OCR…
WHERE IS IT GOING NOW?

Jo Ellen Whitney

JoEllenWhitney@davisbrownlaw.com

Davis Brown Law Firm

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.

DAVIS BROWN LAW FIRM

Jo Ellen Whitney, JD

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

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

Davis Brown Law Firm

215 10th Street, Ste. 1300

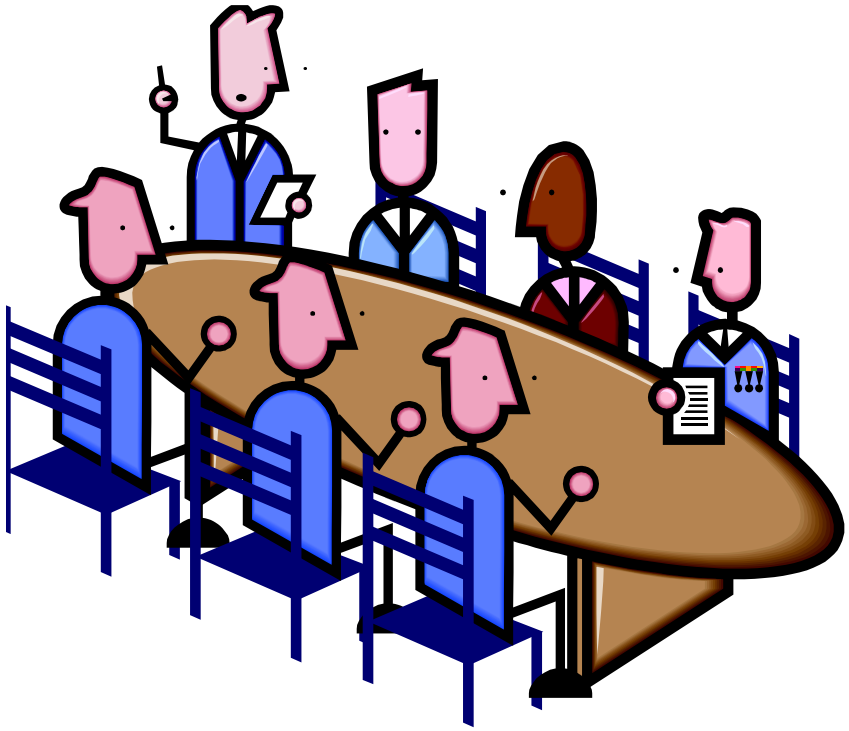
Des Moines, IA 50309

515-246-7993

JoEllenWhitney@davisbrownlaw.com

THE MORE THINGS CHANGE….

- The biggest issue is still people



PEOPLE JUST DO STUFF

- February 6, 2014 - US Attorney Eastern District Texas, announced CFO for Shelby Regional Medical Center in Texas has been indicted for defrauding the government of over $800,000 via false attestations regarding meaningful use to CMS.
- Possible Penalty 7 years prison and $500,000 fine.

NOT TECHNOLOGY - PEOPLE

- *Failure to put security patches in place*
- *Work around safeguards*
- *Share passwords*
- *3rd party sharing (dropbox, google)*
- *Don't think about the big picture*

DAVIS BROWN LAW FIRM

RESIDENTS SHARE RESULTS

- Google shared files for patient treatment and outcomes but . . . . . Before Google agreed to sign BA agreements AND the passwords never changed. (Utah)

IDAHO STATE

- $400,000 fine when Idaho State self reported that 17,500 patient records were accidentally unsecured for at least 10 months. After maintenance they forgot to put the firewall back up.

SKAGIT COUNTY WASHINGTON

- $215,000 PENALTY
- Money receipts relating to seven individuals were accessed when the ePHI was accidentally moved to a public access server. Total possible compromise -1,581 records.

SKAGIT . . .

- "OCR's investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security, and Breach Notification Rules."

SKAGIT RESOLUTION

1) Provide breach notice via major print or broadcast media or posted on homepage, a toll free hotline must be provided for 90 days.
2) Submit to HHS for review within 60 days its hybrid entity documents.
3) Conduct an accurate and thorough security review.
4) Create and update policies & procedures.
5) Training (may not access ePHI unless trained).

In Case We Were Feeling Smug

- March 7, 2014 the Register reported that "Inappropriate practices by two state workers led to a security breach including personal information about 2,042 people in Polk County….."

Polk County/DHS

- Involved people being assessed in child or dependent adult abuse cases
- Inappropriate use of personal email accounts, online storage accounts, and personal electronic devices
- Data included Social Security #s and PHI

ONC LAUNCHES NEW TOOL

SECURITY RISK ASSESSMENT

www.healthit.gov/providers-professionals/security-risk-assessment

OCR BY THE NUMBERS

- Investigated in excess of 22,222 cases where some action was required.
- 10,005 investigated found no violation.
- 54,944 cases weren't HIPAA
  - Not a CE or prior to HIPAA
  - Untimely or withdrawn
  - Activity does not violate HIPAA (such as reporting vaccinations)

MOST COMMON TYPE COMPLAINT

- Impermissible use and disclosure
- Lack of safeguards
- Lack of patient access
- More than minimum necessary information released
- Lack of administrative safeguards

ENTITIES
(In Order of Frequency)

- Private Practice
- General Hospital
- Outpatient
- Health Plans
- Pharmacies

OIG December 2013 Audit

- Audit logs should always be operational
- CMS and ONC should use collaborative efforts to address fraud vulnerability
- CMS should develop guidance on the use of copy and paste functions

AUDIT PROGRAM
(Sue McAndrew OCR Deputy Director)

- 115 CE Audited and Pilot Program Completed

PILOT PROGRAM REVELATIONS IN PRIVACY

- Failure to provide accurate NPP
- Failure to grant individual access
- Compliance with minimum necessary
- Failure to obtain authorizations

PILOT PROGRAM REVELATIONS IN SECURITY

- Risk Analysis

- Media Storage / Disposal

- Audit Controls

- General Monitoring (Idaho State)

NOT JUST COMPUTERS

- 22% of all OCR Complaints are about paper records and “fundamental principles”

The Audit Plans Announced

- 350 CE's (Fall 2014)
- 50 BA's (2015)

Who Will Do

- KPMG did the pilot audits.
- These will be done by OCR Staff.
- Desk audits with a more limited number of comprehensive audits.

PROTOCOL

- OCR will make an updated protocol available “soon” on its website.

Target Areas

- Risk Analysis
- Proper NPP
- Patient Access to Data
- Storage Media Controls
- Transmission Security
- Work Force Training

Audit

- Data Map
- Inventory
- Privacy Assessment/Audit
- Security Assessment/Audit
- Training/Agreement
- Plan/Policies
- Follow-up

DAVIS BROWN LAW FIRM

Coming Soon

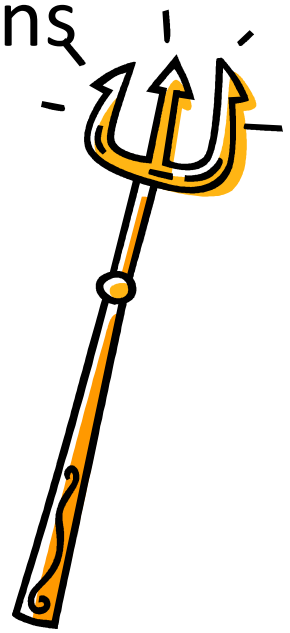
- 2016 – Encryption
- Minimum Necessary

  "A covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

  45 CFR 164.502(b)(i)

THE DEVIL IS IN THE DETAILS

- Must identify who needs access to such information to carry out their duties
- What categories of information each group can access and any conditions relating to such access
- Must make reasonable efforts to limit access



FOR DISCLOSURES

- Limit to amount reasonably necessary to achieve purpose
- For routine matters-apply standard policy
- For non-routine assess criteria on an individualized basis
- Create some double check system for non-routine matters

CE to CE

Greater latitude in what is disclosed

Reasonable reliance standard

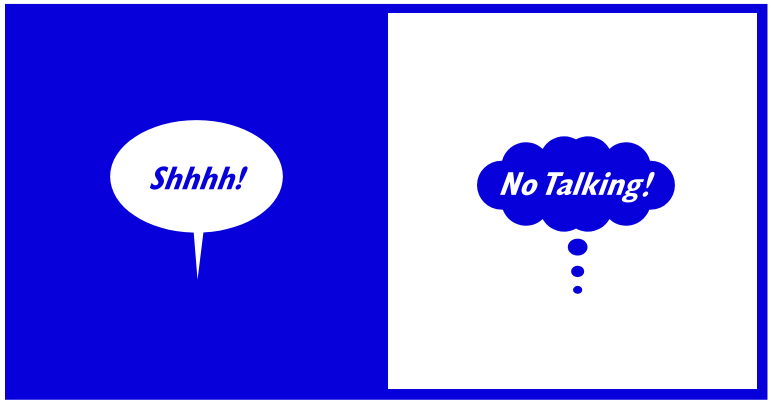
Does All of This Apply to BA's?

- Yes, as the rule is currently written, they must also comply with the CE's standards (privacy, security, and minimum necessary).

IS IT A BREACH?

- OCR/HHS says

  " . . . Uses or disclosures that impermissibly involve more than the minimum necessary information . . ., may qualify as breaches."



HOSPITAL TELEPHONE MESSAGE

Hospital employee left a telephone message on a patient's home number detailing diagnosis and treatment.

- Patient had asked for use of work number
- Too much information was left

DENTAL RED FLAG

Dental practice physically flagged files with a red sticker “AIDS” and other patients could see the files. All stickers moved to inside cover and the practice met with the effected patient to apologize.

Thank you

Jo Ellen Whitney

JoEllenWhitney@davisbrownlaw.com

Davis Brown Law Firm