAA violations. He was also fined $2000 on the misdemeanor offenses. Prosecutors say that this is the first jail sentence for HIPAA violations by a healthcare worker.

The FBI charged that the employee was terminated from his employment in 2003 for performance issues, and then launched into a 3-week long course of accessing records on an unauthorized basis. Among the records were those of his superior, his co-workers and celebrity patients in the UCLA Health System. Tom Hanks, Drew Barrymore and Arnold Schwarzenegger were among more than 320 individuals whose records were accessed.

The attorney for the man told television reporters that his client had no idea that looking at other people’s records was a federal crime for which he could go to jail.
$140 K for paper disposal

State Settles HIPAA Case for $140,000 - HealthcareInfoSecurity

Massachusetts Attorney General Martha Coakley has fined a now-defunct medical billing company and four pathology groups a total of $140,000 in a settlement stemming from a breach involving improper disposal of paper medical records for 67,000 residents. The settlement is with Goldthwait Associates and four of its clients - Milford Pathology Associates, Milton Pathology Associates Pioneer Valley Pathology Associates, and Kevin Dole, M.D., former president of Chestnut Pathology Services.

The medical records were discovered by a Boston Globe photographer in July 2010 when he was disposing of his own trash at the Georgetown Transfer Station and observed a large mound of paper which, upon closer inspection, he determined were medical records, according to a statement from Coakley.
Health Breach Tally Tops 500 Milestone
But Do the Stats Show Signs of Progress?

By Marianne Kolbasuk McGee, October 23, 2012. ⭐ Credit Eligible

Major U.S. healthcare data breaches have surpassed a significant milestone: More than 500 breaches have been confirmed since September 2009, when the U.S. Department of Health and Human Services began keeping tabs.

Those incidents, each affecting 500 or more individuals, have impacted a combined total of 21.2 million individuals.

Hitting the 500-breach milestone is a signal that "healthcare continues to lag in its commitment to resources for privacy and security programs," says Mac McMillan, CEO of CynergisTek, a data security and privacy consulting firm. Until organizations pay more attention to breach prevention, "we're going to continue to see these kinds of results," he says.
Here are the 10 largest data breaches in history. So far....

- Heartland Payment Systems, 2008-2009: 130 million records compromised
- Target Stores, 2013: 110 million records compromised
- Sony online entertainment services, 2011: 102 million records compromised
- National Archive and Records Administration, 2008: 76 million records compromised
- Epsilon, 2011: 60 million to 250 million records compromised
- Evernote, 2013: More than 50 million records compromised
- Living Social, 2013: More than 50 million records compromised
- TJX Companies Inc., 2006-2007: 46 million records compromised
- Adobe Systems, 2013: At least 41 million records compromised
- Card Systems Solutions, 2005: More than 40 million records compromised
Small Pharmacy fined

Small Pharmacy gets $125,000 HIPAA Fine for Willful Neglect

HIPAA HITECH Compliance News

Posted May 27, 2015 by Jack Anderson, CEO, Compliance Helper

No HIPAA risk assessment, no HIPAA written policies and procedures, and no HIPAA training equals “willful neglect” and earned a $125,000 HIPAA fine for a Colorado compounding pharmacy.

The investigation revealed that they had completely ignored HIPAA regulations thus triggering the “willful neglect” designation. This can be punished by up to $1.5 million per incident per year so while $125,000 was a lot for a small pharmacy it could have been a lot worse. In fact it actually is worse than the $125,000 because studies have shown that over 60% of patients will leave a healthcare organization that has a breach.

If this pharmacy had been a client of Compliance Helper and ACR2 Solutions they would have had the Cycle of Compliance in place which would have provided them with a HIPAA risk assessment meeting the NIST standards, written policies and procedures tailored to their organization, access to a HIPAA expert, and on-going training and awareness for their staff based on their policies and procedures. The cost would have been around $200 per month. You do the math.
HIPAA Audits

HIPAA Audits: A Preliminary Analysis

Security a Bigger Challenge Than Privacy

By Marianne Kolbasuk McGee, June 20, 2012. Credit Eligible

The initial 20 HIPAA compliance audits found that more organizations had trouble with security compliance than privacy compliance, and smaller organizations had more difficulties than larger ones, a preliminary analysis by federal officials shows.

Many of the audited organizations hadn't been conducting regular risk assessments, says Linda Sanches, a federal official involved in supervising the audits. For some of the organizations audited, "HIPAA hasn't been a priority for several years. ... Risk assessments were done six years ago and haven't been looked at since," she says.
Anthem Blue Cross Fined in Breach Case
State Settlement Also Requires Process Changes

By Marianne Kolbasuk McGee, October 2, 2012.

California Attorney General Kamala Harris has entered into a settlement with Anthem Blue Cross in a data breach case involving the insurer mailing almost 34,000 letters printed with the Social Security numbers of certain members viewable through the envelopes' windows.

Under the terms of the settlement recently filed in Superior Court of California, County of Los Angeles, Anthem Blue Cross, also known as California Blue Cross, agreed to pay a $150,000 penalty. That payment by one of California's largest insurers includes $40,000 that's being placed in a state Unfair Competition Law Fund and $110,000 for legal and investigative costs related to the case.

The privacy breach case involved a marketing letter Anthem Blue Cross sent in April 2011 to more than 31,000 Medicare supplemental coverage members and more than 2,600 payment collection letters to Medicare Part D members mailed between December 2011 and March 2012.

RELATED CONTENT
- Accretive Health Responds to Lawsuit
- Cancer Center Reports 2nd Data Breach
OCR fines

OCR Fines Phoenix Cardiac Practice for HIPAA Privacy/Security Violations

Phoenix Cardiac Surgery, P.C, with offices in Phoenix and Prescott, Ariz., will pay a $100,000 fine and implement a corrective action plan under a resolution agreement with the HHS Office for Civil Rights following HIPAA privacy and security rule violations.

OCR began an investigation after learning that the physician practice was posting clinical and surgical appointments on an Internet-based calendar that was publicly accessible, according to an April 17 announcement from the agency. The investigation found that the practice had few policies and procedures to comply with the privacy and security rules.
A Strong Incentive for Risk Assessments
Recent Fines Demonstrate Feds Enforcing HIPAA Requirements


The lack of a current, thorough risk assessment can prove to be very costly, recent action by federal regulators illustrates.

Authorities have issued penalties in excess of $1 million to two organizations that were investigated following relatively small breaches and found to be lacking a current risk assessment as required under HIPAA. The resolution agreements in each case also pointed out other alleged HIPAA compliance shortcomings. But the lack of risk assessments that could have identified factors leading to the breaches seemed to be key in the regulator's decisions to levy hefty penalties.

_These cases show that risk assessment continues to be a priority for the Department of Health and Human Services._
Criminal Attacks: The New Leading Cause of Data Breach in Healthcare

May 7, 2015, 9:00 am

The Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, sponsored by ID Experts, shows that, for the first time, criminal attacks are the number-one root cause of healthcare data breaches. We calculated a 125 percent growth in these attacks over the last five years—a huge net change in any study. Employee negligence and lost or stolen devices still result in many data breaches, according to the findings. However, one of the trends we are seeing is a shift of data breaches—from accidental to intentional—as criminals are increasingly targeting and exploiting healthcare data. Cyber criminals recognize two critical facts about the healthcare industry: 1) healthcare organizations manage a treasure trove of financially lucrative personal information and 2) they do not have the resources, processes, and technologies to prevent and detect attacks and adequately protect healthcare data.

This year, we expanded the study beyond healthcare organizations to include business associates. This provides a broader and more holistic view of the healthcare industry and shows the impact third parties have on the privacy and security of healthcare data. With sensitive information flowing and new threats emerging daily, healthcare organizations and their business associates are at great risk for data breach. In fact, 91 percent of healthcare organizations and 59 percent of business associates experienced a data breach.
What Should we be doing?
What should Our Organization be doing?  
At minimum you should be...

- Do a Risk Assessment
- Document existing Policies and Procedures that are in use
- Train your employees on Privacy and Security concepts and HIPAA specifically
- Document Document. If it’s not written down, it doesn’t count in HIPAA or any other compliance.
- Assign a Privacy and Security Compliance Officer and start building a team
- Build a Culture of Security and Compliance
- Look into Cyber Security Insurance
- Build a budget or a plan for ongoing on next year compliance
Summary of Key Points

1. You may be both a CE and/or a BA!
2. HIPAA is **Not an Option**
3. Big $$ Fines and Enforcement is **Here No**
4. Doing a compliant Risk Assessment helps to significantly limit your liability if you start remediating the found deficiencies
5. Using outsourced services such as BA’s and EHR Vendors do not make you HIPAA compliant
6. Your Business Associate’s Need to be compliant
7. Deadline for BA Compliance was Sept 23, 2014
Guide to Privacy and Security of Health Information

Remember that there’s now real liability Up to $1.5 million per identical violations!

Thank you!

Contact: Jack Kolk
707.742.4211
Jack.K@acr2solutions.com