By Anthony L. Holton

Healthcare lawyers: Ensure your clients (and your colleagues) are compliant with HITECH

The Health Information Technology for Economic & Clinical Health Act ("HITECH"), adopted as part of the Federal Stimulus Package of 2009 (or the "American Recovery & Reinvestment Act of 2009"), was enacted to encourage the implementation and utilization of electronic health records by healthcare providers. While the broad push for an electronic infrastructure in the healthcare industry undoubtedly provides significant advantages, it also carries added risks, especially with regard to disclosures of protected health information ("PHI") and other privacy breaches. HITECH addresses these risks by advancing some of the most significant changes yet to the privacy and security measures in the Health Insurance Portability & Accountability Act of 1996 ("HIPAA"). These changes have greatly affected legal and healthcare professionals alike, imposing complex administrative and regulatory demands on healthcare providers ("covered entities" under the Act) and their business associates along with a new civil penalty structure for those who are noncompliant. It is incumbent on those who practice health law to be vigilant in following the regulatory developments of HIPAA compliance, and these demands are even more rigorous with the passage of HITECH.

Anthony L. Holton
Wilkinson, Goeller, Modesitt, Wilkinson & Drummy LLP
Terre Haute, Ind.
ALHolton@wilkinsonlaw.com

Although HITECH was enacted in 2009, it wasn't until Jan. 25, 2013, that the Department of Health & Human Services ("HHS") released its Final Rule to implement the provisions of HITECH and amendments to HIPAA. Healthcare providers and their business associates were expected to be in full compliance with much of the law by Sept. 23, 2013.[1] Therefore, the time is ripe for legal professionals to ensure that healthcare professionals and their business associates are compliant with HITECH rules and regulations and understand how the new rules may interact with state law.

The Final Rule released by HHS addresses proposed regulations under HITECH that sparked the most discussion (and concern), including (1) the extension of HIPAA privacy and security rules to business associates of covered entities; (2) required risk assessments and breach notifications when an individual's protected health information is compromised; and (3) the expansion of an individual's right to restrict disclosure of PHI to health plans when paying out of pocket for healthcare items or services.[2]

Extension of HIPAA security and privacy rules to business associates

Before the adoption of HITECH, business associates of covered healthcare entities were not directly liable for breaches or improper disclosures of PHI in the performance of their services. With the enactment of HITECH, not only are business associates expected to comply with HIPAA's privacy and security rules, but also subcontractors of business associates and other "downstream" players must ensure compliance. This broad expansion of HIPAA's privacy and security rules fueled much debate about the reach and scope of HITECH.

A "business associate" is generally defined as a person or entity performing functions, services or activities on behalf of a covered entity that involve the receipt, maintenance, use or disclosure of protected health information.[3] This definition would encompass patient safety organizations, health information organizations, "E-Prescribing Gateways," records vendors, record storage organizations, as well as attorneys, accountants and any other entity or individual that receives or maintains PHI.[4] Not only are these entities considered business associates, but also their subcontractors and any other downstream entities who maintain PHI are considered business associates and expected to comply with the enhanced HIPAA privacy and security rules. This is so even if the business associate doesn't actually view the PHI; all that is required is the receipt and maintenance of PHI.[5]

With the enactment of HITECH, business associates are directly liable under various HIPAA rules, including rules for impermissible uses and disclosures of health information,[6] for failure to provide notification to a covered entity in the event of a breach of confidentiality,[7] for failure to provide access to a copy of electronic PHI to either the covered entity or the individual, for failure to disclose PHI where required by the Secretary to investigate or determine the business associate's compliance with the HIPAA rules,[8] and for failure to comply with the requirements of the security rule.[9]

Business associates must also bear in mind that they have certain contractual obligations. Covered entities must establish a Business Associate Agreement that requires business associates to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confiden-

tiality, integrity and availability of the electronic PHI that they create, receive or maintain on behalf of a covered entity.[10] The agreement must also provide that business associates take reasonable measures to ensure that any downstream agent, including a subcontractor, safeguards PHI.[11] Section 164.504(e) specifies the provisions required in the Business Associate Agreements,[12] and beyond these requirements, as with any contracting relationship, covered entities and business associates may include other provisions or requirements that dictate and describe their relationship.[13] These may or may not include additional assurances of compliance, indemnification clauses or other risk-shifting provisions.[14]

The requirements for contracts or other arrangements between a covered entity and a business associate apply in the same manner to contracts between business associates and subcontractors.[15] Each subsequent agreement in the "business associate chain" must be as stringent or more stringent as the prior agreement with respect to permissible uses and disclosures of PHI.[16] For those having a need to draft a Business Associate Agreement for their clients, the Department of Health & Human Services provides sample provisions on its website.[17]

Breach notifications and risk assessments

Section 13402 of HITECH requires HIPAA-covered entities to provide notification to affected individuals and – in certain circumstances – to the Secretary of HHS following the discovery of a breach of unsecured protected health information. A breach is treated as "discovered" on the first day the covered entity knows – or should reasonably have known – of the breach.[18] In the event a breach is discovered by a business associate of a covered entity, the Act requires the business associate to notify the covered entity.

A "breach" is the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information.[19] The interim HITECH rule proposed that the standard by which a "compromise" should be reported is when a breach poses a significant risk of financial, reputational or other harm to the individual. However, the Final Rule released this year amended this proposed rule, providing that *all* impermissible disclosures are

(continued on page 12)

presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. "Breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised."[20] Thus, a breach notification is not required under the Final Rule only if a covered entity or a business associate demonstrates through a "risk assessment" that there is a low probability that the PHI has been compromised, not merely that there is no significant risk of harm to the individual.[21]

Although some commentators pushed for a more objective bright-line standard to govern when a breach notification is required, a "risk assessment" requirement stems from a recognition by HHS that there are several situations in which an unauthorized disclosure of PHI is so inconsequential that it does not warrant notification.[22] The Final Rule provided some baseline factors that a covered entity or business associate should consider in its risk assessment, including: (1) the nature and extent of the PHI involved (*e.g.,* records of a common cold versus mental health information), including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made (*e.g.,* an individual's friend versus a paper shredding service); (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.[23] Other factors may be considered in addition to the foregoing, keeping in mind that every impermissible disclosure is presumed to be a breach, and HHS expects risk assessments to be thorough and completed in good faith, and for the conclusions reached to be reasonable.[24] A more thorough examination of these factors is outlined in the HHS Final Rule, which is available for public viewing on the Federal Register.

Upon discovery of a breach, a covered entity must notify individuals without unreasonable delay, but in no case later than 60 calendar days from the date of discovery.[25] This timeframe imposes an obligation of promptness on covered entities and their business associates to conduct their investigations and risk assessments. In some cases, waiting until the 60th day might be considered an unreasonable delay.[26] Notifications should include, to the extent possible: (1) a brief description of what happened, including the date of the breach and the date of discovery; (2) a description of the types of PHI involved; (3) any steps individuals should take to protect themselves; (4) a brief description of what the covered entity is doing to investigate and mitigate the damage; and (5) contact procedures for individuals to ask questions.[27]

The individual's right to request a restriction of uses and disclosures

Prior to the enactment of HITECH, covered healthcare providers had discretion to accept or reject an individual's request to restrict the use or disclosure of PHI for treatment, payment and healthcare operations purposes.[28] Now, HITECH sets forth circumstances in which a covered entity *must* comply with an individual's request to restrict disclosure of PHI to his or her health plan. Specifically, when an individual requests a

(continued on page 14)

restriction on disclosures of PHI to health plans where the purpose of the disclosure is solely for purposes of payment or healthcare operations, *and* the individual pays out of pocket in-full for the healthcare item or service, the covered entity is required to comply with the individual's request, unless disclosure is otherwise required by law.[29]

This requirement caused a great deal of confusion amongst healthcare providers and legal professionals. Many questions naturally arose from commenters covering a wide range of topics. What should providers do for services covered by state or federally funded Medicaid or Medicare programs, which may require disclosure of PHI through obligatory audits or otherwise? What is the effect of this provision where certain state laws prohibit "balance billing," making it illegal for a provider to bill the patient for any covered service over and above any permissible copayment, coinsurance or deductible amounts?

Commentators also raised issues such as how a provider is to operate in an HMO setting requiring submission of a claim or other disclosure of PHI, and whether a provider faces liability when "downstream providers," *e.g.,* pharmacies, are unaware of an individual's restriction request and disclose PHI to a health plan. Or what if an individual's out-of-pocket payment is not honored (*e.g.,* a bounced check) – is the covered entity still obligated by the individual's restriction request?

Many of these questions were addressed in varying degrees in the HHS Final Rule. The Rule clearly provides that covered entities are safe deferring to state law in instances where the law conflicts with an individual's restriction request under HITECH.[30] With respect to concerns about meeting legal obligations under state law, such as disclosing information to Medicare or Medicaid for required audits, HITECH allows disclosures that are otherwise required by law, notwithstanding an individual's requested restriction on disclosures.[31] For instance, Indiana's Medicaid regulations provide for certain audits and requests for information.[32] If the Medicaid Office requests certain PHI during an audit as required by state law, then a provider will not commit a HITECH violation by disclosing what is *minimally necessary* to comply with state Medicaid rules and regulations.[33]

Nor will a covered entity commit a HITECH violation by submitting a claim to a health plan for a covered service where a particular disclosure is required by federal

law, such as Medicare.[34] Exceptionally, for those concerned about contractual obligations in an HMO setting, HHS does "not consider a contractual requirement to submit a claim or otherwise disclose protected health information to an HMO to exempt the provider from his or her obligations under [HITECH]."[35]

With respect to maintenance of medical records, the Final Rule does not require covered entities to create separate medical records or otherwise segregate PHI to protect against inadvertent disclosures. However, covered entities will need to employ some method of "flagging" or notations in the record to ensure that PHI is not inadvertently sent to a health plan.[36] The Final Rule notes that covered entities should already have in place, and thus be familiar with applying, minimum necessary procedures that limit the PHI disclosed to a health plan to the amount reasonably necessary to achieve the purpose of the disclosure.[37]

Another area of concern amongst commentators is how to address the scenario in which an individual requests a restriction with respect to only one of several healthcare items or services provided in a single encounter, and it is administratively burdensome to unbundle the item or service for billing purposes. The Final Rule suggests that a provider should unbundle the services if able to do so.[38] If unbundling would cause an administrative burden, then the provider should inform the individual and give him or her the opportunity to restrict and pay out of pocket for the entire bundle of items or services.[39]

Covered entities are encouraged in many scenarios to engage in open dialogues with individuals about their rights under HITECH. For purposes of "downstream" services, where an individual prefers that downstream providers, *e.g.,* pharmacies, abide by restriction requests, providers should assist the individual, if feasible, in alerting downstream providers of PHI restrictions and should inform individuals of the possibility of inadvertent disclosures.[40] With respect to follow-up care, where a prior service was paid out of pocket and not disclosed, and the provider needs to include information that was previously restricted in the bill to a health plan in order to have the services deemed medically necessary or appropriate, HHS highly encourages covered entities to engage in an open dialogue with individuals to ensure that they are

(continued on page 16)

aware of the possibility of disclosure.[41]

As in all cases, best practice is to err on the side of caution, speaking openly with individuals regarding the possibility – despite requesting otherwise – that PHI could be disclosed to health plans, whether through an audit, a downstream or follow-up service, or otherwise. For additional caution, it would be wise to draft and issue a formal policy to those patients who request restrictions in order to inform them of HITECH's limitations.

Refresh your clients' procedures and policies to comply with HITECH

HITECH is both exciting and daunting. Moving toward a digital infrastructure for the collection and use of medical data can lead to higher efficiency and decreased costs of healthcare services. However, HITECH's rules and regulations are complex, and a thorough understanding is required for those advising healthcare clients. For healthcare professionals and their advisors, it is essential that policies and procedures are updated to reflect the changes advanced by HITECH. The new regulatory framework surrounding Business Associate Agreements, PHI disclosure restrictions, and risk assessment practices are powerful and broad in scope. Healthcare lawyers should consult the HHS Final Rule as well as surrounding law to ensure that their clients are in full compliance with HITECH and, of course, other past and future HIPAA developments. ⚖

1. 78 Fed. Reg. 5566 (Jan. 25, 2013), amending 45 C.F.R. Parts 160 and 164.
2. The HHS omnibus rule also provides an extensive interpretation of the updated restrictions on the use and disclosure of PHI for marketing, sales and fundraising purposes.
3. 45 C.F.R. §160.103; 78 Fed. Reg. 5572 (Jan. 25, 2013).
4. *Id.* at 5571.
5. 78 Fed. Reg. 5572 (Jan. 25, 2013).
6. 45 C.F.R. §164.502(a)(3).
7. 45 C.F.R. §164.410.
8. 45 C.F.R. §164.502(a)(4)(i).
9. 45 C.F.R. §164, Subpart C.
10. 78 Fed. Reg. 5589 (Jan. 25, 2013).
11. *Id.*
12. 45 C.F.R. §164.504(e).
13. 78 Fed. Reg. 5601 (Jan. 25, 2013).
14. *Id.*
15. *Id.* at 5590.
16. *Id.* at 5601.
17. U.S. Dep't of Health & Human Services, Business Associate Contracts, at ***http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html*** (last visited Jan. 26, 2014).
18. 45 C.F.R. §164.404(a)(2).
19. 42 U.S.C. §17921(1)(A).
20. 78 Fed. Reg. 5641 (Jan. 25, 2013).
21. *Id.*
22. *Id.* at 5642.
23. *Id.*
24. *Id.* at 5643.
25. 45 C.F.R. §164.404(b).
26. 78 Fed. Reg. 5648 (Jan. 25, 2013).
27. *Id.*
28. 45 C.F.R. §164.522(a).
29. 78 Fed. Reg. 5628 (Jan. 25, 2013).
30. *Id.*
31. *Id.*
32. 405 Ind. Admin. Code §5-3-4 (2013); 405 Ind. Admin. Code §5-24-4(2013).
33. 78 Fed. Reg. 5628 (Jan. 25, 2013).
34. For instance, when a physician or supplier furnishes a service that is covered by Medicare, then Section 1848(g)(4) of the Social Security Act will apply, requiring a claim submission to Medicare. However, there is an exception to this rule where a beneficiary refuses to authorize the submission of a bill to Medicare. In such cases, a Medicare provider is not required to submit a claim for the covered service and may accept out-of-pocket payment. *Id.*
35. *Id.* at 5629.
36. *Id.* at 5628.
37. *Id.*
38. *Id.* at 5629.
39. *Id.*
40. *Id.*
41. *Id.* at 5630.

Anthony L. Holton is an associate with the Terre Haute firm Wilkinson, Goeller, Modesitt, Wilkinson & Drummy LLP. His practice consists of business and commercial litigation, insurance defense litigation and healthcare regulatory compliance. Tony is a graduate of I.U. Robert H. McKinney School of Law.