HIPAA & HITECH and the Discovery Process

Heather L. Hughes, J.D.
U.S. Legal Support, Inc.
363 North Sam Houston Parkway East
Suite 900
Houston, Texas 77060
713-653-7100
hhughes@uslegalsupport.com
www.uslegalsupport.com

I. Introduction to HIPAA

Anyone involved in litigation that requires a review of medical records should be familiar with the acronym *HIPAA.* The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") established a minimum federal standard for patient privacy and healthcare industry standards.[1] In 2001, the U.S. Department of Health and Human Services published a final rule on patient privacy entitled "Standards for Privacy of Individually Identifiable Health Information." More commonly referred to as the "Privacy Rule," it addresses the uses and disclosures of individual protected health information ("PHI") by organizations subject to the Privacy Rule called "covered entities." [2]

A. Affected Groups

Health care clearinghouses, health plans, and health care providers are all covered entities under the Privacy Rule.[3] Every health care provider who electronically transmits health information in connection with certain transactions is a covered entity. These transactions, such as claims and benefits eligibility requests, are covered whether the health care provider electronically transmits them directly or uses a third party billing service or other entity to do so on its behalf.[4]

Health care providers are the covered entities more commonly referred to as "custodians" when legal professionals are requesting medical information in relation to litigation. Custodians have become increasingly cautious about releasing patient records since the Privacy Rule compliance deadline of April, 2003. Many have not become educated with the specific regulations that allow for the release of PHI during litigation and thus sometimes cause delay when attorneys try to obtain the information during discovery.

PHI is defined as any individually identifiable health information; including demographic information, that relates to the past, present, or future physical or mental health or condition of an individual and is transmitted by electronic media.[5] Covered entities may not use or disclose PHI unless specifically permitted by the Privacy Rule. Permitted disclosures that do not require the individual's authorization include those to the individual, and those used for the covered entities for treatment, payment, and healthcare operations.[6] Under most circumstances, the individual's written authorization must be obtained by the covered entity to disclose PHI for any other reason not permitted by the Privacy Rule.[7]

B. HIPAA and Discovery, Myths and Facts

The Privacy Rule has specific exceptions that apply to the disclosure of PHI in the course of litigation and this has caused there to be several myths and misconceptions about how HIPAA affects the discovery process.

MYTH: Medical records cannot be released without subpoena.

FACT: A covered entity may release PHI in response to:

1. A court order signed by a judge, provided that only the information expressly authorized by the order is disclosed.[8]
2. Subpoena or discovery request signed by an attorney and accompanied by satisfactory notice by proof of service showing that the individual or his or her attorney was served a copy of the subpoena or discovery request and a **reasonable** time of object has expired.[9]
3. Qualified Protective Order-- a court order that prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the information was requested, and requires the return of the PHI to the covered entity or destruction of the PHI at the end of the litigation.[10]
4. A valid Authorization

MYTH: Subpoenas, Authorizations, or other court orders are needed to obtain medical records when the custodian is a party to the litigation (plaintiff *or* defendant).

FACT: Covered entities are permitted to disclose PHI *without* patient authorization for the purposes of treatment, payment and healthcare operations which include such activities as; compliance reviews, business planning, financial and accounting reviews, and legal activities. [11]

- When representing a covered entity, attorneys are responsible for ensuring that others hired to assist in providing legal services to the covered entity will also safeguard the privacy of the PHI.
  This includes jury experts, joint counsel, investigators, litigation support, etc.
- This does not include opposing counsel.[12]

MYTH: Subpoenas and Authorizations are both needed to obtain medical records when the custodian is *not* a party to the litigation.

FACT: Authorizations, if compliant with the elements required by the Privacy Rule, are sufficient to obtain PHI.[13]

- Description of information to be disclosed (radiology, pathology, entire record, etc.)
- Identity of the person authorized to make disclosure (custodian)
- Identity of the person to whom the covered entity can disclose the PHI (law firm, litigation support firm, expert witness, etc.)
- Description of the purpose of the request for disclosure ("for purposes of litigation" is sufficient)
- Expiration date or event ("at the end of litigation" is allowed, a specific date is NOT required)
- Signature of the person authorizing disclosure with date
- Individuals right to revoke authorization in writing
- Statement that information disclosed may be subject to redisclosure and no longer protected by the Privacy Rule
- The ability or inability to condition treatment, payment, enrollment or eligibility of benefits on the authorization
- Plain language requirement
- Copy to the individual

MYTH: Subpoenas and Authorizations must specify the dates of treatment for which records are requested and may not request the entire record.

FACT: The Office of Civil Rights has stated that a request for the "entire medical record" is valid. This can also be written as "complete patient file." An Authorization listing "all protected health information" without further definition is not sufficiently specific enough however. [14]
**This is especially useful for those defending products liability and toxic tort cases where the entire medical record may yield information about previous health conditions.*

MYTH: HIPAA changes state public records or "freedom of information" laws, which provided certain public access to government records.

FACT: If a state agency is not a covered entity, it is not required to comply with the Privacy Rule and any public records disclosures would not be subjected either.

- If a state agency is a covered entity, the Privacy Rule applies to the disclosures of PHI.

- The Privacy Rule permits disclosures of PHI as "required by other law," including state law. So if a state public records law mandates the disclosure of PHI, then the public records law requirements apply.[15]

MYTH: HIPAA regulations do not apply to deceased individuals.

FACT: Patient health information is protected after the patient dies. The proposed 1998 regulations applied for a "limited time" but the final rule extended the protection indefinitely.

II. HIPAA and HITECH

Obtaining medical records during the course of litigation has become increasingly difficult since 2003. Law firms representing covered entities now need to pay special attention to the HIPAA Privacy and Security Rules because of HITECH. The Health Information Technology for Economic and Clinical Health (HITECH) Act, was enacted as part of the American Recovery and Reinvestment Act of 2009 and amended several aspects of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HITECH affects all business associates of covered entities, including law firms. Business associates are entities that act on behalf of covered entities by performing duties that involve the transmission, creation

or maintenance of PHI. Law firms representing hospitals and health insurance companies, consulting firms, etc. are all now required to comply with the HIPAA Security Rule.[16]

Previously, business associates of covered entities had only contractual obligations under HIPAA. Covered entities drafted the Business Associate Agreements and their lawyers, consultants and other vendors signed them, ensuring that PHI would be protected. Now, under HITECH, those same business associates must proactively comply with the Security Rule provisions of HIPAA and they face the same fines and reporting requirements as covered entities. This includes ensuring that anyone assisting the law firm with litigation involving a covered entity must also be HIPAA compliant.

Business associates must now comply with the physical, technical and administrative safeguards as outlined in the Security Standards for the Protection of Electronic Protected Health Information.[17] Any lawyer representing a covered entity was required to comply with these rules as of December 29, 2009. The requirements for these law firms include; drafting or revising existing firm policies regarding PHI, training employees, as well as drafting or renegotiating business associate agreements with all outside vendors.

Enforcement and penalties now apply to law firms and lawyers can be investigated by the federal government and/or their state attorney general and fined for security breaches. The following only addresses what the Security Rule "requires" of covered entities and their business associates. For items that are recommended only or "addressable", see the Security Standards Matrix at the Centers for Medicare and Medicaid Services ("CMS"). Many covered entity clients are requiring their outside counsel to sign updated business associate agreements addressing these new requirements. Some even require that their outside counsel carry "Privacy" insurance to cover any possible breaches of electronic PHI.

A. Administrative Safeguards

Business associates are required to conduct a "Risk Analysis" to determine any areas where there may be a need for new policies and procedures. This involves a complete and thorough assessment of any potential vulnerabilities to the confidentiality of electronic PHI. This should be the first step taken to ensure compliance as it will alert the law firm or other business associate to the areas that need immediate attention.

The following policies are required under the Administrative Safeguards provision: [18]

- Risk management to implement any new policies to ensure compliance with the Security Rule
- Sanction policy against any employees who fail to comply with the security measures adopted by the business associate
- Review of all information systems including audit logs, activity, access reports and incident tracking
- Workforce security to prevent unauthorized access to electronic PHI which includes training for all employees, including management.
- Incident reporting to identify and respond to any suspected or known security incidents and maintain documentation of all incidents
- Contingency plan must include data backup plan, disaster recovery plan and emergency mode operation plan to retrieve and restore any lost data in the event of an emergency
- Business associate contracts to require all outside vendors to comply with the Security Rule as well
  **For law firms, this means all litigation support firms (court reporting firms, expert witnesses, legal copy companies, etc.) must sign business associate agreements drafted by the firm.*

B. Physical Safeguards

There must be policies and procedures in place that simultaneously allow authorized employees to access the data in order to complete their job duties and limit physical access to everyone else. The storage and destruction of PHI within law firms must be addressed under this provision.

The following policies are required under the Physical Safeguards provision: [19]

- Paper records must be shredded or otherwise destroyed to render them indecipherable
  **Paper PHI may NOT be recycled*
- Disposal of electronic information must be addressed with policies, procedures and workforce training

- Media re-use policies to address that electronic PHI is removed from any media before they are returned or re-used. This includes copiers and scanners returned to the leasing company, recycling of laptops, etc.
- For electronic media, the following methods can be used to destroy the PHI:
    - Clearing or overwriting the data with non-sensitive data
    - Purging or exposing the data to a strong magnetic field
    - Destroying through pulverizing, melting, incinerating or shredding
    - HIPAA rules utilize the "NIST SP 800-88 Guidelines for Media Sanitization"

Some common controls that law firms can implement can include key-card entry to areas with PHI, signs warning of restricted areas, requiring escorts for all firm visitors, visitor tags and alarms.

C. Technical Safeguards

Business associates must take appropriate measures to ensure that no unauthorized access to their electronic communications networks occurs. Desktop computers, laptop computers, smartphones, and network servers must all be protected against hacking, theft and other types of unauthorized access. For law firms, policies must be drafted regarding such things as passwords and log-out times for any employees with access to the firm email system and servers.

The following policies are required under the Technical Safeguards provision: [20]

- Unique User Identification to allow the covered entity to track use activity as well as prevent unauthorized access
- Emergency access procedures to obtain electronic PHI in case of power failure, natural disaster, etc. must be implemented to ensure the information is maintained and accessible

Questions often arise regarding the transmission of electronic PHI, specifically emailing medical records. The Security Rule allows for electronic PHI to be sent electronically over an open network as long as it is protected.[21] Encryption and integrity controls are only "recommendations" of the Security Rule, however, many covered entities are requiring encryption of electronic communications like emails. The main objective is that any electronically transmitted PHI is not improperly modified during transmission.

D. Breach Notification

Under the new HITECH rules, business associate law firms are now required to report any breaches of PHI that occur while representing covered entities. Depending on the severity of the breach, the business associates will have to notify the Department of Health and Human Services ("HHS"), the patients whose PHI was affected and, in some instances, the media. In every breach, the law firm must notify their covered entity client according to the terms in the business associate agreement but no later than 60 days from the discovery of the breach.[22]

The HITECH Act defines breach as "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual."[23]

This rule applies when the PHI is "unsecured" as defined as PHI that is "not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS in guidance." [24]

Business associate law firms must pay special attention to how they store and destroy the PHI in their files and offices as they are much less likely to be required to notify the patients or the media if safeguards have been implemented to secure the PHI. A breach notification policy should be included in the firm's HIPAA policies and procedures and all employees and volunteers should be trained on incident reporting mechanisms in case of a PHI breach.

III. Enforcement and Penalties

Prior to the HITECH Act, HHS could not impose penalties of more than $100 for each violation or $25,000 for all identical violations of the same provision. In February of 2009, the HITECH Act strengthened both the criminal and civil enforcement of the HIPAA rules which sent the message to covered entities and their business associates that the security of PHI was a priority for HHS.

Violations are investigated by the Office of Civil Rights of HHS and are only applicable if the offenses occurred after April 14, 2003. If the Office of Civil Rights suspects that a criminal violation has occurred, the Department of Justice may become involved in the investigation as well.

A. Civil Monetary Penalties

The penalties for violation of the HIPAA Security Rule now range from $100 to
$1, 500,000. The previous affirmative defense in which the covered entity could avoid fines for violations in which the covered entity did not know, or by reasonable diligence would not have known, of the violation has been removed.[25]

The amounts of the fines now increase in tiered levels according to the following levels of culpability: [26]

- A violation without knowledge of the violation results in $100 per violation with an annual maximum amount of $25,000 in penalties for violations of identical provisions
- A violation that is due to reasonable cause results in $1,000 per violation with an annual maximum amount of $100,000 in penalties for violations of identical provisions
- A violation that is due to willful neglect and is corrected results in $10,000 per violation with an annual maximum of $1,500,000 in penalties for violations of identical provisions
- A violation that is due to willful neglect and is *not* corrected results in $50,000 per violation with an annual maximum of $1,500,000 in penalties for violations of identical provisions

The HITECH Act also granted enforcement authority to the states attorneys general to bring civil actions on behalf of their states when they learn of a breach. [27] In January 2010 the first action by a state attorney general under this provision was brought by the Connecticut attorney general's office against health plan for failing to secure the electronic medical records of over 400,000 enrollees.

B. Criminal Violations

A criminal violation occurs when a person or entity knowingly obtains or discloses PHI in violation of the Privacy Rule. The Department of Justice investigates and imposes the penalties, including possible jail time, for criminal violations.

The criminal penalties are scheduled to increase in 2011 but are currently tiered in the following levels: [28]

- A violation that is due to knowingly obtaining or disclosing PHI in violation of the Privacy Rule may result in a criminal penalty of up to $50,000 and up to one-year imprisonment
- A violation that is due to wrongful conduct involving false pretenses may result in a criminal penalty of up to $100,000 and up to five years imprisonment
- A violation that is due to wrongful conduct involving the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm may result in a criminal penalty of up to $250,000 and up to ten years imprisonment

C. Case Examples

Several covered entities have been investigated and fined under the new provisions of the HITECH rule: [29]

- Cignet of Prince George's County, Maryland was fined $1,300,000 for refusing to give patients access to their records. An additional $3,000,000 was imposed for failing to cooperate with the Office of Civil Rights' investigation.
- Mass General (General Hospital Corporation and Massachusetts General Physicians Organization, Inc.) was fined $1,000,000 for a loss of PHI. The incident occurred when documents containing patient medical records were left on a subway train by a Mass General employee while commuting to work.
- In July 2011 The UCLA Health System agreed to pay $865,000 to settle potential violations of the HIPAA Privacy and Security Rules involving UCLA employees viewing the medical records of celebrity patients without permissible reason.

IV. Conclusion

Law firms representing covered entities must now comply with the HIPAA Privacy and Security Rules as well as HITECH in all business dealings with their clients. The first step to compliance is the risk assessment to discover issues should be addressed. Attorneys should create specific HIPAA policies and procedures that cover the administrative, technical and physical safeguards of the Security Rule to ensure that

PHI is secured at all times. The law firm workforce should be trained on the HIPAA policies and incident reporting mechanisms should be implemented to track and correct any suspected breaches of PHI.

While these rules and regulations will require changes in the way law firms handle medical records during discovery, proper security measures can limit the exposure to both the firm and clients. When representing covered entities, HIPAA compliant policies and procedures in law firms are not only a requirement under the new regulations, but they can also be an attractive marketing tool with potential clients.

Heather L. Hughes received her Bachelor of Science from Florida State University and her Juris Doctorate from The South Texas College of Law. She has over 20 years of experience in healthcare compliance and risk management.

Ms. Hughes is the HIPAA Privacy Officer for U.S. Legal Support, Inc. and she presents continuing legal education seminars on HIPAA & Discovery as well as consulting services for law firms and corporations affected by the HIPAA and HITECH regulations.

U.S. Legal Support, Inc. is a nationwide litigation support company providing records retrieval, court reporting and ESI services to law firms, insurance companies and corporations across the country.

www.uslegalsupport.com

Endnotes:

[1] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996)
[2] 45 CFR 160-164 (2002)
[3] 45 CFR 160.102, 160.103
[4] 45 CFR 160.103
[5] 45 CFR 164.501
[6] 45 CFR 164.502(a)(1)
[7] 45 CFR 164.508
[8] 45 CFR 164.512(e)(1)
[9] *Id*. at (ii)(A)
[10] *Id. at* (ii)(B)
[11] 45 CFR 164.502(a)(1)
[12] 45 CFR 164.504(e)
[13] 45 CFR 164.508
[14] *Id.*
[15] 45 CFR 164.512(a)
[16] Pub. L. No. 111-5 (2009) ("HITECH Act")
[17] 45 CFR Part 160 and Part 164, Subparts A and C ("Security Rule")
[18] Security Rule at 308
[19] Security Rule at 310
[20] Security Rule at 312
[21] Security Rule at 312 (e) (1)
[22] HITECH ACT at 13402
[23] *Id.*
[24] 45 CFR 164.402
[25] HITECH Act at 13410 (d)
[26] *Id.*
[27] HITECH at 13410 (e)
[28] 42. U.S.C. 1320d-6
[29] As reported by the Office for Civil Rights, Health and Human Services website, Health Information Privacy section