April 4, 2013

The Granade Law Firm

Dedicated to Counseling the Health Care Industry Regarding Privacy and Security Laws

HIPAA Alert #2: Changes to the Breach Regulations

The new HIPAA Final Rule was promulgated by the U.S. Department of Health and Human Services (HHS) on January 25, 2013. While the Final Rule brings tremendous change to the HIPAA privacy and security regulations, this alert – the second in a series – focuses on the impact of the Final Rule on covered entities' and business associates' obligations to identify and respond to the breach of protected health information ("PHI"). The "compliance deadline" for the data breach provisions of the new HIPAA Final Rule is September 23, 2013. All policy and procedure revisions must be adopted by this date, and workforce member training concerning the newly revised policies and procedures also must be completed prior to September 23, 2013.

Definition of Breach Expanded; Burden of Proof Shifted

1. The Final Rule expands the definition of "breach" to clarify that an impermissible use or disclosure of PHI is now presumed to be a breach unless the covered entity or business associate that experienced the breach demonstrates that there is a low probability that the PHI has been compromised. *See* 78 Fed. Reg. at 5641. The impact of this change is two-fold:

    a. Notification to individuals is required unless the covered entity or business associate experiencing the breach can demonstrate that there is "a low probability that the PHI has been compromised." Under the Final Rule, rather than assessing harm to determine if a Breach occurred, a covered entity or business associate must *presume* each impermissible use or disclosure of PHI is a Breach unless an exception applies[1] or there is a low probability that PHI has been compromised as determined through a risk assessment", and

    b. The burden of proof that the PHI was not compromised falls squarely on the covered entity and/or business associate. Realistically, the burden falls most heavily on the covered entity, since notification of a breach by a business associate will cause the covered entity to initiate an investigation, and if the covered entity agrees a breach occurred, comply with the Rule's requirements to notify, mitigate and remediate.

2. The Final Rule eliminates the "no significant risk of harm to the individual" standard and replaces it with "a low probability that PHI has been compromised" standard for use when determining if a Breach occurred. See below, New Risk Assessment Method.

[1] The Final Rule adopted the exceptions in the Interim Final Rule. Specifically, acquisition, access, use or disclosure of PHI is not a breach if: 1) it was deemed unintentional, or a good faith acquisition, access or use of PHI by a workforce member within the scope of authority; 2) there is an inadvertent disclosure by an authorized person to another authorized person within the same entity or organized health care arrangement; or 3) the disclosure to an unauthorized person occurs and there is a good faith belief that the person would not reasonably have been able to retain the information. Note that the Final Rule removes the exception to notification if the PHI at issue consists of a limited data set that excludes dates of birth and zip codes.

New Risk Assessment Method: Determining If PHI Compromised

The Final Rule identifies four objective factors, below, that covered entities and business associates (CEs and BAs) must consider when performing a risk assessment to determine if PHI has been compromised (i.e., breached). *See* 78 Fed. Reg. at 5642, 45 C.F.R. Section 164.402. The risk assessment must be documented, regardless of the outcome (i.e., breach or no breach), and retained for at least six years following the incident.

Factor #1: *The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification*. The goal of this element of the risk assessment is to help entities determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or to further the recipient's own interests. This factor requires CEs/BAs to evaluate the nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification. In assessing this element of the test, the CE/BA should consider the "sensitivity" of the PHI. For example, information subject to identity theft, such as credit card number or social security number likely would be considered sensitive information. Regarding clinical information, such as medication lists and test results, not only the nature of the services but also the volume of the information should be considered.

Factor #2: *The unauthorized person who used the PHI or to whom the disclosure was made*. In assessing this factor, the CE/BA should consider whether the person who received the PHI has an obligation to protect the privacy and security of the information. For instance, information disclosed to another CE may result in a lower probability that PHI has been compromised because the CE is also obligated to protect PHI. If the information impermissibly used or disclosed is not immediately identifiable, the CE/BA also must consider whether the recipient has the ability to re-identify the information.

Factor #3: *Whether the PHI was actually acquired or viewed*. For this factor, the CE/BA will need to assess the extent to which the PHI was acquired or viewed. For example, a forensic analysis of a stolen laptop may indicate that the PHI was never accessed or viewed.

Factor #4: *The extent to which the risk to the PHI has been mitigated*. With respect to this factor, a CE/BA will need to consider the extent to which the risk to the PHI has been mitigated. This may include obtaining the recipient's satisfactory assurances that the information will not be further disclosed or will be destroyed. Clearly, consideration of factor number four ties closely with factor number two.

Breach Notification Obligations and Compliance Deadlines:

1. In comments to the Final Rule, HHS reminded CEs that the breach notification obligation solely belong to CEs, even if the breach is experienced by the BA.
2. The breach notification requirements remained largely unchanged in the Final Rule. Covered entities are required to provide breach notification to the affected individuals without unreasonable delay and in no event later than sixty (60) days following discovery of the breach.
3. The Final Rule changes became effective on March 23, 2013; however, the compliance deadline is September 23, 2013.

Role of Business Associates in Data Breaches:

1. Consistent with HITECH, the Final Rule provides that BAs are directly liable for compliance with all of the HIPAA security regulations, and many of the HIPAA privacy and security regulations, including:

a. Impermissible uses and disclosures of PHI;

b. Failure to provide breach notification to the covered entity;

c. Failure to comply with minimum necessary standards;

d. Failure to enter into business associate agreements with subcontractors that create or receive a covered entity's PHI on behalf of the BA; and

e. Failure to comply with the administrative, physical and technical safeguard implementation specifications of the HIPAA security regulations.

2. The Final Rule adds a vicarious liability component for CEs and BAs to consider if the BA/subcontractor is acting as an agent. CEs are liable under the Final Rule for violations resulting from the acts or omissions of a BA if that BA is an agent of the CE; similarly, BAs are liable for violations resulting from the acts or omissions of a subcontractor if that subcontractor is an agent of the BA and the subcontractor is acting within the scope of that agency arrangement. *See* 78 Fed. Reg. at 5581.

3. Please refer to our ***Alert #1: Business Associates*** for more information.

Practical Implications for Covered Entities and Business Associates:

1. Breach notification policies and procedures should be updated to reflect changes in the definition of Breach.

2. PHI that is identified as "unsecured" should be evaluated to determine whether the unsecured PHI can be made secure using approved technologies and methodologies (e.g., encryption, which can render data unusable, unreadable, and indecipherable to unauthorized persons and thereby demonstrating a low probability that the PHI was compromised).

3. Consider the impact that state laws may impose with respect to breach notification.

4. Train workforce members regarding the revised policies and procedures. Document all training.

5. Evaluate the "minimum necessary" standard in relation to all uses and disclosures of PHI, including those to BAs. The less PHI disclosed, the lower the risk a breach might occur.

6. Ensure that business associate agreements include clear language regarding responsibility and liability for breach notification obligations. HHS makes it clear that the parties, covered entity and business associate, or business associate and subcontractor – may add additional provisions to their business associate agreements, such as indemnification or reimbursement for costs/expenses related to a data breach.

7. Note: Indemnification and/or reimbursement provisions, as well as cyber liability/data breach insurance, should be considered with legal counsel's involvement.

The new HIPAA Final Rule made significant changes to the HIPAA breach regulations. Please let us know if we can assist your company with its compliance activities.

THE GRANADE LAW FIRM, LLC
1266 West Paces Ferry Road, Suite 204
Atlanta, Georgia 30327
(678) 705-2507

PHYLLIS F. GRANADE
pgranade@granadelaw.com

AJAY R. VYAS
avyas@granadelaw.com