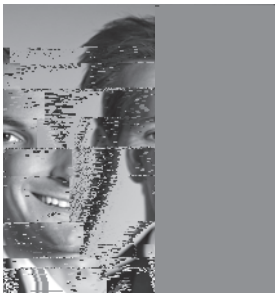
The Health Information Technology for Economic & Clinical Health Act

8E:OFMH9FCC;8?M;I&8H;9FDGCB8EJNBJA017.-0



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

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]

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 (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 (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.

restriction on disclosures of PHI to health plans where the purpose of the disclosure is solely for purposes of payment or healthcare operations, *a* state 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

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, 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

aware of the possibility of disclosure.[41]

As in all cases, best practice is to err on the side of caution, speak-