



New Laws Require Health Care Providers To Implement Additional Security Measures

In the past year, health care providers have seen a dramatic increase in the focus on the security of patient information. Although many health care providers may have adopted HIPAA security policies and may even be aware of, and complied with, State identity theft notification requirements, **there is still more to do**. Of particular note over the past year are two significant actions by separate branches of the Federal Government. The Federal Trade Commission (“FTC”) passed regulations referred to as Red Flag Rules that the FTC interprets as requiring most health care providers to adopt an Identity Theft Prevention Program. In addition, the Center for Medicare and Medicaid Services (“CMS”) has imposed penalties on a health care facility for failure to implement adequate electronic security mechanisms. As is discussed below, these developments should emphasize that it is not enough to merely adopt security policies. Implementation and integration of electronic security measures into the daily operations of the health care provider are necessary to avoid regulatory penalties and legal action resulting from identity theft.

Red Flag Rules

Effective May 1, 2009¹, the FTC is requiring 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.

The second, 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” which indicate the possible existence of identity theft. The FTC has confirmed that hospitals meet the definition of “Creditor” because hospitals defer payment for services and allow patients to enter into payment plans. By this analysis other health care facilities and 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 therefore, 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

¹ The original deadline was November 1, 2008, but that deadline was recently delayed until May 1, 2009.

continued...

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. Nevertheless, it is not enough to merely have a HIPAA privacy or security program and policies, new policies and/or revisions to existing policies are required. We can assist you in preparing the documents necessary to comply with these Red Flag requirements.

CMS Assesses Penalty in HIPAA Security Audit

Finally, CMS and HHS have extracted their first 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 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, covered entities need to continuously monitor the details of their execution, and ensure that these efforts include effective privacy and security staffing, employee training and physical and technical features.

* * * * *

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 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 mailing 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.