

Ten Things Lawyers Should Know about the New HITECH Act

by Amy S. Leopard

The American Recovery and Reinvestment Act of 2009 (ARRA) included sweeping changes to Health Insurance Portability and Accountability Act (HIPAA) medical privacy and security rules. The Health Information Technology for Economic and Clinical Health (HITECH) provisions of ARRA significantly expand privacy and security protections over protected health information (PHI) for covered entities.

Your clients who are healthcare providers or health plans have been busy updating their HIPAA training programs and revising policies and procedures governing PHI to account for the HITECH amendments effective February 17, 2010. But be aware that service providers such as law firms now have additional responsibilities if they act as business associates under HIPAA.

HITECH extends HIPAA privacy and security obligations to anyone acting as a business associate when receiving PHI from, or creating or maintaining PHI for a covered entity while providing services on their behalf. Covered entities provide PHI to their attorneys for a variety of purposes – perhaps to an antitrust lawyer to define the relevant market when defending a hospital restraint of trade or to a malpractice defense lawyer that needs a medical record to defend a claim against the provider. Healthcare attorneys may receive PHI to represent providers in payment disputes and advise on compliance, risk management, peer review or public health, accreditation and licensing obligations.

Here are a few things you will need to know about the new HITECH rules when handling PHI on behalf of a client that is a covered entity under HIPAA.

1. Your firm already may be regulated directly by HIPAA.

Under HIPAA, you may have been asked to provide your covered entity client substantial assurances of compliance with certain HIPAA provisions in the form of a “Business Associate Agreement.” Under HITECH, business associates are now required to comply directly with many HIPAA privacy and security standards that covered entities follow, namely using and disclosing PHI only as HIPAA permits, implementing appropriate administrative, physical and technical safeguards and policy and procedures, and detecting and reporting certain security breaches to covered entities.

That’s right -- HIPAA now regulates law firms directly when they provide legal services involving the disclosure of PHI from a covered entity or another business associate of the covered entity.

2. If so, you have new privacy and security obligations effective February 17, 2010.

Effective as of February 17, 2010, business associates that do not comply and implement necessary privacy and security provisions are subject to the civil and criminal penalties that currently apply to covered entities. HIPAA privacy standards now apply directly to business associates and prohibit using or further disclosing PHI in a manner that would violate the HIPAA privacy standards. The U.S. Department of Health and Human Services (HHS) is implementing many HITECH requirements by regulation.

On the privacy side, most law firms have sound safeguards in place for dealing with confiden-

tial information in the workplace owing to the confidences and secrets we keep on a daily basis. These practices need to have supporting policies and procedures under HIPAA. On the security side, business associates must perform or review their security risk assessments and address applicable security standards. Administrative, physical, and technical safeguards must reasonably and appropriately protect the confidentiality, integrity, and availability of any PHI the business associate receives, creates or maintains electronically pursuant to its legal representation of a covered entity. For both privacy and security, these safeguards require any agent or subcontractor to whom the firm provides PHI to agree to implement appropriate safeguards as well.

3. The penalties for noncompliance can be severe.

HIPAA enforcement has historically been complaint driven, and covered entities have often provided HHS with corrective action plans in lieu of paying civil monetary penalties. Further, HHS could not impose penalties when (i) the violator did not know (and by exercising reasonable diligence would not have known) that a HIPAA provision was violated, or (ii) noncompliance was due to reasonable cause (not to willful neglect) and was corrected within 30 days (or longer if HHS provided an extension based on the nature and circumstances of the compliance failure).

HITECH implements a new, tiered system of civil monetary penalties for HIPAA violations whereby fines increase based on the violator’s intent, as follows:

HIPAA/HITECH Violation was:	Penalty range for each violation
Not known and through reasonable diligence would not have been known by person in violation	\$100–50,000
Due to reasonable and not willful neglect	\$1,000–50,000
Due to willful neglect: <ul style="list-style-type: none"> corrected within 30 days not corrected within 30 days 	\$10,000–50,000 \$50,000

Tort damages are not necessary, and HITECH also authorizes state attorneys general to obtain damages on behalf of state residents or to enjoin HIPAA violations in federal district court.

4. How clients provide you information may change under HITECH.

Covered entities may disclose PHI only for a permitted purpose, and with certain exceptions, must make reasonable efforts to disclose only the minimum amount of information necessary to accomplish the intended purpose of the disclosure. Under HIPAA, covered entities could rely on the lawyer's representation regarding the amount of information needed for the representation.

Under HITECH, covered entities must limit permitted disclosures to the extent practicable to a limited data set of the PHI or to the extent minimum necessary as determined by the covered entity, at least until HHS issues guidance on the minimum necessary rule.

5. How you acquire, use or disclose patient health information is key.

In addition to discussing whether and the extent to which obtaining PHI is necessary, covered entities and their business associates should discuss whether the PHI can and should be created, transmitted or maintained electronically. Business associates now must comply with the HIPAA security standards for protected health information in electronic form. If you do not receive, create, maintain, or transmit PHI electronically, you are not subject to these specific standards for electronic PHI.

6. Whether you receive, create or transmit patient information electronically raises new security issues.

If you acquire, create or transmit PHI electronically, considerable compliance documentation is necessary. You must appoint a security official, establish physical safeguards for individual workstations, consider whether to implement technology to encrypt electronic PHI, and implement reasonable and appropriate policies and procedures to comply with the HIPAA security provisions.

7. Breach detection, notification, and mitigation preparedness is vital.

Last fall, HHS published a final HITECH breach notice rule requiring covered entities to provide detailed notices to affected individuals without unreasonable delay and no later than 60 days from the date of discovering a breach of their unsecured PHI. The rule requires notice of what happened, how it happened, the types of PHI involved, and steps being taken to investigate the breach, mitigate harm, and protect against further breach. Covered entities also must notify HHS and for certain breaches, provide public notice via media and website. Notice is not required in certain instances where there is no significant risk of financial, reputation or other harm to the individual and mitigation would not require reporting.

Now, HITECH and the HHS rules require the business associate to notify the covered entity of any unsecured PHI breach it discovers without unreasonable delay and no later than 60 days from the date of discovering the breach. The notice to the covered entity must contain sufficient information to allow the covered entity to make its required disclosures. Since attorneys typically would be considered an agent of the covered entity under the federal common law of agency, the law firm's discovery date of an unsecured PHI breach will trigger the client's notice obligations. As a result, law firms must have in place methods

and procedures to promptly notify a client should a breach occur.

8. You can manage some of these risks through a limited data set or encryption.

Sometimes attorneys need to receive PHI in electronic form in connection with the engagement. The HITECH breach notice requirement applies only to unsecured PHI, that is, PHI not secured through technology standards endorsed by HHS or stripped of certain identifiers.

HHS has encouraged encryption when the security risk is significant, and HHS endorsed encryption standards that now serve as "safe harbors" for data at rest or in transmission. Many covered entities are working closely with their business associates to develop procedures and implement technologies under the "encryption safe harbors."

Most covered entities have now adopted encryption as a method for securing and transmitting PHI. Covered entities transmitting PHI electronically must implement technical security mechanisms to guard against unauthorized access. Security mechanisms should be agreed upon in advance of the transmission, commensurate with the relative risk.

Often, using and disclosing PHI through a limited data set provides sufficient information and has the same potential for reducing exposure.

9. Compliance documentation for the engagement is also necessary.

The most significant compliance documentation required between you and your client is a Business Associate Agreement in place for engagements requiring the use of PHI. HIPAA also requires a Data Use Agreement to support the use of a limited data set. Whether existing agreements can or should be updated specifically for HITECH depends upon whether they adequately address the applicable requirements.

The major consideration under HITECH is that the Breach Notification Rule places new obligations on both parties. Some covered entities may expect business associates to use encryption and limited data sets or include explicit breach reporting timeframes and cost allocations. HIPAA business associate agreements have always required reporting to a covered entity any HIPAA violations or security incidents of which the business associate becomes aware, so many covered entities are

simply sharing their updated breach notice policies regarding to whom and how to report breaches as part of their HIPAA incident reporting procedures. Covered entities also may ask about the firm's insurance in the event of such a breach or seek reimbursement or indemnification for the cost of notification and mitigation from business associates who cause a reportable breach.

10. If your client breaches, you may have an obligation to report this to HHS, so be careful how the business associate agreement is drafted and watch for bar associations and health lawyers to comment on any rule that restricts lawyer-client communications.

Be aware that under the so called HITECH "snitch" provisions, business associates have an affirmative duty to take reasonable steps to cure a HIPAA violation or breach of the business associate agreement by the covered entity, or in some instances, terminate the agreement if feasible. If termination is not feasible, the business associate must report the breach or violation to HHS.

It is unclear whether the business associate's obligation to cure or terminate in light of a breach by the covered entity applies to the

covered entity's duties under the business associate agreement or more broadly to the covered entity's obligations and requirements under HIPAA. Bar associations will certainly object to any HHS interpretations of this statutory mandate that impinge upon communications between attorneys and their clients or discourages covered entities from obtaining legal advice in the event of a breach.

Lawyers and firms dealing with patient information must understand how HITECH impacts legal practice so that they may properly limit how PHI is obtained and used and prepare compliance documentation and breach notification policies. Compliance is now required by law. Now is a great time to re-evaluate your business practices and client relationships in light of HITECH. ➔



Amy S. Leopard heads the health care practice group at the law firm of Walter & Haverfield LLP and may be reached at aleopard@walterhav.com.

PRIVATE MEDIATOR



THOMAS REPICKY, ESQ.
EXPERIENCED AND EFFECTIVE
OVER 700 PRIVATE
MEDIATIONS CONDUCTED

PERSONAL INJURY
MEDICAL NEGLIGENCE
COMMERCIAL CASES
EMPLOYMENT
CONSTRUCTION

SELECTED BY HIS PEERS IN 2009
ADR SPECIALTY
OHIO SUPERLAWYERS
30 YEARS OF LEGAL EXPERIENCE

www.ClevelandMediator.com
Email: TomRepicky@sbcglobal.net

Tel: 440-247-3898
Cell: 440-725-1224



GILMOUR CAMPS

Something for Everyone...

PRESCHOOL CAMP: June 14 - July 30
(440) 684-4574

For boys and girls: half-day and full-day sessions

DAY CAMP: June 14 - July 30
(440) 684-4580

For boys and girls entering Kindergarten - eighth grade

WEEKLY CAMPS: June 14 - July 30
(440) 684-4580

For boys and girls third - eighth grade—explore moviemaking, nature, baking, dance, drama, photography, piñata making, 3D art, and much more!

SPORTS CAMP AND HOCKEY SCHOOL: June 14 - August 13
(440) 449-7490

For boys and girls ages 4-18—this camp includes hockey, baseball, golf, outdoor adventure, and more!

**NEW
SWIMMING
POOL!**

REGISTER ONLINE AT www.gilmour.org