



New Regulations Issued by the U.S. Department of Health and Human Services (“HHS”)

Effective September 23, 2009, new regulations issued by the U.S. Department of Health and Human Services (“HHS”) will require covered entities to notify affected individuals and HHS following the discovery of a breach of patient information. These regulations are more expansive than other notification laws that may already exist. Under these new regulations, covered entities must analyze every privacy and/or security incident to determine whether a notification requirement exists and then satisfy detailed notice requirements.

What is a “Breach”?

A “breach” is defined as the unauthorized acquisition, access, use or disclosure of unsecured Protected Health Information (“PHI”) which compromises the security or privacy of the PHI. It is important to note that this definition of breach is broader than most state notification laws under which most covered entities have already been operating for a number of years. While state notification laws may only require notification when there is an unauthorized disclosure of social security numbers or other specific kinds of personal information, under these new Federal regulations, unauthorized access, acquisition, use or disclosure of **any PHI**, not just social security number, is a potential breach. Further, unauthorized **uses** of PHI, not just access or disclosure, requires notification.

These notice requirements also apply when breaches occur while PHI is held by a business associate. Therefore, it is important to educate business associates regarding their reporting obligations.

What is “Unsecured Patient Information”?

Unsecured PHI is defined as PHI that is not secured through the use of a technology or methodology specified by HHS in guidance. In order to be secured, PHI must be rendered unusable, unreadable or indecipherable to unauthorized individuals. Examples of accepted security methodologies include encryption of data and shredding of documents.

How do you determine whether security/privacy has been “Compromised”?

The notice requirements only apply when there has been a breach that compromises the security or privacy of an individual’s PHI. A compromise of security or privacy occurs when there is a significant risk of financial, reputational or other harm to the individual. When evaluating the risk of harm, covered entities should consider, as applicable: (1) who impermissibly used the information; (2) to whom the information was impermissibly disclosed; and/or (3) the type and amount of PHI involved. Such risk assessment must be fact specific and documented in order to substantiate notification determinations.

When does the notification need to be made?

Notification of the breach should be sent **without unreasonable delay** and no later than 60 calendar days from the date of discovery. The date of discovery of the breach is the first day the breach is known or should reasonably have been known by the covered entity, including its employees and agents (e.g., certain business associates). The regulations specify the contents of the notification, as well as requirements for substitute notice when contact information for an individual is not available or incorrect.

continued...

Does HHS need to be informed of the Breach?

Providers must annually provide HHS with a log of all security breaches that have occurred during the past year. In addition, if over 500 individuals are affected by the breach, HHS must be notified of the breach at the same time as the affected individuals. HHS will post breaches involving more than 500 individuals on its website.

What do covered entities and business associates need to do?

We recommend that covered entities and business associates proactively put into place a security breach response program that defines notification requirements and the steps that must be taken to address breaches as they occur. At the very least, HHS has explicitly stated that it expects covered entities to educate workforce members regarding the breach notification requirements so as to ensure timely breach notifications when necessary. In addition, business associates and other agents must be made aware of the reporting and notification requirements. Finally, if a potential breach occurs, the covered entity will need to perform the risk assessment discussed above, and if a risk of harm exists, notify the affected individuals and HHS as required by the regulations.

* * * * *

If you would like assistance in preparing a security breach response program or responding to a privacy/security incident, or if you have any questions regarding the new breach notification requirements, contact your regular GWT attorney or any member of the GWT HIPAA practice group.

About Garfunkel, Wild & Travis, P.C.

Garfunkel, Wild & Travis, P.C. was founded in 1980 with a single purpose in mind: to become a pre-eminent health care law firm attending to the unique business and legal needs of its clients. Since then, the firm has grown to over 80 attorneys devoted to addressing the complex legal, regulatory, business and financial needs of its diverse clients.

If you would like to receive Legal Alert mailings from Garfunkel, Wild & Travis, P.C. electronically in the future, or if you would like to be removed from the mailing list, please contact us at (516) 393-2258 or subscriptions@gwtlaw.com. You may also visit the Firm's website at www.gwtlaw.com.

THIS MATERIAL IS INTENDED AS INFORMATIONAL ONLY AND THE CONTENT SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. READERS SHOULD NOT ACT UPON INFORMATION IN THIS MATERIAL WITHOUT FIRST SEEKING PROFESSIONAL ADVICE.

111 Great Neck Road
Great Neck, NY 11021
(516) 393-2200 | fax (516) 466-5964

411 Hackensack Avenue
Hackensack, NJ 07601
(201) 883-1030 | fax (201) 883-1031

350 Bedford Street
Stamford, CT 06901
(203) 316-0483 | fax (203) 316-0493