FOULSTON SIEFKIN LLP

ATTORNEYS AT LAW

www.foulston.com

Overland Park Topeka Wichita

HEALTH LAW FOULSTON SIEFKIN ISSUE ALERT

HHS Issues HITECH Guidance

April 20, 2009

Scott Palecki
spalecki@foulston.com
316.291.9578

Marta Fisher Linenberger
mlinenberger@foulston.com
785.233.3600

On Friday, April 17, 2009, the Secretary of Health and Human Services issued new guidance on the protection of health information which every HIPAA covered entity and business associate should review. The guidance was mandated by the American Recovery and Reinvestment Act of 2009 ("ARRA") and compliance will enable covered entities and business associates to avoid public security breach notifications.

President Obama signed the "ARRA" into law on February 17, 2009. One essential component of the ARRA is designed to stimulate development and use of electronic health records. Title XIII of the ARRA (Sections 13001-13424) or HITECH (Health Information Technology for Economic and Clinical Health Act) includes financial incentives for certain health care providers who adopt electronic records systems and imposes various obligations related to the privacy and security of electronic health records. One obligation is to utilize technologies and methodologies to protect the electronic transmission of health information from incursion from unintended sources. The information must be made unusable, unreadable or indecipherable to the unauthorized. The Secretary of HHS was charged with issuing guidance specifying acceptable technologies for this purpose on or before April 17, 2009. On Friday the Secretary issued the following: HITECH Act Breach Notification Guidance and Request for Public Comment. The Guidance is published on the HHS Office of Civil Rights website.[1] It is effective April 17, 2009, and applies to security breaches occurring 30 days after publication of the interim final regulation. The regulations are due to be issued by August 17, 2009.

The Guidance describes steps covered entities and business associates can take to secure health information. As with most of the HITECH provisions the utilization of the technologies and methodologies described in the Guidance is a "carrot". Use of the technologies described in the Guidance is the equivalent to a "safe harbor" for federal HITECH (not State) breach notification regulations. The "stick" is that unsecured health information that is breached warrants notification to the patient or, in some circumstances, the public.

Section 13402 of the HITECH Act imposes *breach* notification requirements on HIPAA covered entities and business associates following discovery of a breach of *unsecured* protected health information.[2] *Unsecured protected information* means PHI that is not secured through the use of a technology or methodology specified by the Secretary. A *breach* is the "...unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." Two exceptions to *breach* are also defined. The exceptions are: (1) the unintentional unauthorized acquisition, access or use of PHI by an employee (or person acting under the authority of the covered entity or business associate) if occurring in good faith and within the scope of employment, and if the PHI is not further acquired, accessed, used or disclosed; and (2) an inadvertent disclosure by a person who is authorized to access PHI to another similarly situated person at the same facility as long as the PHI is not further acquired, accessed, used or disclosed without authorization.

The Guidance notes that it is not addressing the use of de-identifying PHI as a

[1] View the HITECH Breach Notification Guidance and Request for Public Comment by **clicking here**.

[2] Kansas also has a Security Breach Notification law, codified at K.S.A. 50-7a01 *et seq.*

Continued on Page 2

methodology for rending it unusable, unreadable or indecipherable to unauthorized persons because de-identified PHI is no longer considered PHI. Limited data sets are addressed in the context of whether the limited data set is vulnerable or whether it should be inherently considered unusable, unreadable or indecipherable for the purposes of breach notification. This concern arises because limited data sets are not completely de-identified. HHS is requesting comments be directed to this issue.

The Guidance does not address how to prevent privacy and security breaches - those issues are covered under the general HIPAA Privacy and Security Rules. Vulnerabilities to breaches should be discovered and addressed through the covered entity's Security Rule Risk Analysis. The Guidance only addresses how PHI should be made unusable, unreadable, or indecipherable.

HHS identified two methods of protection: encryption and destruction suitable for "data in motion", "data at rest", "data in use" and "data disposed". HHS warns that these methods and technologies are not simply illustrative. HHS additionally cautions that the successful use of encryption depends upon the strength of the algorithm and the security of the decryption key or process. The use of the technologies specified includes the condition that the processes or key used for decryption have not been breached and are secured. The assumption follows that if this condition is not met, then the safe harbor is not available.

1. Encryption:

Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. Encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption for End User Devices.*

Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs* and may include others which are FIPS 140-2 validated.

2. Destruction:

Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise reconstructed.

Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitation* such that the PHI cannot be retrieved.

Covered entities and business associates should consult with their Security Officer and Information Technology Department to ascertain whether they are in compliance with the encryption and destruction standards set forth in the Guidance. If not, a move toward implementation and compliance is recommended. Further, methods of securing decryption processes and keys should be developed and implemented.

For Further Information

Foulston Siefkin's health care lawyers maintain a high level of expertise regarding federal and state regulations affecting the health care industry. The firm devotes significant resources to ensure our attorneys remain up-to-date on daily developments. At the same time, the relationship of our health care law practice group with Foulston Siefkin's other practice groups, including the taxation, general business, labor and employment, and commercial litigation groups, enhances our ability to consider all of the legal ramifications of any situation or strategy. If you are interested in additional information regarding these matters, please visit our website at **www.foulston.com** or if you would like to discuss specific ways in which Foulston Siefkin can help you can contact **Scott Palecki** at (316) 291-9578, or spalecki@foulston.com or **Marta Linenberger** at (785) 233-3600 or mlinenberger@foulston.com.

####