
Jeffery P. Drummond
Jackson Walker L.L.P.
901 Main Street, Suite 6000
Dallas, Texas 75202
(214) 953-5781
jdrummond@jw.com
www.hipaablog.blogspot.com

But first, a little history
(HIPAA’s baseline)

The Health Insurance Portability and Accountability Act of 1996
“HIPAA”
“It’s more than insurance portability and accountability…”

TITLE I
Health Insurance Access
Insurance Portability
Insurance Renewal

TITLE II
Fraud and Abuse Control Programs
Administrative Simplification
Medical Liability Reform

TITLE III
Medical Savings Accounts
Health Insurance Tax Deductions

TITLE IV
Enforcement of Group Health Plan
Provisions

TITLE V
Revenue Offset Provisions

“Administrative Simplification”
• Transaction and Code Sets
• Privacy
• Security

The HIPAA Privacy Rule
• Direct applicability to “Covered Entities”
  – Physicians, hospitals and other healthcare providers
  – Health insurance plans
  – “Healthcare clearinghouses”
• Indirect and direct applicability to “Business Associates” of CEs

The HIPAA Privacy Rule
• “Protected Health Information”
  – Individually Identifiable
  – Past, present or future
  – Condition, provision, or payment
• “Minimum Necessary”
  – Except for treatment, always required
  – Default definition: limited data set
Privacy Regulations in General Cover:
- Disclosure and use of protected health information (the "Rule")
- Individual rights regarding protected health information (the "Rights")
- Administrative Safeguards (the "Duties")

The HIPAA Privacy Rule
- Absolute prohibition with exceptions
  - For treatment, payment, or healthcare operations
  - To the individual
  - With permission of the individual
  - As required by law

Other Specific Use/Disclosure Issues
- Marketing and Fundraising
- Personal Representatives
- Hybrid Entities and Organized Health Care Arrangements
- Uses allowed without authorization: public health, HHS, law enforcement, military, prisoners
- State law preemption issues
- Psychotherapy notes have special rules

Privacy Standards: Business Associates
- Determine who your business associates are.
- Draft form business associate agreements.
- Look for Special Circumstances:
  - Accounting for disclosures.
  - Specific services.

Privacy Standards: Individual Rights
- Right to Notice of Privacy Practices
  - Describes individual’s rights to access, inspection, accounting
  - Duties of covered entity
  - Complaints and contacts
  - How covered entity will use and disclose their health information
- Information cannot be used or disclosed for any purpose not included on the Notice.
- Individual must be notified if information is used in a new fashion not covered by the old Notice

Privacy Standards: Individual Rights
- Right to Access own Information
- Right to Request Amendment
  - Accepting amendments
  - Denying amendments
  - Grounds for denial
- Right to Request Restrictions
  - Can refuse
    - If agree, are bound to it
- Right to Request Communications in alternative fashion
  - Correspondence sent to alternate address
  - Must accommodate reasonable requests
- Right to Receive an Accounting of Disclosures
  - Date and purpose
  - Recipient name
  - Description of information disclosed
  - Exceptions for treatment, payment and health care operations
  - Exception for disclosures pursuant to an Authorization
Administrative Requirements

- Appoint a privacy officer/security officer
- Adopt HIPAA policies and procedures (Security)
- Train your employees
- Document compliance and complaints
- Risk assessment (Security)

Documents and Forms

- Notice of Privacy Practices
- Consent (if you want one)
- Authorization (if you need one)
- Business Associate Agreement(s)
- Policies and Procedures

Security Rule

- Covered Entities must maintain administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of PHI in electronic format that they maintain or transmit.

Security Requirements

<table>
<thead>
<tr>
<th>Four Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Procedures</td>
</tr>
<tr>
<td>Physical Safeguards</td>
</tr>
<tr>
<td>Technical Security Services</td>
</tr>
<tr>
<td>Technical Security Mechanisms for Data Transmission over a Network</td>
</tr>
</tbody>
</table>

Administrative Requirements (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
  - Access Control and Validation Procedures
  - Maintenance Records
- Workstation Use
- Workstation Security
- Device and Media Controls
  - Disposal
  - Media Re-use
  - Accountability
  - Data Backup and Storage

**Technical Security Services Requirements**

- Access control
  - Unique User Identification
  - Emergency Access Procedures
  - Automatic Logoff
  - Encryption and Decryption
- Audit controls
- Integrity
  - Mechanism to Authenticate E-PHI
  - Person or Entity Authentication

**Technical Security Mechanisms**

- Guard Against unauthorized access to data that is transmitted over a communications network
- Communication/Network controls specifically include Integrity Controls and Encryption, but may also include:
  - Access controls
  - Alarms
  - Audit trails
  - Entity authentication
  - Event reporting
  - Message authentication

**Security Rule Requirements**

- Appoint Security Officer
- Conduct a Risk Analysis
  - Determine vulnerabilities, threats, and risks
  - Track the Security Rule requirements
- Policies and Procedures
  - Specifically for all Required requirements
  - Document all Addressable requirements

**So, What’s New?**

(HITECH and State Law changes)

**“HITECH Act” Provisions**

- New Data Breach Rules
  - “unsecured” PHI is the key
- Business associates are now treated like covered entities
- “Hide” rule
- Marketing/fundraising
- Accounting for disclosures if you use an EMR
- 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
- De-identified data breach need not be reported
- If breach meets subjective “no harm” standard, no need to report

The “Hide” rule:

- If the patient
  - Pays in full, out of pocket, for the service, and
  - Requests that the provider NOT disclose the information to the patient's insurer,
- The provider must comply, and not disclose the information, if the disclosure is for payment OR healthcare operations (you can disclose for treatment purposes)

Applicability to Business Associates

- Formerly, “business associates” were indirectly covered
- Covered entities still required to have “business associate agreements” in place to contractually bind business associates to HIPAA requirements
- Under HITECH, business associates directly subject to HIPAA privacy rules

New Enforcement Concerns

- Increased penalties
- State Attorneys General can prosecute HIPAA violations
  - OCR is now teaching state AGs how to pursue HIPAA cases
- Injured individuals may get some of the fine money

Penalties and Enforcement

<table>
<thead>
<tr>
<th>Degree of impact and action taken on patient</th>
<th>Minimum penalty</th>
<th>Maximum penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor impact only or embarrassment</td>
<td>No penalty</td>
<td>Maximum value</td>
</tr>
<tr>
<td>Moderate impact or patient inconvenience</td>
<td>Maximum value</td>
<td>Maximum value</td>
</tr>
<tr>
<td>Severe impact or severe patient inconvenience</td>
<td>Maximum value</td>
<td>Maximum value</td>
</tr>
<tr>
<td>Resultant information lost (unencrypted)</td>
<td>Maximum value</td>
<td>Maximum value</td>
</tr>
<tr>
<td>Resultant information lost (encrypted)</td>
<td>Maximum value</td>
<td>Maximum value</td>
</tr>
<tr>
<td>Resultant information lost (incident)</td>
<td>Maximum value</td>
<td>Maximum value</td>
</tr>
<tr>
<td>Resultant information lost (incident)</td>
<td>Maximum value</td>
<td>Maximum value</td>
</tr>
</tbody>
</table>

U.S. vs. Gibson (Seattle, Washington)
- Phlebotomist employee of Seattle Cancer Care Alliance found patient data in files and engaged in identity theft
- Acquired credit cards in the name of a cancer patient and charged purchases
- 16 month jail time, plus restitution

Enforcement Actions so far
Enforcement Actions so far

- **U.S. vs. Ramirez (south Texas)**
  - Receptionist for physician who provided physical exams for FBI agents offered to sell medical information on FBI agents to a man she thought was a drug dealer
  - The man was actually an FBI agent himself
  - 6 months jail time, 4 months home confinement, 2 years supervised release

- **U.S. vs. Machado; U.S. vs. Ferrer (south Florida)**
  - Cleveland Clinic employee accessed thousands of Medicare patient records and sent information to her cousin
  - Cousin and group of associates used the information to submit false bills to Medicare in the amount of $2.8 million
  - Machado pled for 3 years and $2 million in restitution; Ferrer found guilty for 7 years and $2 million in restitution

- **U.S. vs. Smith (Arkansas)**
  - Northeast Arkansas Clinic pediatric nurse viewed medical records of husband’s ex-wife, found out ex-wife was pregnant
  - Husband mentioned it during negotiations involving child support/custody proceeding
  - No jail time, but nurse lost her job and, as a convicted felon, her ability to serve in a pediatric role

“Snoopin” cases

- Britney Spears
- Farrah Fawcett
- Bill Clinton
- Anne Pressly (Little Rock news anchor)
- The Octomom
- Michael Jackson
- Gabrielle Giffords
- Blaine, Minnesota high school ravers

Recent Enforcement Actions

- **Data/Identity Theft cases**
  - Florida, Colorado, Alabama
  - Usually rogue employees
- Walgreens, CVS, Rite Aid
  - Dumpster-diving journalists
- HealthNet and Wellpoint
  - State AGs get into it

Recent Enforcement Actions (cont’d)

- Cignet Health: $4,300,000 fine
  - Crime: failure to cooperate
- Mass General: $1,000,000
  - Crime: super-sensitive data
- Many more to come
Texas Privacy Laws

- "Texas HIPAA" (Health & Safety Code § 181)
  - Originally drafted to mirror federal rule
  - Duplicative items removed
  - Mainly addresses use of PHI for marketing and fundraising
  - Broader definition of "Covered Entities"

- Texas Breach Notification Law (Business & Commerce Code § 521)
  - Not specific to healthcare
  - Computer system breaches
  - PHI is "sensitive personal information" by definition

House Bill 300

- Revised "Texas HIPAA"
  - "Covered Entities" must conduct training within 60 days of employment, and at least once every 2 years
  - Access to electronic records more quickly than required under HIPAA
  - Prohibition on sale of PHI (similar to HIPAA)
  - Increased penalties


Jeffery P. Drummond
Jackson Walker L.L.P.
901 Main Street, Suite 6000
Dallas, Texas 75202
(214) 963-5781
jdrummond@jw.com
www.hipaablog.blogspot.com