



HIPAA BREACH NOTIFICATION INTERIM FINAL RULE RELEASED; REGIONAL CONTACTS IDENTIFIED

HEALTHCARE ATTORNEYS

Karen S. Rieger
Healthcare Practice
Chair

Kevin D. Gordon
Healthcare Litigation
Practice Chair

Jennifer L. Ivester Berry

Laura Brookins

LeAnne Burnett

Jordan K. Field

Eric S. Fisher

Richard C. Ford

James H. Holloman, Jr.

Alison M. Howard

Christopher B. Keim

Michael S. Laird

Jay W. Larimore

Cori H. Loomis

Robert McCampbell

Kenni B. Merritt

Brooke S. Murphy

Cherish K. Ralls

Gary C. Rawlinson

Mary Robertson

Malcolm E. Rosser IV

Timila S. Rother

David A. Shipley

Earl A. Skarky

Roger A. Stong

Rustin Strubhar

HIPAA Breach Notification for Unsecured PHI

On Wednesday, August 19, 2009, the Department of Health and Human Services (HHS) released its interim final rule for "breach notification," ("IFR") as required under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The IFR was published in the *Federal Register*, 74 FR 42740, on Monday, August 24, 2009. The rule will be effective on September 23, 2009 and comments on the rule are due to the HHS Office of Civil Rights by October 23, 2009. The Final Rule may contain changes based on comments received.

Guidance on Definition of Unsecured PHI

Section 13402 of the HITECH Act requires breach notification following the discovery of a breach of *unsecured* PHI. On April 17, 2009, HHS issued guidance specifying that encryption and destruction are the technologies and methodologies for rendering PHI not unsecured.

There has been confusion regarding the impact of the breach notification requirements on a covered entity's responsibilities under the HIPAA Security rule. The IFR emphasizes that the breach notification requirement "does nothing to modify a covered entity's responsibilities with respect to the Security rule nor does it impose any new requirements upon covered entities to encrypt all [PHI]". Under the Security Rule, encryption is an addressable implementation specification. Therefore, "a covered entity may be in compliance with the Security Rule even if it reasonably decides not to encrypt electronic [PHI] and instead uses a comparable method to safeguard the information." To illustrate this point, the IFR includes the following example:

[I]f a covered entity chooses to encrypt [PHI] to comply with the Security Rule, does so pursuant to the [April 17] guidance, and subsequently discovers a breach of that encrypted information, the covered entity will not be required to provide breach notification because the information is not considered "unsecured" . . . On the other hand, if a covered entity has decided to use a method other than encryption. . . , then although that covered entity may be in compliance with the Security Rule, following a breach of this information, the covered entity would have to provide breach notification to affected individuals. For example, a covered entity that has a large database of [PHI] may choose, based on their risk assessment under the Security Rule, to rely on firewalls and other access controls to make the information inaccessible, as opposed to encrypting the information. While the Security Rule permits the use of firewalls and access controls as reasonable and appropriate safeguards, a covered entity that seeks to ensure breach notification is not required in the event of a breach of the information in the database would need to encrypt the information. . . "

Clarification of "Breach"

The IFR makes several significant clarifications to the definition of "breach". First, the IFR states that for 'an acquisition, access, use or disclosure of [PHI] to constitute a breach, it must constitute a violation of the Privacy Rule. Therefore, one of the first steps in determining whether notification is necessary . . . is to determine whether a use or disclosure violates the Privacy Rule."

Next, the IFR notes that the HITECH Act limits the definition of "breach" to a use or disclosure that "compromises the security or privacy" of PHI. HHS concludes that this quoted statutory language encompasses a harm threshold. Therefore, the language "compromises the security or privacy of [PHI]" means "poses a significant risk of financial, reputational, or other harm to the individual." HHS instructs that "to determine if an impermissible use or disclosure of [PHI] constitutes a breach, covered entities and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure." This risk analysis must be very fact specific and encompass a number of factors.

In addition, the IFR also addresses breaches of limited data sets by requiring the risk analysis of breaches of limited data sets as described in the preceding paragraph, unless the limited data set information disclosed also does not include zip codes or dates of birth. The IFR gives the following example:

Through a risk assessment, a covered entity or business associate may determine that the risk of identifying a particular individual is so small that the use or disclosure poses no significant risk of harm to any individuals. For example, it may be determined that an impermissible use or disclosure of a limited data set that includes zip codes, based on the population features of those zip codes, does not create a significant risk that a particular individual can be identified. Therefore, there would be no significant risk of harm to the individual. If there is no significant risk of harm to the individual, then no breach has occurred and no notification is required.

Guidance regarding Notification to HHS Secretary

Section 13402(e)(3) of the HITECH act requires covered entities to notify the Secretary of HHS of breaches of unsecured PHI. For breaches involving 500 or more individuals, the HITECH Act requires covered entities to notify the Secretary *immediately*. HHS is interpreting the word 'immediately' to require notification be sent to the Secretary in the case of large breaches *concurrently* with the notification sent to the individual, which must be sent without unreasonable delay but in no case later than 60 calendar days following discovery of a breach.

HIPAA Regional Coordinators

On August 14, 2009, the Office of Civil Rights identified [regional coordinators](#) for HIPAA privacy and security issues. Pursuant to Section 13403(a) of the HITECH Act, regional coordinators are to offer "guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to Federal privacy and security requirement for protected health information."

Oklahoma is in Region VI along with Arkansas, Louisiana, New Mexico and Texas. The name of the regional coordinator and his contract information is set forth below.

Ralph Rouse, Regional Manager
Office for Civil Rights
U.S. Department of Health and Human Services
1301 Young Street, Suite 1169
Dallas, TX 75202
Voice Phone (214)767-4056
FAX (214)767-0432
TDD (214)767-8940

This Advisory highlights some of the clarifications and information contained in the IFR. The IFR contains numerous clarifications that we could not address in this abbreviated format, such as guidance on the exceptions to the breach notification requirements and details on the methods and manner of providing the notice. We recommend that those responsible for implementing and administering the HIPAA requirements, obtain a copy of the IFR from the Office of Civil Rights website to review and use as a reference. The OCR website address is <http://www.hhs.gov/ocr/privacy/index.html>.

If you have questions about the breach notification requirements or this advisory, please do not hesitate to contact Karen S. Rieger, Co-Chair of the Healthcare Practice Group at (405) 235-7788, Karen.Rieger@crowedunlevy.com, or Cori H. Loomis at (405) 234-3238, Cori.Loomis@crowedunlevy.com.