

HIPAA Omnibus Rule Will Require Contract & Policy Changes

On Jan. 25, 2013, the U.S. Department of Health and Human Services (HHS) published an omnibus rule that made significant changes to HIPAA privacy and security regulations. Key provisions expanded compliance obligations beyond covered entities to directly apply to their business associates and subcontractors, changed the definition of breach, and stiffened non-compliance penalties.

Privacy & Security Rules

Under the HIPAA Omnibus Final Rule related to the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and the Genetic Information Non-Discrimination Act of 2008 (GINA), business associates and their subcontractors may be held **directly accountable** for their conduct. They must comply with the limitations on disclosure of Protected Health Information (PHI) and ensure that required administrative, physical and technical safeguards are put in place. Business associate agreements now must require that the business associate comply with the HIPAA Security Rule obligations. Agreements between business associates and their subcontractors must also comply with the requirements for business associate agreements and may not permit the subcontractor to engage in any activities impermissible for a business associate.

The new rules explicitly define business associate as health information organizations, e-prescribing gateways, or other persons that provide data transmission services with respect to PHI and that require access to such information on a routine basis; a person

that offers a personal health record to one or more individuals on behalf of a covered entity; and any subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate.

Business associate agreements and internal policies and procedures should be carefully reviewed for compliance. Relationships with other contractors and subcontractors should also be reviewed as they might now need to meet the requirements for business associate agreements. The Center for Medicare and Medicaid Services (CMS) may now audit covered entities or business associates and will investigate complaints regarding non-compliance. If agreements and internal policies are found to be noncompliant significant monetary penalties may be imposed.

Breach Notification Rule

The new rules amend the “significant risk of financial, reputational, or other harm” standard to more clearly state that breach notification on the part of a covered entity or business associate is the expected norm rather than the exception in the case of breaches of PHI. The rules preserve the existing exceptions, but any other acquisition, access, use, or disclosure of



unsecured PHI not permitted under the rules is **presumed to be a breach** unless the covered entity or business associate demonstrates there is a low probability the PHI has been compromised. “Low probability” is determined through an assessment of the nature and extent of the PHI involved; the unauthorized person who used the PHI or to whom it was disclosed; whether the PHI was actually acquired or viewed; and the extent to which the risk to the PHI has been mitigated.

Non-Compliance Sanctions

This rule now incorporates the tiered civil money penalty structure set forth in the HITECH Act that sets fines for noncompliance according to three levels of culpability: offenses rising in the case of “reasonable cause,” “reasonable diligence,” or “willful neglect.” The rule establishes that covered entities as well as business associates can be held liable for non-compliant actions and can be held liable for the actions of their agents. Civil money penalties of up to **\$50,000** per incident totaling up to **\$1.5 million** per year may be imposed on entities found to be in violation of the rule. Failure to bring agreements and policies into compliance could potentially lead to significant penalties.

Other Provisions

The omnibus rule also:

- affords individuals the right to receive an electronic copy of their health information from a covered entity;

- allows individuals to restrict disclosure of certain PHI to health plans in cases where the individual pays for services from a covered entity;
- prohibits most health plans from using or disclosing genetic information for underwriting purposes;
- redefines marketing activities and establishes parameters within which PHI may be used in those activities;
- allows parents to verbally authorize a covered entity to disclose proof of immunization to schools; and
- clarifies the application of the rules to the health care units of “hybrid entities.”

Next Steps & Action Items

The rule has significant implications for covered entities and business associates, and both should carefully examine the implications of these changes with respect to current operations.

Action items:

- revise business associate agreements to bring into compliance;
- review any other relationships with contractors that relate to PHI that might now require a business associate agreement;

- review and amend internal policies and procedures as needed; and
- retrain personnel with regard to new requirements under the rules.

The final rule will be effective March 26, 2013 and establishes a compliance date of Sept. 23, 2013. Agreements that are compliant under the old rules and entered into before Jan. 25, 2013 can be relied on until Sept. 23, 2014. However, if such an agreement is renewed after March 26, 2013, it must comply with the new rule. Agreements entered into after Jan. 25, 2013 will need to be compliant by Sept. 23, 2013.

For additional information, contact:

*Jonathan M. Joseph
Christian & Barton, LLP
909 East Main Street, Suite 1200
Richmond, Virginia 23219
jjoseph@cblaw.com
804.697.4125*

Case results depend on a variety of factors unique to each case and results do not guarantee or predict a similar result in any future case undertaken. This article is provided as an informational service and does not constitute legal counsel or advice, which can only be rendered in the context of specific factual situations. If a legal issue should arise, please contact the attorney listed in this article or retain the assistance of other competent legal counsel.

**ADVERTISING
MATERIAL**