



New Laws Require Health Care Providers To Implement Additional Security Measures

In the past year, health care providers have seen several new developments with regard to the security of patient information. Although health care providers may have adopted HIPAA security policies and may be aware of State identity theft notification requirements, **there is still more to do**. In the last year: (1) the Federal Trade Commission (“FTC”) passed regulations referred to as “Red Flag Rules” which the FTC interprets as requiring most health care providers to adopt an identity theft prevention program; (2) Connecticut has passed legislation regarding protection of personal information such as social security numbers and health insurance identification numbers; and (3) the Centers for Medicare and Medicaid Services (“CMS”) has imposed penalties on a health care system for failing to implement adequate electronic security. As is discussed below, each of these developments should emphasize that it is not enough to merely adopt security policies. Implementation and integration of security measures into the daily operations of a health care provider are necessary to avoid regulatory penalties and legal action resulting from identity theft and other security incidents.

Red Flag Rules

Effective November 1, 2009¹, the FTC is requiring that most health care providers to adhere to the “Red Flag Rules” issued by the FTC. One of the “Red Flag Rules” requires users of consumer reports, which include hospitals and many other health care providers, to have policies and procedures to respond to reports from consumer reporting agencies regarding address discrepancies. For example, if a physician office receives an address discrepancy report from a consumer reporting agency, the physician office must have policies in place to identify the correct address of the patient and inform the consumer reporting agency of such information.

Another more significant “Red Flag Rule” requires an entity that regularly extends, renews, or continues credit (“Creditors”) to implement an identity theft prevention program to identify, detect, respond to and mitigate potential “red flags” that indicate the possible existence of identity theft. FTC representatives have stated that hospitals meet the definition of “Creditor,” because hospitals routinely defer payment for services and allow patients to enter into payment plans. By this analysis, other health care providers may also fit within the definition of Creditor. For example, a cosmetic surgery physician practice that allows patients to participate in a payment plan would most likely fit within the definition of Creditor and would be required to have an identity theft program.

There is an ongoing debate about whether health care providers qualify as Creditors. Nevertheless, the FTC continues to state a very broad view of the definition of “creditor” and even though this issue is still being considered, we recommend that hospitals and other health care providers begin the process of preparing required policies and procedures described in this Legal Alert.

The FTC has given Creditors significant flexibility to determine which “red flags” are relevant to their operations and what procedures are needed in order to prevent identity theft. It is, however, not enough to merely have HIPAA privacy or security policies. New policies and/or revisions to existing policies may now be required.

¹ The original deadline was November 1, 2008 but was recently delayed by the FTC until November 1, 2009.

continued...

Protection of Personal Information

Effective October 1, 2008, Connecticut's new "Act Concerning the Confidentiality of Social Security Numbers," (Public Act No. 08-167) requires any person in Connecticut in possession of personal information of another person to safeguard such information from misuse by a third party. This includes destroying, erasing or making unreadable data, computer files and documents containing personal information prior to disposal. "Personal information" is defined as "information capable of being associated with a particular individual through one or more identifiers, including, but not limited to Social Security numbers, a driver's license number, a state identification card number, an account number, a credit or debit number, a passport number, an alien registration number or health insurance identification number." Any information that is lawfully made available to the general public from federal, state or local government records or widely distributed media is excluded from the definition of "personal information."

Furthermore, a "privacy protection policy" is required to be developed and publicly displayed by employers who collect Social Security numbers. Such privacy protection policy must address (1) protection of the confidentiality of Social Security numbers, (2) prohibitions on unlawful disclosure of Social Security numbers, and (3) limitations on access to Social Security numbers. Failure to comply with the law may result in civil remedies.

CMS Assesses Penalty in HIPAA Security Audit

CMS and HHS have extracted their first significant monetary payment from a covered entity for its failure to protect electronic protected health information. Between 2005 and 2006, computer systems and related software of two entities within the Providence Health System, Providence Home and Community Services and Providence Hospice and Home Care, were stolen or lost compromising the protected health information of 386,000 patients. Providence followed applicable State law and notified the patients of the stolen and lost computers and hardware. However, even though Providence also self-reported to HHS, HHS determined that Providence had breached the HIPAA Privacy and Security Rules. Although CMS did not impose a civil monetary penalty, on July 15, 2008, it required Providence to pay \$100,000 as a "resolution amount" and to accept a three-year corrective action plan. This case confirms that effective compliance with HIPAA means more than just having written policies and procedures. To protect the privacy and security of patient information, health care providers need to continuously monitor their implementation of their HIPAA policies and update such policies as new requirements and concerns arise.

* * * * *

If you have any questions or require any assistance in complying with these new requirements or in assessing the effectiveness of your privacy and security programs, please contact your regular GWT attorney.

About Garfunkel, Wild & Travis, P.C.

Garfunkel, Wild & Travis, P.C. was founded in 1980 with a single purpose in mind: to become a preeminent 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 have any questions regarding this Legal Alert, please contact Patrick J. Monahan II, Esq. at (203) 316-0483.

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.