

May 20, 2010

HHS Issues Guidance on Risk Analysis Required by HIPAA Security Rules

The U.S. Department of Health and Human Services (HHS) has issued draft Guidance on Risk Analysis for covered entities and business associates. This guidance was issued, in part, to fulfill HHS's mandate under the Health Information Technology for Economic and Clinical (HITECH) Act to provide annual guidance on the most effective and appropriate technical safeguards for carrying out the HIPAA Security Rule standards. The draft Guidance on Risk Analysis is the first of a series of guidances that HHS will issue under the mandate.

Risk analysis is one of the four required implementation specifications under the HIPAA Security Rule's security management process standard. Importantly, the draft Guidance explains several elements that risk analysis "must incorporate." Briefly, these elements are:

- Sufficient scope to encompass all e-PHI that is created, received, maintained or transmitted by the organization, regardless of the electronic media;
- Identification of where e-PHI is stored, received, maintained or transmitted;
- Identification and documentation of reasonably anticipated threats to e-PHI and vulnerabilities that create risks for the security of e-PHI;
- Assessment and documentation of current security measures used to safeguard e-PHI;
- Assessment of potential risks to the confidentiality, availability and integrity of e-PHI;
- Assessment of the magnitude of the potential impact resulting from a threat or vulnerability that affects the confidentiality, availability and integrity of e-PHI;
- Assignment of risk levels for all threats and vulnerability combinations identified;
- Documentation of the risk analysis; and
- Periodic review and update of the risk analysis.

The draft Guidance on Risk Analysis also includes definitions of vulnerability, threat and risk, terms that are used, but not defined, in the HIPAA security standards. These definitions are based on, or adapted from, the definitions of those terms in National Institute of Standards and Technology (NIST) publications.

The draft Guidance on Risk Analysis is available at:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf>

For more information, please contact your Katten Muchin Rosenman LLP attorney, or:

Megan Hardiman

312.902.5488 / megan.hardiman@kattenlaw.com

Sheila Sokolowski

312.902.5456 / sheila.sokolowski@kattenlaw.com

www.kattenlaw.com

CHARLOTTE

CHICAGO

IRVING

LONDON

LOS ANGELES

NEW YORK

WASHINGTON, DC

Published as a source of information only. The material contained herein is not to be construed as legal advice or opinion.

©2010 Katten Muchin Rosenman LLP. All rights reserved.

Circular 230 Disclosure: Pursuant to regulations governing practice before the Internal Revenue Service, any tax advice contained herein is not intended or written to be used and cannot be used by a taxpayer for the purpose of avoiding tax penalties that may be imposed on the taxpayer. Katten Muchin Rosenman LLP is an Illinois limited liability partnership including professional corporations that has elected to be governed by the Illinois Uniform Partnership Act (1997). London affiliate: Katten Muchin Rosenman Cornish LLP.