# HHS Imposes Penalty for Breach of HIPAA Security Standards Related to Online Application Database

**July 17, 2013**

On July 8, 2013, the U.S. Department of Health and Human Services (HHS) executed a Resolution Agreement with Wellpoint, Inc., a managed care company, and imposed a penalty of $1.7 million against the Company for violations of the privacy and security provisions of HIPAA. This penalty is one of the largest penalties to be imposed under HIPAA within recent years.

The HHS Office of Civil Rights (OCR) initiated an investigation of Wellpoint in response to a data breach report filed by Wellpoint. OCR concluded that Wellpoint had violated HIPAA based on the company's failure to (1) implement policies and procedures for access to electronic protected health information (ePHI) in an online database; (2) conduct an adequate evaluation of its technical safeguards after a software upgrade was installed; and (3) maintain adequate technical safeguards to protect the ePHI maintained in an online database. As a result, OCR found that Wellpoint had inappropriately disclosed personal information—including name, date of birth, address and social security number—for over 612,000 individuals.

The Wellpoint investigation highlights the importance of implementing the physical, administrative and technical safeguards required by the security provisions of HIPAA and the policies and procedures necessary to ensure that the safeguards are put in place. As more and more business is conducted through on line applications and web-based portals, the technical safeguards become the key to protecting individual personal health information. In addition, the technical safeguards must be designed to allow the secure collection and retention of personal health information through web-based systems, verification of the authenticity of those seeking access to these systems, and protection against inappropriate access, use, and disclosure of the information.

The Wellpoint case, similar to the 2012 settlements with Blue Cross Blue Shield of Tennessee and Phoenix Cardiac, P.C., illustrates the importance of reassessing administrative and technical safeguards any time you have operational changes or your information technology software or hardware systems are upgraded. Companies should regularly review, revise and update privacy and security policies and procedures and conduct employee trainings to ensure compliance with HIPAA.

If you have questions or would like additional information, please contact **Kathrin Kudner** at 734-214-7697, kkudner@dykema.com or **Joanne Lax** at 248-203-0816, jlax@dykema.com.



## Practice Areas

Health Care

HIPAA—Health Information Privacy & Security

Hospitals and Health Care Systems