Jackson Walker LLP

SILHOL LAW
The law of health business

Jeffery P. Drummond

Jamie Sorley

# Lawyers as HIPAA Business Associates:

Ethical Obligations and Practical Tips for Compliance

Dallas Bar Association
January 17, 2018

## Agenda

- An Overview of HIPAA
  - The Privacy Rule
  - The Security Rule
  - The HITECH Act
  - The Omnibus Rule
- Lawyers as Business Associates
- Law Firm Compliance with BA Obligations
- Noncompliance Risks


# HIPAA Background and History

## Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Based on the Kennedy-Kassebaum bill
- Created to:
  - Assure health insurance portability
  - Reduce health care fraud and abuse
  - Increase electronic data interchange in the healthcare industry through standardization
  - Guarantee security and privacy of health information

## The Health Insurance Portability and Accountability Act of 1996 "HIPAA"

***"It's more than insurance portability and accountability…"***

| | |
|---|---|
| TITLE I<br>Health Insurance Access<br>Insurance Portability<br>Insurance Renewal | TITLE II<br>Fraud and Abuse Control Programs<br>Administrative Simplification<br>Medical Liability Reform |
| TITLE III<br>Medical Savings Accounts<br>Health Insurance Tax Deductions | TITLE IV<br>Enforcement of Group Health Plan Provisions |
| TITLE V<br>Revenue Offset Provisions | |

## "Administrative Simplification"

- Transaction and Code Sets
- Privacy
- Security

## A brief history of HIPAA

- 1996: HIPAA statute passes
- 2000/2001: Privacy Rule published
- 2003: Privacy Rule enforceable, Security Rule published
- 2005: Security Rule enforceable
- 2009: HITECH Act passes, initial regulations passed
- 2013: HITECH "omnibus rule"

## HITECH Act Expansion

- Under original HIPAA, only health plans, providers and clearinghouses are CEs
- HITECH (legislatively) expands HIPAA to directly apply to BAs
  - BAs are now liable for some Privacy Rule provisions
  - BAs are now liable for virtually all Security Rule provisions

## Protected Health Information (PHI)

- Any health information relating to -
  - Past, present or future physical or mental health or conditions;
  - Provision of health care; or
  - Past, present or future payment for health care
- Created/received by covered provider, plan, employer or clearinghouse (or by a BA on behalf of CE)
- Individually identifiable or presents reasonable basis to believe the information can be used to identify the individual
- In any medium
  - Written
  - Verbal
  - Electronic

## NOT PHI

- Education records (mostly covered by FERPA)
- Employment records (even if they contain medical information)
- Records relating to someone who has been dead for at least 50 years
- Records entirely unrelated to a Covered Entity

# Lawyers as HIPAA Business Associates

## The Privacy Rule:

- An absolute prohibition with exceptions:
- "Thou shalt not": A CE or BA may not use or disclose protected health information, except:
  - For treatment, payment, or healthcare operations
  - With the individual's authorization or to the individual
  - As otherwise required by law or otherwise permitted or required under the privacy regulations

## Privacy Rule Compliance

- Abide by the BAA
- Enter Subcontractor BAAs with any subcontractors
- Abide by HITECH privacy requirements
  - Minimum necessary
  - Data breach rules
- Restrict uses and disclosures of PHI
- Control access to PHI

## Law Firm BAAs


- Lawyers as Business Associates must enter into BAAs with their Covered Entity clients and with firm's subcontractors
- Be aware of the ethical obligations that arise when you negotiate an agreement with your own client
- Clients have their form BAAs; don't use them.
  - Why? Lawyers are not like other vendors

## Law Firm BAAs

- "Secretary of HHS' Access to Books and Records" provision of BAA (required by Privacy Rule) could constitute a waiver of attorney-client privilege
  - Other vendors don't have privileged communications
- Indemnification provisions may void lawyers' malpractice insurance
  - Other vendors don't carry malpractice insurance

## Subcontractor BAAs

- If your vendors/contractors create, receive, maintain or transmit your client's PHI, you must downstream the BAA obligations your client put on you onto your vendors
- Does the vendor work for the law firm (is a subcontractor BA) or for the client (is a BA)?
- Make sure there are no gaps between the subcontractor BAA and the BAA

## The Security Rule

- Technically, the Security Rule only covers "electronic PHI:"
  - Electronic data is at greater risk
  - Easier to steal, undetected, from far away
  - Easier to search, use, and sell
- However, keep in mind that the Privacy Rule has a safeguarding requirement, so keep your paper records safe too.

## Security Rule Compliance

- Policies and procedures (45 C.F.R. § 164.3xx)
  - Administrative (§ 164.308)
  - Physical (§ 164.310)
  - Technical (§ 164.312)


- Must do a Risk Analysis to determine what policies and procedures to adopt
- Encryption? Special Record-keeping? Minimum Necessary? Audit/restrict access?

## Addressable vs Required

- CEs and BAs must adopt administrative, physical, and technical safeguards to reasonably protect the confidentiality, integrity and availability of PHI
- Regulations are "technologically neutral"
- Regulations are divided into "required" and "addressable" categories.
  - Addressable does not mean optional

## Administrative Safeguards

- Assigned Security Responsibility
- Security Management Process
  - Risk Analysis**
  - Risk Management
  - Sanction Policy
  - Information System Activity Review
- Workforce Security
  - Authorization and Supervision
  - Workforce Clearance Procedure
  - Termination Procedure
- Information Access Management
  - Isolating Clearinghouse Function
  - Access Authorization
  - Access Establishment and Modification


## Administrative Safeguards (cont.)

- Security Awareness and Training
  - Security Reminders
  - Protection from Malicious Software
  - Log-in Monitoring
  - Password Management
- Security Incident Procedures
  - Response and Reporting
- Contingency Plan
  - Data Backup Plan
  - Disaster Recovery Plan
  - Testing and Revision Procedure
  - Applications and Criticality Analysis
- Evaluation
- Business Associate Contracts

## Physical Safeguards

- Facility Access Controls
  - Contingency Operations
  - Facility Security Plan
  - Maintenance Records
  - Access Control and Validation Procedures
- Workstation Use
- Workstation Security
- Device and Media Controls
  - Disposal
  - Media Re-use
  - Accountability
  - Data Backup and Storage

## Technical Safeguards

- Access control
  - Unique User Identification
  - Emergency Access Procedure
  - Automatic Logoff
  - Encryption and Decryption
- Audit controls
- Integrity
  - Mechanism to Authenticate E-PHI
- Person or Entity Authentication
- Transmission Security (encryption)

## Risk Analysis: the Precursor

- Neither a CE nor a BA can know what safeguards are reasonable without doing a risk analysis first
- Neither a CE nor a BA can know whether addressable safeguard standards should be adopted until a risk analysis has been done
- Risk analysis is the most common ultimate source of failure of HIPAA audits and enforcement actions

## Risk Analysis

- Systemic:
  What computer or information systems hold or transfer PHI?
  What databases are used?
  How? Who has access/control?
- Geographic:
  - Where is the data stored or transmitted? When? How? What issues are raised by location issues (different state law breach requirements)?
- Operational:
  - How does the entity store/transmit/deal with data? What protections are required?
- Personnel:
  - Who access data? Why? Special issues?
- Other:

## Risk Analysis

- Who should be involved in your Risk Analysis?
  - Size of the firm impacts the answer
  - Top tech person, Privacy Officer, lead internal counsel, operational staff in charge of files, etc.
- Consider outside consultants
- When should Risk Analysis be re-done?
  - Major change in technology
  - Major change in firm focus (new types of cases)
  - Turnover of tech administrators
  - Turnover of lawyers

## Training

- Who should be trained?
  - Anyone who touches PHI
  - Discovery (esp. document production)
- Who should train?
  - Privacy Officer or outside consultant
- When and how often?
  - HIPAA: within "reasonable time" upon hire
  - Texas Medical Records Privacy Act: within 90 days of hire
  - **Preferably before handling PHI**

## Documentation

- BAAs (upstream for your CE clients who don't know they need one with you) and Subcontractor BAAs (downstream)
- Policies and Procedures (documenting your Security Rule safeguards and Risk Analysis results)
- Training materials
- Client form documentation (NoPP, BAA, etc.)

## Breach Notification under HIPAA

- CE required to notify affected individual, HHS, and potentially the media of breach of unsecured PHI that compromises data
- BA is required to report to CE (under HIPAA and under the BAA) breaches of which it is aware
- BAA usually determines logistics of reporting, but CE usually makes the decisions

## Breach Notification under State Law

- Most states have data breach reporting laws (not limited to PHI, but includes PHI)
- CE usually has state law obligations in addition to direct HIPAA obligations
- BA usually has state law obligations in addition to indirect HIPAA obligations
- Possible conflicts between BAA requirements and state law requirements

## "Omnibus Rule" Provisions

- New Data Breach Rules
  - "harm" is out, "low probability of compromise" is in
- Business associates and subcontracting business associates
- Enforcement: Reasonable Cause and Willful Neglect
- Marketing/Fundraising/Sale of PHI
- Dead People
- Increased enforcement, penalties
  - State AGs can prosecute

## Breach Notification

- HITECH provisions of "Stimulus" Bill require notification in cases of breach
  - To the affected patient
  - To the media if the breach is big
  - To HHS
- "secured" (encrypted) data breach need not be reported
- "low probability of compromise" breach need not be reported
- State Law obligations as well

## Using HIPAA Protected Documents in Litigation

## Litigation Releases

45 C.F.R. § 164.512(e)

- Court Order
- Subpoena (be aware of who can issue one)
  - Notice to patient
  - Patient did not object and time passed
  - Patient objected but court allowed it
- Qualified Protective Order
- Disclosing covered entity attempts to notify patient or obtains protective order

## When the Litigation Ends . . .

- Destroy or Return when possible.
- Follow Qualified Protective Order if applicable.
- De-duplicate and eliminate extraneous copies.
- Don't keep data you don't need.

## Law Enforcement Disclosures

45 C.F.R. § 164.512(f)

- Court order or court warrant, subpoena or summons
- Grand jury subpoena
- Administrative request/investigative demand, with limitations
- To officer if requested to locate victim or subject, but limited to name, DOB, SSN, ABO blood type, type of injury, date/time of treatment/death, scars/tattoos/physical description (no DNA or dental records)

## Minimum Necessary Rule

- All uses and disclosures except for treatment or pursuant to specific authorization must be limited to "minimum necessary."
- Subpoena should be limited, and data gained should be used only within the minimum necessary restriction.

## State Data Breach Laws

- A law firm that is not a covered entity and not a business associate is not subject to HIPAA.
- However, it may be subject to similar state laws simply because it receives or uses PHI type data.

# Penalties for Violations

## Non-Compliance Risks

- Clients can be fined for HIPAA breaches caused (or not prevented) by their attorneys, even if the attorneys are not BAs of those clients (don't get PHI).
- Attorneys who are BAs can be fined for their own HIPAA breaches.
- Most HIPAA breaches by lawyers will be considered malpractice.

## HITECH Act Enforcement Concerns

- Increased penalties
  - Level of culpability drives penalty level
- State Attorneys General can prosecute HIPAA violations
- Injured individuals may get some of the fine money

## State Law Enforcement Concerns

- Clients can violate state laws because of failure of attorney to advise regarding state law
- Attorneys and law firms are often directly liable under state breach reporting laws

## Tips for Smart Attorneys

- Follow the Security Rule safeguards
  - Conduct a Risk Assessment
  - Adopt policies and procedures
  - Train Staff
  - BAAs with clients, SubBAAs with expert witnesses, vendors, etc.

## Tips for Smart Attorneys

- Document Communications
  - Know who contacts data when
  - Know who is responsible for data
    - Procuring
    - Storing
    - Returning
  - Look for odd activities

## Tips for Smart Attorneys

- Protect confidentiality of PHI
  - Consider when and how PHI is transferred
    - Encrypt data in motion where possible
    - Use portals or secure communications
    - Use safe faxing policies
  - Consider where and how PHI is stored
    - Encrypt data at rest
    - De-duplicate and delete
    - Safe storage and safe backups

## Tips for Smart Attorneys

- Protect confidentiality of PHI
  - Consider whether to print PHI records or rely on electronic storage
    - Do you need to keep paper records if you have electronic records (safely stored and backed up)?
  - Consider a high security document storage solution
    - Make sure you have a SubBAA in place if your clients are covered entities.

## Tips for Smart Attorneys

- Protect confidentiality of PHI
  - Follow the HIPAA Subpoena rules
  - Follow the minimum necessary rule
  - Use Qualified Protective Orders

## Other HIPAA Hot Spots

- Social Media
- Mobile devices
- Connection between MU and HIPAA
- Connections between HIEs and HIPAA
- Health Plan issues (providers or BAs – including law firms – with self-insured plans are twice covered entities)

## Resources

- OCR Guidance for Professionals
  - https://www.hhs.gov/hipaa/for-professionals/index.html
- Sample BAA
  - https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
- Security Risk Analysis Guidance
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es
- Breach Notification
  - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- Jeff's HIPAA Blog
  - https://hipaablog.blogspot.com/

# Questions?

**Jeffery P. Drummond**
Jackson Walker L.L.P.
2323 Ross Ave, Suite 600
Dallas, Texas 75201
jdrummond@jw.com
214.953.5781

**Jamie Sorley**
Silhol Law, PLLC
7557 Rambler Ave, Suite 1425
Dallas, Texas 75231
jamie.sorley@lawsilhol.com
214.245-0793