

## HIPAA goes HITECH with Substantial Civil Money Penalties

3/25/2011

By ALAN S. WERNICK, ESQ.

T: 847.786.1005 – E: [ALAN@WERNICK.COM](mailto:ALAN@WERNICK.COM)

Privacy protection is important in all businesses, including both for-profit and not-for-profit businesses. In recent developments substantial civil money penalties have been assessed against privacy violators in the health care industry. One of the fines was for \$4.3 million against one medical facility, and another was a \$1 million fine against a different hospital.

Perhaps you have heard anecdotal stories about the neighborhood intersection where neighbors start to notice that increased traffic through the intersection presents increased risks to children and others in the area. The neighbors complain to the local governing authority, but nothing happens until a few significant personal injuries occur in the intersection, and only then traffic signals are installed or law enforcement begins more closely monitoring the intersection. Whether or not those anecdotal stories are true, in some organizations, large and small, the approach to privacy is often like that hypothetical intersection—an accident waiting to happen.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act and amended the penalty amounts established under HIPAA, combine to form a strong statutory foundation for organizations handling health care information to pause and give serious consideration (and resources) to prevent privacy violations.

A review of the Department of Health & Human Services (HHS) Oct. 20, 2010, and Feb. 4, 2011, letters to Cignet Health Center (Cignet) in Maryland present an unfortunately all too common response that some businesses take towards privacy—the classic ostrich (i.e., head in the sand, avoidance) strategy. Consider the following partial excerpts from the [Oct. 20, 2010, Notice of Proposed Determination](#) letter from the Office for Civil Rights in HHS to Cignet:

“4. Cignet did not respond to the 41 individuals ... who requested copies of their medical records maintained by Cignet.

7. Cignet did not respond to OCR's written notification of the investigations, numerous follow-up attempts to contact Cignet by telephone, or to two subsequent letters ... informing Cignet of its obligation at 45 C.F.R. §164.524 to provide the individuals access to obtain a copy of the protected health information about them in the designated record sets (medical records) maintained by Cignet.

10. On June 26, 2009, OCR issued a subpoena duces tecum directing Cignet to produce the medical records of the individuals in the first group of 11 complaints by no later than July

27, 2009. The subpoena was delivered to Cignet by United States Postal Service certified mail, return receipt requested, and was received by Cignet's agent on June 29, 2009.

11. Cignet failed to produce the medical records as directed in the subpoena and failed to respond to OCR in any way regarding the June 26, 2009 subpoena.

14. On February 4, 2010, through the representation of the Department of Justice, Civil Division, Federal Programs Branch, OCR filed a petition to enforce its subpoena duces tecum in the United States District Court for the District of Maryland .... The Court issued an order for Cignet to show cause and scheduled a hearing for March 29, 2010. Cignet did not appear at the hearing, did not respond to the petition and did not defend the action.”

The OCR Notice of Proposed Determination further informed Cignet of the proposed civil money penalties (“CMP”) of \$4,351,600 and Cignet’s right to a hearing. As the Feb. 4, 2011, [OCR Notice of Final Determination to Cignet](#) states, Cignet failed to request the hearing or file an appeal. Thus, the civil money penalty was final.

The Feb. 22, 2011, HHS news release states, “Covered entities and business associates must uphold their responsibility to provide patients with access to their medical records, and adhere closely to all of HIPAA’s requirements,” said OCR Director Georgina Verdugo. ‘The U.S. Department of Health and Human Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules.’”

As privacy violations continue to increase both in the health care and other industries, enforcement efforts will increase. As these violations approach a tipping point, more federal and state agencies will enforce the law against violators, and more civil money penalties will be imposed.

The bottom line is that all businesses today need to be proactive stewards of data subject to privacy laws, and seek knowledgeable counsel in dealing with information technology law and data privacy law issues.