Paper delivered on September 30, 2016 in New Orleans, LA at the Proving Pain, Suffering and More in Personal Injury Litigation Seminar of the National Business Institute.

Ethical Management of Client Files

By: Franklin D. Beahm, Esq.
BEAHM & GREEN
145 Robert E. Lee Boulevard, Suite 408
New Orleans, LA 70124
frank@beahm.com

Whether you represent a hospital, an insurance company, or an individual personal injury victim, you need to be aware of the rules and regulations impacting the way you handle your clients' files and personal information. This presentation provides an overview of HIPAA regulations, HITECH's changes to HIPAA, and recent developments with HIPAA and same sex marriages and criminal background checks. The presentation concludes with an overview of the proper procedure for obtaining consent or authorization from an incapacitated individual.

The Health Insurance Portability and Accountability Act of 1996

Brief Timeline:

- August, 21, 1996: HIPAA passes Congress and was signed into law.
- August 21, 1999: Congress fails to pass health info privacy law.
- January, 2001: Absent Congressional action, DHHS was authorized to produce administrative regulations.
- April 14, 2001: DHHS finalizes its Privacy Rule with President Bush's approval.
- August 14, 2002: Bush administration modifies original Rule.
- April 14, 2003: The Rule becomes effective for most "covered entities" [or one year later for small health plans].
- April 14, 2004: The Rule is fully effective for all covered entities.
- 2009: HITECH Implemented
- 2013: Omnibus Rule revised some provisions and added new ones

- Added requirement to report breaches to patients
- Made Business Associates (including attorneys) directly liable under HIPAA
- Increased civil penalties
- Increased limits on fundraising and marketing

HIPAA's Structure: Privacy & *Security*

Privacy Rule: Provides standards for maintaining the privacy of identifiable health information: "A Covered Entity may not use or disclose an individual's protected health information, except as otherwise permitted or required by this subpart. .."

Security Rule: establish a national set of security standards for protecting certain health information that is held or transferred in electronic form.

Where do *Attorneys Fall within HIPAA Regulations*

Covered Entities (CEs):

- Health Plans;
- Health Care Clearinghouses;
- Health Providers that exchange identifiable health data electronically; and
- Business Associates
    - Claims or data processors
    - Billing companies
    - Quality assurance providers
    - Utilization reviewers
    - Lawyers
    - Accountants
    - Financial service providers

What Information is Protected

Protected Health Information: The Privacy Rule protects all "*individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

Examples:

- The individual's past, present or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual
- Name, address, birth dates, SSN

De-Identified Health Information: There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

There are two ways to de-identify information:

(1) a formal determination by a qualified statistician; or

(2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

HIPAA's Privacy Rule

General Principle for Uses and Disclosures

Required Disclosures: A covered entity must disclose protected health information to:

- Individuals (or their personal representatives) when they request their protected health information; and
- HHS during a compliance investigation or review or enforcement action.

Permitted Uses and Disclosures:

- Authorization (specific written authorization from individual);
- Treatment, Payment, and Health Care Operations;
- Opportunity to Agree or Object (e.g. facility directory of patients on premises);
- Incident to an otherwise permitted use and disclosure (Minimum Necessary Rule);
- Public Interest and Benefit Activities (e.g. child abuse, public health tracking, judicial proceedings); and
- Limited Data Set for the purposes of research, public health or health care operations (direct identifiers removed).
- Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

- **Minimum Necessary:** Limit uses and disclosures to the minimum necessary.

- **Access and Uses:** Restrict access and uses of protected health information based on the specific roles of the employees; Identify the persons who need access to protected health information to carry out their duties and limit access to the categories needed.

- **Privacy Policies and Procedures:** Develop and implement written privacy policies and procedures that are consistent with the Privacy Rule and flexible to adapt to the entity's size and resources.

- **Privacy Personnel:** Designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.

- **Workforce Training and Management:** Train employees on privacy policies and procedures; Develop and apply appropriate sanctions against those who violate the privacy policies and procedures

- **Mitigation:** Mitigate, to the extent practicable, any harmful effect caused by the use or disclosure of protected health information

- **Data Safeguards:** Maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information;

  - shred documents containing protected health information
  - secure medical records with lock and key or pass code
  - limit access to keys or pass codes.

- **Documentation and Record Retention:** Maintain privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions and activities until six years after the later of the date of their creation or last effective date.

HIPAA's Security Rule

Scope of Rule

Electronic Protected Health Information: The Security Rule applies to a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form.

General Rules

The Security Rule requires covered entities to maintain reasonable and appropriate **administrative, technical,** and **physical** safeguards for protecting e-PHI.

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and Y Ensure compliance by their workforce.

Factors to *consider when developing appropriate safeguards*

- The size, complexity, and capabilities of the entity;
- Technical, hardware, and software infrastructure;
- The costs of security measures; and
- The likelihood and possible impact of potential risks to e-PHI.

Administrative Safeguards: Perform risk analysis that includes, but is not limited to, the following activities:

- **E**valuate the likelihood and impact of potential risks to e-PHI;

- Implement appropriate security measures to address the risks identified in the risk analysis;

- Document the chosen security measures and, where required, the rationale for adopting those measures; and

- Maintain continuous, reasonable, and appropriate security protections.

Physical Safeguards: Limit physical access to its facilities while ensuring that authorized access is allowed.

- Have policies and procedures that specify proper use of and access to workstations and electronic media;

- Have policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media.

Technical Safeguards:

- Allow only authorized persons to access e-PHI;

- Implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI;

- Put in place electronic measures to confirm that e-PHI has not been improperly altered or destroyed;

- Guard against unauthorized access to e-PHI by using secured networks

HITECH ACT of 2009

(Health Information Technology for Economic and Clinical Health Act)

What does HITECH Do?

- Provides specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers;
    - Allows for provider to transmit protected information in electronic form upon proper authorization, doing away with paper copy time/cost

- Widens the scope of privacy and security protections available under HIPAA;
    - Business Associates now directly liable for failure to comply with HIPAA and HITECH's requirements
- Increases the potential legal liability for non-compliance;
    - Mandatory and increased penalties for "willful neglect;"
- Enhanced Enforcement
    - Authorizes State Attorney General to file action against covered entity on behalf of his or her residents;
    - Requires HHS to conduct periodic audits of covered entities and business associates
- Mandatory Breach Notification

Recent Developments:

Reporting for National Background Checks

On January 4, 2016, HHS used its rule making authority to expressly permit certain covered entities to disclose to the National Instant Criminal Background Check System (NICS) the identities of those individuals who, for mental health reasons, already are prohibited by Federal law from having a firearm.

Who:

- Covered entities that either make the mental health determinations that disqualify individuals from having a firearm or are designated by their States to report this information to NICS;
- The rule does not apply to most treating providers and does not allow reporting of diagnostic, clinical, or other mental health treatment information.

What Can be Disclosed:

- The minimum necessary identifying information (but not clinical information) about individuals who have been involuntarily committed to a mental institution or otherwise have been determined by a lawful authority to be a danger to themselves or others or to lack the mental capacity to manage their own affairs.

Court's Ruling on Same-Sex Marriage and It's Implications on HIPAA

In *United States v. Windsor*, the Supreme Court held section 3 of DOMA to be unconstitutional, which had provided federal recognition of only opposite-sex marriages. In light of the Windsor decision, covered entities and business associates need to understand how the new definition of "spouse" and "marriage" implicates the rights and obligations under HIPAA.

- *Spouse* now includes individuals who are in a legally valid same-sex marriage sanctioned by a state, territory, or foreign jurisdiction (as long as, as to marriages performed in a foreign jurisdiction, a U.S. jurisdiction would also recognize the marriage);

- *Marriage* now includes both same-sex and opposite-sex marriages, and *family member* includes dependents of those marriages. All of these terms apply to individuals who are legally married, whether or not they live or receive services in a jurisdiction that recognizes their marriage.

- *Family member* is relevant to the application of§164.510(b) *Standard: Uses and disclosures for involvement in the individual's care and notification purposes.* Under certain circumstances, covered entities are permitted to share an individual's protected health information with a family member of the individual. Legally married same-sex spouses, regardless of where they live, are family members for the purposes of applying this provision.

HYPOTHETICAL PROBLEM FOR DISCUSSION
NBI SEMINAR SEPTEMBER 30, 2016

OBTAINING, SAFE KEEPING, USING (TRANSMITTING) DESTRUCTION VIOLATIONS AND PENALTIES - HIPAA

Mr. Youngman is a new attorney working in the law firm of Duey, Cheatum & Howe that handles, among other client matters, the legal affairs of Titan Hospital System. The Managing Partner assigned the task of insuring the firm was HIPAA compliant to Mr. Youngman.

After reading up on the statutory and regulatory law, both state and federal, he realizes a) the client is covered entity; and b) the firm is a business associate performing functions on behalf of the covered entity. Mr. Youngman embarks on the effort of locating the firm's Business Associate Agreement with the client. Upon approaching the partner in charge of the healthcare section for the firm, the young associate learns the Partner-in-Charge has no idea what a BAA is or why one is needed, let alone where it might be located.

The Partner-in-Charge orders the associate to find the BAA, but under no circumstance is he to contact the hospital for a copy. After several queries of attorneys and staff members of the health care section,

the associate was instructed to ask the firm's administrator. Upon approaching the firm's administrator, the associate was told perhaps that "old" Agreement is in retained storage off site but it will take a few days to retrieve the Agreement. Dutifully reporting back to the Partner-in-Charge, the associate explained, again the importance of a BAA and the ramifications of not having a current Agreement. The Partner-in-Charge, reflecting how long the firm has been representing the hospital system, thinks things will be fine with or without an up to date BAA. Meanwhile the firm will continue providing services to the hospital client Titan.

Finally, three days after his urging the firm administrative gave the associate the BAA by and between Titan Regional Hospital and Duey & Smith dated January 10, 1997. Returning to the Partner-in-Charge, the Associate explained the deficiencies of the BAA and its ramifications.

Accordingly, the associate was tasked to draft a compliant BAA for the firm and for the client's use. The BAA must now include _____.

Because the firm and the hospital was not compliant under the old BAA, any resulting penalty for this violation?

- ¬ Who should be the Custodian of the BAA for the firm?
- ¬ How long must the BAA be in place?

¬ What does the BAA accomplish?

Among the many clients of the firm, it also has an entertainment section representing famous celebrities, movie stars, recording artists, sports figures, etc. One such client is Jimmy Goofball, world acclaimed recording artist who happens to be a recovering addict, both alcohol and drugs. Jimmy has been sober for some time, but before obtaining his sobriety, he was in and out of treatment programs that the firm was aware of and would receive, with Jimmy's permission, copies of his addiction treatment records. The records are stored on the firms' server, but not password protected. A temporary staff member working in the firm's general litigation section accidentally came across Jimmy's addiction treatment record. The temporary staff member downloaded Jimmy's records onto a thumb drive and took it home. Hoping to parlay the addiction records of Jimmy into a pay day, the temporary staff member contacts a national tabloid with the intent to sell these records of Jimmy. After showing the content of Jimmy's addiction treatment records the tabloid paid the temporary staff member $3,500.00 and asks if he can find records/dirt on other celebrities. If so, he will be placed on a monthly stipend while feeding this information to the tabloid. The temporary staff member agrees and starts trolling through the firm's server.

Unbeknownst to the temporary staff member, the firm had on its server a document tracker that logs all activity in any document when accessed and who accessed. The firm's IT Director routinely reviews the document tracker, mainly to track who is using the server versus staff or lawyers; but, only to determine who is actually working. The IT Director has noticed a trend the temporary staff member's server activity has picked up and is significantly greater than the activity of any other staff or attorneys. In fact, the IT Director realizes the Temp has accessed, systematically all of the medical records on the server for all sections starting with the Entertainment Section. Thinking the temporary staff member was simply an eager beaver, he recommended to HR the temporary staff member be hired as a permanent employee. Meanwhile, the temporary staff member was feeding confidential client information to the tabloid in exchange for money- to the tune of $3,500.00 per medical chart and any other previously known information the tabloid believed of value.

The Director of the firm's entertainment section has noticed an unusual up-tickof complaints from its client base about private confidential information, medical and otherwise appearing in the Tabloid. The Director of entertainment section puts out an internal firm notice to the partners about this upward trend. The IT Director sees this memo and checks the

server document tracker and discovers the temp staff member has reviewed client documents on both closed and open matters in excess of five hundred matters.