



DHHS ISSUES REGULATIONS REGARDING HIPAA NOTICE REQUIREMENTS

D. Brent Wills, Esq.
September 14, 2009

The federal Department of Health and Human Services (“HHS”) recently issued interim final regulations regarding certain changes implemented by the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) to the privacy and security requirements applicable to covered entities under the Health Information Portability and Accountability Act (“HIPAA”). Under the regulations, HIPAA now requires, for the first time, that, in the event of a breach of any unsecured protected health information (“PHI”),¹ covered entities and their business associates must provide certain, specified notice to individuals affected by the breach, HHS and, in some cases, the media.

This Client Alert merely provides an overview of the HIPAA notice requirements. If you have particular questions regarding particular aspects of the regulations or whether or how the regulations may apply to you or your employer, we recommend that you obtain the advice of appropriate legal counsel.²

1. What triggers the HIPAA notice requirements?

HHS emphasizes that the HIPAA notice requirements apply only in the event of a breach of unsecured PHI. For this purpose, a “breach” is any “unauthorized acquisition, use or disclosure of [PHI] which compromises the security or privacy of [PHI].” In other words, the HIPAA notice requirements are *not* triggered unless (i) “unsecured” PHI is involved; (ii) the unsecured PHI is “breached”; and (iii) the breach “compromises the security or privacy” of the unsecured PHI.

¹ For this purpose, “protected health information” means any individually identifiable health information. “Identifiable” refers not only to data that is explicitly linked to a particular individual, but also information that includes data that reasonably could be expected to allow individual identification. “Health information” means “any information, whether oral or recorded in any form or medium” that (i) “[i]s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse”; and (ii) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”

² For additional information regarding the HITECH Act and HIPAA, including details regarding the heightened obligations of business associates, as well as the increased civil monetary penalties for HIPAA violations, please see the Client Alert dated March 10, 2009 we prepared and forwarded to you this year. You may access this document electronically at our firm’s website: www.kgmlegal.com/resourceDetail.cfm?id=36.

2. What is “unsecured” PHI?

The regulations provide a “safe harbor” from the HIPAA notice requirements for PHI that has been rendered “unusable, unreadable or indecipherable to unauthorized individuals.” HHS has specified, though, in prior guidance, that encryption and destruction are the only means to render PHI “unusable, unreadable or indecipherable.”³ All other PHI, including electronic PHI protected by firewalls and any access controls other than encryption, is “unsecured,” so that any breach triggers the HIPAA notice requirements.

3. What is a “breach” of unsecured PHI?

As indicated above, a “breach” can be any “unauthorized” acquisition, use or disclosure of PHI that “compromises the information’s security or privacy.” The regulations provide that a breach is “unauthorized” only if it violates the HIPAA privacy rule.⁴ A thorough discussion of the HIPAA privacy rule is beyond the scope of this Client Alert. In general, however, any use or disclosure of PHI violates the rule, unless the use or disclosure is (i) specifically required or permitted by the rule⁵; or (ii) authorized in writing by the individual who is the subject of the PHI.

Even if an acquisition, use or disclosure of PHI is unauthorized, the HIPAA notice requirements are not triggered unless the acquisition, use or disclosure “compromises the security or privacy” of the information – that is, the acquisition, use or disclosure involves “a significant risk of financial, reputational or other harm to the individual” who is the subject of the PHI. Consequently, in the event a covered entity discovers a potential breach of unsecured PHI, it must conduct a risk assessment to determine whether the potential breach poses a significant risk of financial, reputational or other harm, and the risk assessment should entail examinations of factors including, but not necessarily limited to, (i) who impermissibly acquired, used or disclosed the PHI and/or to whom the PHI was disclosed; (ii) whether the covered entity recovered the PHI prior to it being accessed or used for an improper purpose; and (iii) the type and amount of PHI involved. On the other hand, the regulations provide that an unauthorized acquisition, use or disclosure of PHI does *not* compromise the security or privacy of PHI if it involves only a limited data set, as defined in the HIPAA privacy rule⁶ and does not include the subject individual’s date of birth or zip code.

³ The regulations do not specify what constitutes “encryption,” but certain encryption processes tested by the National Institute of Standards and Technology (“NIST”) have been judged to meet this standard. Additional information regarding these encryption processes may be accessed at <http://www.csrc.nist.gov/>.

⁴ The HIPAA privacy rule is set forth at 45 C.F.R. Parts 160 and 162.

⁵ The HIPAA privacy rule sets forth a number of circumstances where a covered entity is required or permitted to use and disclose PHI without violating the rule. Specifically, the rule requires that a covered entity disclose PHI to (i) the individual who is the subject of the PHI, upon request; and (ii) to HHS in connection with a compliance review or investigation. The rule permits a covered entity to use and disclose PHI, generally, only (i) to the individual who is the subject of the PHI, except in certain situations; (ii) for purposes of treatment, payment and health care operations; (iii) in circumstances that clearly give the individual who is the subject of the PHI the opportunity to agree, acquiesce or object to the use or disclosure (e.g., individual is incapacitated, listing PHI in facility patient directory); (iv) incident to an otherwise permitted use or disclosure; and (v) for any of twelve (12) public interest-type uses (e.g., for law enforcement purposes, or in connection with certain public health activities), as specified in the rule; or (vi) in the form of a “limited data set,” from which certain specified direct identifiers of individuals and their relatives, household members and employers have been removed.

⁶ For description of a limited data set, please see note 4, *supra*.

Finally, even if an unauthorized acquisition, use or disclosure of PHI occurs, and the acquisition, use or disclosure poses a significant risk of financial, reputational or other harm to the individual who is the subject of the PHI, the acquisition, use or disclosure is nonetheless *not* a breach, so as to trigger the HIPAA notice requirements, if any of the following exceptions apply:

(1) The acquisition, use or disclosure of the relevant PHI (i) was unintentional; (ii) was made by a workforce member or agent of the applicable covered entity in good faith; (iii) was made within the course and scope of the workforce member or agent's authority; and (iv) does not result in any further use or disclosure that violates the HIPAA privacy rule.⁷

(2) The acquisition, use or disclosure of PHI (i) was inadvertent; (ii) was made by a person authorized to access the PHI at the relevant covered entity or a business associate of the covered entity to another such individual at the same covered entity or business associate or within an organized healthcare arrangement in which the covered entity participates; and (iii) does not result in any further use or disclosure that violates the HIPAA privacy rule.

(3) The covered entity, or the business associate of the covered entity, has a good faith belief that an unauthorized person to whom the PHI was disclosed would not reasonably have been able to retain such information.⁸

If an unauthorized acquisition, use or disclosure of PHI has occurred, and the relevant covered entity has conducted a risk assessment and determined that the acquisition, use or disclosure poses a significant risk of financial, reputational or other harm to the individual who is the subject of the PHI, and the acquisition, use or disclosure does not meet one of the above-referenced exceptions, then the covered entity must notify the individuals affected by the breach, HHS and, in some cases, the media, all as explained below.

4. In the event a covered entity discovers a breach of unsecured PHI, what notice must a covered entity provide?

If a covered entity discovers a breach of unsecured PHI, it must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of the breach.⁹ The notice must be delivered without unreasonable delay and in no event later than 60 days after the covered entity discovers the breach.¹⁰

⁷ The regulations provide examples to illustrate this exception. In one example, a billing employee of a covered entity mistakenly receives and, unaware of the mistake, opens an email containing PHI. HHS provides that, if the billing employee alerts the sender and deletes the email before any further impermissible use or disclosure of the PHI occurs, no breach has occurred, and the HIPAA notice requirements are not triggered.

⁸ For example, if a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits to the wrong individuals, some of which are returned by the post office, unopened, as undeliverable, the regulations provide that (i) the individuals to whom the returned explanations were addressed could not reasonably have retained the PHI; and (ii) the explanations that were not returned should be treated as breaches, potentially subject to the HIPAA notice requirements.

⁹ Covered entities must provide notice to each affected individual by first-class mail to the individual's last known address (unless the individual has previously agreed to receive electronic notice, in which case electronic notice would suffice). The notice must include, to the extent possible, (i) a brief description of the breach of unsecured PHI, including the date the breach occurred and the date the breach was discovered; (ii) a general description of the types of unsecured PHI affected by the breach (e.g., full name, social security number, date of birth, home addresses, disability code); (iii) any steps the individual should take to mitigate the harm that could result from the breach; (iv)

The covered entity must also notify HHS regarding breaches of unsecured PHI.¹¹ In general, a covered entity is only required to notify HHS once per year (specifically, within 60 days after the end of each calendar year) regarding breaches that occurred during the preceding year. However, if the breach affects more than 500 individuals, the covered entity must notify HHS concurrently with the affected individuals.

In addition, if a breach of unsecured PHI affects more than 500 individuals in a particular state or jurisdiction, the covered entity must notify prominent media outlets serving that state or jurisdiction.¹²

5. What happens if a business associate of a covered entity discovers that a breach of unsecured PHI?

If a business associate¹³ of a covered entity discovers a breach of unsecured PHI, the business associate must notify the covered entity¹⁴ regarding the breach without unreasonable delay and in no event later than 60 days after it discovers the breach.¹⁵

a brief description of any investigation or mitigation efforts undertaken by the covered entity with regard to the breach; and (v) contact information (e.g., toll-free number, e-mail address, web site, mailing address) where the individual may direct questions to the covered entity regarding the breach. If a covered entity discovers additional information regarding a breach of unsecured PHI after initially notifying an affected individual, it must send additional notices to provide the individual with the additional information, even if the additional information is discovered more than 60 days after the covered entity discovers the breach.

¹⁰ A covered entity is deemed to have discovered a breach of unsecured PHI if the breach has been discovered, or by exercising reasonable diligence would have been discovered, by any member of the workforce or any other agent of the covered entity, other than the person(s) who committed the breach.

¹¹ Although it has not done so as of the date of this Client Alert, HHS has indicated that it will post specifications for notices to be delivered to it pursuant to the HIPAA notice requirements.

¹²The regulations do not define “prominent media outlet.” What constitutes a “prominent media outlet” must be determined based on what sort of notice is appropriate with respect to the particular state or jurisdiction affected by the breach.

¹³ For HIPAA purposes, a “business associate” is an individual or organization who, with respect to a HIPAA covered entity, either (i) performs, or assists in the performance of, on behalf of the covered entity or an organized health care arrangement in which the covered entity participates (other than in the capacity of a member of the workforce of the covered entity or arrangement), (A) a function or activity involving the use or disclosure of PHI, including without limitation claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) any other function or activity regulated by HIPAA; or (ii) provides (other than in the capacity of a member of the workforce of such covered entity) legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the services involves the disclosure of PHI from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the individual or organization.

¹⁴ The regulations allow covered entities and their business associates flexibility to specify how they will collectively fulfill the HIPAA notice requirements. Thus, a covered entity may wish, for example, to negotiate to shorten (relative to the HIPAA notice requirements) the amount of time allowed for its business associate to notify it regarding a breach of unsecured PHI to impose stricter indemnification obligations upon its business associate in the event the business associate fails to provide the required notice.

¹⁵ The requirements relating to delivery and content of the notice required to be given by a business associate to a covered entity are generally the same as the requirements relating to notices required to be given by the covered entity to affected individuals. Please note, however, that, in the event a business associate is acting as the agent of a covered entity (as opposed to an independent contractor) and discovers a breach of unsecured PHI, the business associate’s discovery would be imputed to the covered entity, such that the period during which the *covered entity*

6. *When do the HIPAA notice requirements take effect?*

The HIPAA notice requirements explained in this Client Alert will be effective beginning **September 23, 2009**. However, HHS will impose sanctions only with regard to breaches of unsecured PHI discovered after **February 22, 2010**. The regulations indicate that, prior to the enforcement date, HHS will work with covered entities and business associates, through technical assistance and voluntary corrective action, to achieve compliance.

7. *In the event a covered entity fails to comply with the HIPAA notice requirements, what penalties may apply?*

The HITECH Act strengthened the enforcement mechanisms available to enforce HIPAA compliance. For example, the Act authorizes the HHS Office of Civil Rights (“OCR”) to impose civil monetary penalties (“CMPs”) for noncompliance, up to \$10,000 per violation, if the noncompliance is willful. In addition, the Act authorizes state attorneys general to pursue certain civil remedies for HIPAA violations that occur within their jurisdictions. Moreover, the Act requires that HHS, in conjunction with the Government Accountability Office, establish, within three years, mechanisms whereby harmed individuals may recover a percentage of CMPs imposed by OCR.

IRS CIRCULAR 230 DISCLOSURE: Pursuant to U.S. Treasury Regulations, we are now required to advise you that, unless expressly stated to the contrary herein: (1) the contents and conclusions (if any) contained in this writing are preliminary in nature, (2) nothing contained in this writing is intended to be used, or may be relied upon or used by any taxpayer for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code of 1986, as amended, and (3) any written statement contained in this writing relating to any Federal tax issue may not be used by any person to support the promotion or marketing of or to recommend any Federal tax transaction(s) or matter(s) addressed in this writing.

must deliver its required notices would begin to run immediately upon the discovery of the breach, not whenever it receives notice from the business associate.