What Changes, Stays the Same, New Focus, Same Problems in HIPAA Compliance

Jo Ellen Whitney
Davis Brown Law Firm

DISCLAIMER

Due to limitations and the nature of this program please understand that printed material and oral presentations or other data presented are not intended to be a definitive analysis of the subjects discussed. Users are cautioned that situations involving healthcare and employment law questions are unique to each individual circumstance, and the facts of each situation will dictate a different set of considerations and varying results. Material contained on this site or listed as a reference is a general review of the issues, and must not be considered as a substitute for advice from your attorney on your own independent situations.

Jo Ellen Whitney, JD

I am a Senior Partner at the Davis Brown Law Firm, I work in:

- Employment & Labor Relations
- Health Law
- Privacy & Security (HIPAA)
- My contact information is:

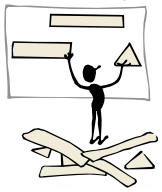
Davis Brown Law Firm
215 10th Street, Ste. 1300
Des Moines, IA 50309
515-246-7993
JoEllenWhitney@davisbrownlaw.com

REGZILLA

HIPAA/HITECH Omnibus Rule was issued on January 25, 2013.

CHANGES

There are a number of significant changes to the Rule which can be broken down in various ways:



NEW KEY LEGAL TERMS

- MENS REA-State of mind, what did you know, what was your intent, what were you thinking?
- CONSTRUCTIVE KNOWLEDGE-Did you know or should you have known that something was a breach?

NOTE: each of these terms places a significant emphasis on being aware of what it going on in your facility and heading off problems before they become significant issues.

Also note, reasonable cause, reasonable diligence and willful neglect, See 160.404.

SECTION 160.102

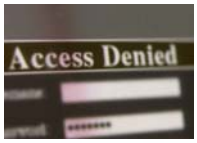
Makes HIPAA provisions, particularly security and reporting provisions, applicable to Business Associates.

YOU SAY TOMATO, I SAY TOMHATO

- Who exactly is a Business Associate?
  - A Business Associate is a person or entity who performs work on behalf of the covered entity and is not a member of its workforce. Such work or services must involve the use or disclosure of PHI.

DON'T FORGET

- Non BA may have access to information. Contracts with non BA should also specify security protocols and indemnification.
- You must minimize the non BA's ability to access such data.



FILING COMPLAINTS

These regulations also allow patients and others affected by HITECH/HIPAA issues to file a complaint directly with the secretary of HHS or State AG regarding a CE, Business Associate or Subcontractor. This includes complaints of retaliation.

BREACH

Major changes have occurred in how a breach is identified. The prior rule states that a breach occurred when there was reputational or other specific harm including potential identity theft.

GUILTY UNTIL PROVEN INNOCENT - BURDEN OF PROOF

The burden of proof has shifted from showing that something such as identify theft was not likely to a heavier burden of proof on the entity to show that the information was not in fact compromised.

NEW STANDARD

Breach now means an assessment of

1) The nature and extent of the PHI involved, including identifiers and likelihood of re-identification;
2) Who may have had access to the PHI or to whom disclosure was made;
3) Was the PHI actually acquired or viewed; and
4) To what extent has the risk of disclosure been mitigated.

4 BASIC TIERS

- DID NOT KNOW: $100-$50,000 excess 1.5 Million.
- REASONABLE CAUSE: $1,000-$50,000 excess 1.5 Million.
- WILLFUL NEGLECT with 30 day correction: $10,000 - $50,000 excess 1.5 Million.
- UNCORRECTED WILLFUL NEGLECT: Maximum $50,000/1.5 Million

SECTION 160.406

IDENTICAL REQUIREMENT

This section specifically states that a separate violation occurs each day, the covered entity or BA is in violation of the provision but will also take into consideration actions taken to mitigate damage and assess cure.

PRIMARY FACTORS RELATING TO DETERMINATION OF PENALTY

1) NATURE OF THE VIOLATION
   a) The number of individuals affected;
   b) The time period during which the violation occurred;

2) NATURE AND EXTENT OF HARM RESULTING FROM THE VIOLATION
   a) Whether the violation caused physical harm;
   b) Whether the violation resulted in financial harm (i.e. loss of job, etc.);
   c) Whether the violation resulted in the harm to the individual's reputation (you live in a small town, what do you think?);
   d) Whether the violation hindered an individual's ability to obtain healthcare (did you blacklist them?).

3) HISTORY OF PRIOR COMPLIANCE
   a) Previous non-compliance;
   b) Have you attempted to take corrective action;
   c) Have you responded to technical assistance from the secretary;
   d) Have you responded to prior complaints.

FINANCIAL CONDITION

1) FINANCIAL CONDITION OF THE ENTITY OR BA;
   a) Do financial problems affect the ability to comply?
   b) Would a civil monetary penalty jeopardize the ability to continue to provide healthcare?
   c) The size of the entity.

ANYTHING ELSE?

- Anything else they think they made need to take into consideration?

"As Justice may require!"

AFFIRMATIVE DEFENSES

1. You already fined me for that, you can't fine me again! (Section 160.410 (a))

Section 160.410 (b)

1) NOT DUE TO WILLFUL NEGLECT
   a) Corrected in the 30 day period where you knew or would have known of the penalty;
   b) Corrected as within a time frame deemed by the secretary.

-

THE HURRICANE EXCEPTION

IN CASE OF AN EMERGENCY IF CONSISTENT WITH PRIOR EXPRESSED PREFERENCE OF THE INDIVIDUAL AND IN THE INDIVIDUAL'S BEST INTEREST.

DIFFICULT ISSUES

- Patient reports to ER and it is determined that she injected miscellaneous drugs into her own IV. She had brought these drugs with her. She had been observed doing this at least once before. She is employed by the hospital as a nurse.

QUESTIONS

1) Patient/doctor confidentiality
2) HIPAA
3) State Law

FLIP SIDE

1) Harm to self or others
2) Drug diversion
3) Ethical obligations to report license holder

CALIFORNIA CASE

- Drug abusing physician was reported to Licensing Board.
- He filed a HIPAA complaint.
- Determination that this fell under the HIPAA health care operations exception.

Since April 2003 OCR Has:

- Received more than 127,184 HIPAA Complaints
- Initiated more than 860 Compliance reviews
- Resolved 121,367 cases
- 33 Resolution Agreements with money penalties
- 4 such agreements already in 2016

Most Frequent Issues:

- Impermissible use and disclosure
- Lack of safeguards
- Lack of patient access
- Lack of administrative safeguards
- Violation of minimum necessary standards

Who?

- Private practices
- General hospitals
- Outpatient Facilities
- Pharmacies
- Health plans

Most Breached Data in U.S.

1. Retail
2. Banking
3. Medical

Since I Saw You Last

- 10 Corrective Action Plans/Fines
- $11,902,200 in Fines

Cornell Pharmacy
March 12, 2015

$125,000

Single location pharmacy in Denver

1,610 Patient Records in the dumpster as reported by a local news team

- No policies
- No training

St. Elizabeth's Medical Center
July 2015

$218,400

- 2012 Complaint regarding Massachusetts Hospital Staff using internet based document sharing App with no data safeguards.
- Failed to respond or mitigate the issue when discovered.
- February 2013 HHS Notification of issues.
- 2014 Use of personal laptop/flashdrive (breach).

Cancer Care Group
August 2015

$750,000

Laptop bag stolen from employee's car in 2012

-unencrypted backup media

-55,000 patients

- No risk analysis
- No policy on removal of media from the premises

Lahey Hospital & Medical Center

$850,000

Massachusetts Hospital where laptop was stolen from unlocked treatment room.

599 patients from radiology compromised.

- No risk analysis
- No physical safeguards
- Lack of unique user names

University of Washington Medicine
December 2015

$750,000

Download of malware through email attachment

- 90,000 patients

Affiliated entity issue "failure to provide accountability and oversight to all portions of the enterprise"

Triple S
November 2015

$3,500,000 (3.5 Million)

Insurance holding company in San Juan

"wide spread non-compliance"

Triple S
November 2015

- Failure to meet minimum necessary guidelines
- No BAA with some vendors
- Failure to have risk analysis
- Access by a former employee

Lincare, Inc.
February 2016

$239,800

- Not a CAP-an ALJ determination
- Lincare has 850 branches in 48 states
- Employee left behind 278 hard copy patient records when she moved
- Took no action to correct issues during pendancy of investigation

Complete P.T. Pool & Land Physical Therapy
March 2016

$25,000

Patient testimonials without appropriate permission

North Memorial Health Care of Minnesota
March 2016

$1,550,000 (1.55 Million)

- No BAA with Major Contractor
- No Organization Wide Risk Analysis

WHAT?

- Unencrypted laptop stolen from BA employee's vehicle – 9,497 patients compromised.

- Accretive Health Inc. had full access to database and paper records with no BAA in place

Feinstein Institute for Medial Research March 2016

$3,900,000 (3.9 Million)

Non-profit Biomedical Research Group in New York

Laptop stolen from employee's car

- 13,000 subjects
  - No policies/procedures
  - Didn't restrict unauthorized users

Why So Much?

- Undermined individuals' trust in the research process

Do We Have a Theme?

- YES-Failure to take the basics seriously and OCR is losing patience.

WHAT?

- Failure to do risk analysis (10)
- Failure to train (10)
- Stolen laptop (5)
- Abandoned paper documents (2)
- BAA Issues (3)

University of Iowa

- Clinic employee termed for discussing "popular athlete's" girlfriend's medical testing.

University of Virginia Medical Center vs. Susan Jordan

Jordan had consent from her husband to access his records and did so 4 times without using the appropriate process.

- She was terminated.
- Court stated it was a wrongful termination as the law did not require an "orderly release" of records limited to Virginia public employee law.

Felice v. Vandevveen (Michigan)

- Cathy Felice consistently demanded a verbal consent when a dental patient was accompanied by another person. She was told this was unnecessary but continued to do so.
- She was terminated.
- The Court said she was not fired in retaliation as the office policies were compliant with HIPAA.

Can't Rely on Assertions by BA

- FTC Settlement with Henry Schein Practice Solutions, Inc. (dental software) for $250,000 for false advertisement about level of encryption for patient data. Security did not meet industry standard encryption algorithms.

100 Million Paid by Lifelock

- FTC contempt charges that they violated a 2010 Court Order regarding protection of customers' data. Deceptive advertising was also at issue.

What Was At Issue?

- No comprehensive security program
- Advertised that data was protected in the same manner banks protect data
- Claimed would send alerts "as soon as" it received any data consumer may be a victim
- Failed to abide by 2010 Court Order relating to record keeping requirements

Where Conflicts Collide?

- 2010 Law – Drug companies must report payments to physicians for promotion
- On-line issues are new

Will a Disclaimer Fit in 140 Characters?

- Who to advise
- How to advise
- Screen shot of disclaimer/disclosure
- Massachusetts Medical Society requires online disclosure

*Statnews.com 2/29/2016

What About that Cool App?

- Integrated App (App + EMR)
- Is the App Developer a BA?

PHI/HIPAA/OCR and Apps

- Patient downloads personal app for use
  - No
- Direct to consumer app – Doc suggest app to track diet then the app sends a summary to the Doc.
  - No-as the consumer initiates (less clear cut)

PHI/HIPAA/OCR and Apps

- Doc contracts with App developer and patients use app per doc request, direct to EHR
  - Yes
- 2 data streams, one CE driven, one consumer driven
  - Must keep data separate, CE driven section requires a BAA

Telemedicine

- IAC 653-13.11
- Adopted April 13, 2015
- Effective June 3, 2015

Patient Relationship

1) Patient seeks assistance from licensee
2) Licensee agrees to undertake diagnosis and treatment
3) Patient agrees to be treated

What About Expanding Technology?

- Facebook
- Twitter
- Answering blog questions

November 2015-OIG says OCR is doing a Bad Job – Report 1

Need to:

- Follow up on patient and OCR notice of breaches
- Enter all breaches in the searchable database
- Track prior breaches

Report 2

- Failed to be pro-active, simply reactive
- Scolded for not rolling out the regular audits
- 26% of cases had incomplete documentation
- 29% of staff said didn't check for "pattern" of abuse

The Audits are Coming! Oh they are here!

March 21, 2016 Phase II of Audits

2016 Phase II

- Primarily desk audits
- Policies, procedures, practices
- HHS.gov

Right to Access

- The Designated Record Set
  - Medical records
  - Billing records
  - Enrollment, payment, claims, management systems
  - Records used to make decisions about individuals

No Right to Access

- Quality assessment
- Peer review
- Patient safety activity
- Business planning
- Psychotherapy notes
- Records prepared in anticipation of litigation

Verification of Identity

- Same process required
- Orally or in writing
- Good faith

NOT OK

- Require patients to "pick up" records
- Only use web portal
- Only accept mailed access requests (Delay)

What About Arguments Among Family?

- Parents of child/patient
- Family in general
- 3rd parties

Fees

- Reasonable cost based fee
  1) Labor for copying
  2) Supplies (paper, cd)
  3) Postage

May Not Include Costs For

- Documentation, verification, search, systems, etc.
- Portal access is <u>free</u>
- OCR wants cheap or free access ($6.50 or free)

Workers' Compensation

- A medical provider or its agent shall furnish an employer or insurance carrier copies of the initial, as well as final clinical assessment, without cost when the assessments are requested as supporting documentation to determine liability for payment of a medical provider's bill for medical services.

Workers' Compensation

When requested, a medical provider or its agent shall furnish a legible duplicate of additional records or reports. Except as otherwise provided in this rule, the amount to be paid for furnishing duplicates of records or reports shall be the actual expense to prepare duplicates not to exceed: $20 for 1-20 pages; $20 plus $1 per page for 21-30 pages; $30 plus $.50 per page for 31-100 pages; $65 plus $.25 per pages for 101-200 pages; $90 plus $.10 per page for more than 200 pages, and the actual expense of postage. No other expenses shall be allowed.

You may not Require a Reason for Requesting Access

MYOB!!

Timelines for Production

- 30 days (outer limit)
- 1 extension 30 days (written notice within 30 days)
- Review of denial "reasonable period of time"

Can I Refuse Because You Haven't Paid the Bill?

NO

HIPAA 45 CFR 164.524(C)(4)

IBM Ethical Rules

Who Pays?

- Cyber Security breach can be expensive
  - Investigation costs
  - Statutes require notifications to government entities and affected consumers
  - Costs of credit monitoring services
  - Potential system damage or business interruption
  - Litigation – civil lawsuits, regulatory matters

Unsettled Area

- Case law unsettled: conflicting court decisions regarding whether system damage considered "physical loss or damage" under commercial property policies
  - Ward General Ins. Services, Inc. v. Employers Fire Ins.
    - loss of electronically stored data after a computer crash resulting in lost productivity and profits was not a physical loss
  - American Guaranty & Liability Ins. Co. v. Ingram Micro
    - loss of access to computer system after power outage destroyed ESI constituted physical damage

Recall Total Info Mgmt. v. Fed. Ins. May 2015

- Subcontractor transporting data tapes with info for 500,000 past and present IBM employees, tapes fell out of van, never recovered

- CGL and umbrella insurers denied Recall coverage in settlement with IBM for costs of responding to loss
- No duty to defend or indemnify
- No "personal injury"
- Lack of "publication"

Travelers v. Portal Healthcare August 2014

- Hospital contracted with Portal to store electronic medical records. Portal subcontracted to host on an electronic server.
  - Patients discovered they could find a direct link to their medical records through Google search of their names
- Question regarding duty to defend class action
- Fell within CGL personal injury coverage due to "publication"

Cottage Health May 2015

- Cyber Insurance at issue
- Cottage Health sought defense costs and $4.125 million settlement reached in class action lawsuit alleging 30,000 patients' records were disclosed after being stored on internet-accessible system without encryption.
- Insurer denied coverage and invoked exclusion for failure to implement risk controls identified in application.

Travelers v. Federal Recovery Services May 2015

- Insurer filed declaratory judgment regarding duty to defend lawsuit against FRS
- Underlying lawsuit against insured alleged:
  - FRS handled electronic data for Global Fitness
  - After Global Fitness sold business, FRS refused to return electronic data without additional payment
- Court held no duty to defend under E&O policy due to intentional tort

Cyber Insurance Considerations

- Consider need for specific cyber insurance
- Read policies and exclusions – wide variety due to rapid evolution of the arena
- Be honest in security assessment
- Consider effect for directors and officers - recent lawsuits have named directors and officers individually

How Do You Reduce Your Cyber Security Risk?

- Establish security policy, designed to:

#1	• Prevent
#2	• Detect
#3	• Respond

Thank you

Jo Ellen Whitney
JoEllenWhitney@davisbrownlaw.com
Davis Brown Law Firm