



Health Law Alert

Legal and political developments affecting the health care industry

A publication of Nixon Peabody LLP

AUGUST 25, 2009

HHS issues breach notification requirements for covered entities and business associates

By Linn Foster Freedman

On August 19, 2009, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued an interim final rule (“the Rule”) related to the Health Information Technology for Economic and Clinical Health Act (HITECH) requiring covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates to provide notification to individuals of breaches of unsecured protected health information to unauthorized individuals. In addition, HHS issued an update to its guidance specifying the technologies and methodologies that render protected health information (PHI) unusable, unreadable, or indecipherable. Section 13402 of HITECH, enacted on February 17, 2009, requires HIPAA covered entities and their business associates that “access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information” to notify the affected individual and the Secretary of HHS following the discovery of a breach of unsecured PHI. In addition, in some instances, HITECH requires notification of a breach to the media. Covered entities must provide the Secretary of HHS with a log of breaches on an annual basis, and the Secretary of HHS will post the list of entities that experienced breaches of unsecured PHI involving more than 500 individuals on the HHS website.

A breach means, generally, “the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.”

HITECH defines “unsecured protected health information” as “protected health information that is not secured through the use of a technology or a methodology specified by the Secretary in guidance.” The Secretary of HHS issued guidance on April 17, 2009, listing encryption or an encryption algorithm and destruction as two technologies rendering PHI unusable, unreadable, or indecipherable. HHS issued further guidance in the Rule that access controls do not meet the statutory standard for rendering PHI unusable, unreadable, or indecipherable, and that only encryption and the destruction of paper PHI render PHI unusable, unreadable, or indecipherable and therefore will

relieve a covered entity or business associate from the breach notification requirement. Further guidance on accepted technologies and methodologies includes the requirement that encryption keys should be kept on a separate device from the data that they encrypt or decrypt and that valid encryption processes for data at rest and data in motion are consistent with NIST Special Publications.

The importance of covered entities and business associates implementing the technologies and methodologies outlined by HHS cannot be overemphasized. If a covered entity or business associate secures or destroys PHI by implementing encryption technology and destroying paper records according to the specified technologies and methodologies, then in the event of a breach, the covered entity will *not* be required to notify individuals of a breach.

The Rule distinguishes the definition of a “breach” from that of HITECH. Both HITECH and the Rule limit the definition of a “breach” to a “use or disclosure that compromises the security or privacy” of the PHI. The Rule clarifies that the definition, “compromises the security or privacy of PHI,” means “poses a significant risk of financial, reputational, or other harm to the individual,” which is more consistent with state breach notification laws. Accordingly, to determine whether a breach has occurred, covered entities and business associates will need to perform a risk assessment regarding the level of harm that may befall the individual as a result of the disclosure. It is important for covered entities and business associates to establish breach notification policies and procedures in order to comply with the Act, and regulations as a specific risk assessment must be done on a case-by-case basis.

The Rule outlines an exception to the breach notification requirement relating to a limited data set (created by removing 16 direct identifiers of PHI). If there is a breach of a limited data set, a covered entity or business associate will have to undergo a risk assessment as in any other breach, but if the information disclosed does not include ZIP codes or dates of birth and the risk assessment indicates that the risk of re-identification poses no significant risk of harm to any individuals, then breach notification to the individual is unnecessary.

The Rule also provides three exceptions to the definition of *breach*:

1. The unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if it was made in good faith, within the course and scope of employment or professional relationship, and does not result in further use or disclosure
2. Inadvertent disclosure of PHI between similarly authorized personnel or within the same facility
3. A disclosure in which an unauthorized person to whom PHI has been disclosed would not have been able to retain the information

The rule requires a covered entity to notify an individual “without unreasonable delay and in no case no later than sixty (60) calendar days after the date the breach was discovered by the covered entity.” The purpose is to give covered entities and business associates time to conduct an investigation and to determine whether there was a breach of unsecured information that poses a significant risk of harm to any individual. The notice must be written in plain language and must include

1. a brief description of what happened, including the date of the breach and discovery of the breach;

2. a description of the type of unsecured PHI that was involved in the breach;
3. any steps individuals should take to protect themselves from potential harm resulting from the breach;
4. a description of the investigation into the breach, mitigation of harm to individuals, and protection against further breaches; and
5. contact procedures, which must include a toll-free telephone number, an email address, website, or postal address.

If the breach involves more than 500 individuals, notice must be provided to prominent media outlets and to the secretary of HHS through a press release. Interestingly, the Rule provides that if the breach involves individuals residing in more than one state, notification to prominent media outlets is required only if more than 500 individuals of one state are involved. Accordingly, if there was a breach of information of 600 individuals, 200 individuals residing in three different states, notification would be required to the individuals and the Secretary of HHS, but notification to the media would not be required. For breaches involving fewer than 500 individuals, a covered entity must maintain a log and submit the log annually to the Secretary of HHS.

HITECH and the Rule require a business associate to provide notification of a breach to the covered entity so that the covered entity can notify affected individuals. In addition to the specific identification of the affected individuals, business associates must provide any other available information that the covered entity is required to include in the notification to the individual and therefore, the Rule suggests that the business associate not delay initial notification of the breach to the covered entity in order for the covered entity to be able to collect the information needed for the specific notification.

HITECH and the regulations require covered entities and business associates to develop and document policies and procedures for notification of individuals, train workforce members on the policies and procedures and implement sanctions for a failure to comply with the policies and procedures. In addition, covered entities and business associates should maintain documentation regarding notifications made, the risk assessment performed and the analysis made to determine that an exception applied to substantiate that notification was not required.

It is extremely important that the breach notification compliance program of covered entities and business associates contain sufficient documentation of the risk assessment and response to the breach as they bear the burden of demonstrating that no breach occurred because it did not pose a significant risk of harm to the individual. In addition, in order to invoke the exception with respect to limited data sets, the covered entity must be able to demonstrate that the information did not include ZIP codes or dates of birth.

Finally, the Rule acknowledges that many states have adopted breach notification laws that may be contrary to the federal regulation. Accordingly, the Rule proclaims that contrary state breach notification laws will be preempted by the HHS breach notification regulations. A state law is contrary if “a covered entity could find it impossible to comply with both the state and federal requirements or if the state law stands as an obstacle to the accomplishment and execution of the full purpose and objectives of the breach notification provisions in the Act.” Accordingly, a covered entity, as part of its breach notification policies and procedures, will have to determine whether the state law of the state in which the individual resides is contrary to the federal breach notification regulations to determine whether preemption applies.

The regulations will be effective 30 days after they are published in the Federal Register and include a 60-day public comment period. Based on concern expressed during the comment period, discretion will be used in imposing sanctions for failure to provide notifications of breaches that are discovered before 180 calendar days from the publication of the Rule.

It is imperative that covered entities—including physicians, dentists, ambulatory care centers, kidney dialysis centers, family planning clinics, home care services, mental health and drug rehabilitation centers, medical laboratories, hospitals and nursing facilities, health insurance firms, third-party administrators, health plans, and pharmacies—and their business associates develop and implement breach notification policies and procedures, including a procedure for risk assessment, in order to comply with the HITECH Act breach notification regulations.

If you need assistance with compliance with HITECH and these regulations, the Nixon Peabody Health Information Technology Team is prepared to assist. For information, contact Linn Freedman at 401-454-1108 or lfreedman@nixonpeabody.com.