Arnall Golden Gregory LLP

Client Alert

Contact Attorneys Regarding This Matter:

Jessica Tobin Grozine
404.873.8526 - direct
404.873.8527 - fax
jessica.grozine@agg.com

Keith A. Mauriello
404.873.8732 - direct
404.873.8733 - fax
keith.mauriello@agg.com

HIPAA Breach Notification Regulations— Sanctions No Longer Discretionary

On February 22, 2010, the U.S. Department of Health and Human Services (HHS) began enforcing penalties for violations of the breach notification regulations, as announced in the Interim Final Rule found at 74 Fed. Reg. 42,739, 42,757 (Aug. 24, 2009). As most healthcare providers and their attorneys are already aware, the Health Information Technology for Economic and Clinical Health (HITECH) Act resulted in the promulgation of new regulations, effective September 23, 2009, that require covered entities to provide notification to individuals, HHS and, in some instances, media outlets when there is a breach of unsecured protected health information (PHI).

When the breach notification regulations went into effect, HHS indicated that it would use its enforcement discretion to not impose sanctions for failing to provide the required notifications for breaches discovered before February 22, 2010. However, covered entities are still expected to comply with the breach notification regulations as of September 23, 2009, including reporting to HHS any breaches occurring between September 23 and December 31, 2009, and no later than March 1, 2010. Covered entities also must include in the following year's report to HHS all breaches occurring in 2010, including those discovered before February 22, 2010.

The breach notification regulations apply only when there is a breach involving "unsecured PHI." The term "unsecured PHI" is defined as PHI that has not been "rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology" approved by HHS (45 C.F.R. § 164.402). Thus, a breach of secured PHI maintained in accordance with HHS guidance would not trigger the notification requirements. Although at first glance it may seem easy to secure all PHI in accordance with HHS guidance, as a technical matter it will likely be challenging and cost prohibitive. As a result, many, if not all, covered entities and business associates will be subject to the new requirements.

Although the regulations are relatively straightforward with respect to the timing and content of the requisite notices, the initial determination as to whether an unauthorized disclosure of unsecured PHI constitutes a "breach" is a fact intensive analysis.

Arnall Golden Gregory LLP
Attorneys at Law
171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031
404.873.8500
www.agg.com

Is There A Breach? Risk Assessment

A "breach" is defined as "the acquisition, access, use, or disclosure of protected health information [...] which *compromises the security or privacy of protected health information*" (45 C.F.R. § 164.402) (emphasis added). The phrase "compromises the security or privacy of protected health information" is further defined in the regulations as posing "a *significant risk* of financial, reputational, or other harm to the individual" (*Id.*) (emphasis added). Although any unauthorized disclosure of PHI may be a violation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and may be subject to sanctions, not all unauthorized disclosures are considered breaches (i.e., posing a significant risk) that require notification to individuals whose information has been disclosed. Note that there are three narrow exceptions to the definition of breach found at 45 C.F.R. § 164.402(2).

This concept of "significant risk" is expounded upon in both the preamble to the breach notification regulations as well as other federal guidelines.[1] For instance, the preamble provides a concrete example to assist covered entities in understanding the parameters and in determining whether a violation of the HIPAA Privacy Rule constitutes a breach:

> [I]f a covered entity improperly discloses protected health information that merely included the name of an individual and the fact that he received services from a hospital, then this would constitute a violation of the Privacy Rule, but may not constitute a significant risk of financial or reputational harm to the individual. In contrast, if the information indicates the type of services that the individual received (such as oncology services), that the individual received services from a specialized facility (such as a substance abuse treatment program), or if the protected health information includes information that increases the risk of identity theft (such as social security number, account number, or mother's maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information.
>
> 74 Fed. Reg. at 42,745

Notification of Breach

Pursuant to 45 C.F.R. § 164.404(a), "[a] covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of such breach." The notice must be given to the affected individuals "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach" (45 C.F.R. § 164.404(b)). Business associates are also required to report breaches of unsecured PHI to their covered entities. (See 45 C.F.R. § 164.410.)

1 The preamble to the breach notification rule references a 2007 Memorandum (M-07-16) issued by the Office of Management and Budget, which provides "examples of the types of factors that may need to be taken into account in determining whether an impermissible use or disclosure presents a significant risk of harm to the individual." (OMB Memo 07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information").

A breach is treated as discovered on the day the entity first knew or, with reasonable diligence, should have known about the breach. The regulations contain specific requirements pertaining to the content of individual notifications, including, but not limited to, the date of the breach, the information disclosed, a contact person at the covered entity and efforts to mitigate harm. (See 45 C.F.R. § 164.404(c).)

Covered entities must also notify HHS of any breach of unsecured PHI. If a single breach involves 500 or more individuals, the covered entity is required to report to HHS at the same time the covered entity notifies affected individuals and in the manner specified on the HHS website. If a single breach of unsecured PHI affects fewer than 500 individuals, the covered entity must maintain a log and report the breach to HHS on an annual basis within 60 days of the end of the calendar year and in the manner specified on the HHS website. (See 45 C.F.R. § 164.406.) HHS has published an online reporting form, which can be found here.[2]

In the event there is a single breach involving more than 500 residents of one state, the covered entity must notify prominent media outlets serving that state without unreasonable delay and no later than 60 days after discovery of the breach. The media notification must contain the same information required in the individual notification. (See 45 C.F.R. § 164.406.)

Conclusion

It is important for covered entities, business associates, and their counsel to become familiar with the breach notification regulations if they have not already done so. While many covered entities may have established procedures following the September 23, 2009, effective date of the regulations, it is imperative at this time to ensure that the regulations and related policies are completely understood now that HHS will start to impose sanctions for failing to provide the required notifications as of February 22, 2010. HHS seemed to be somewhat lenient in delaying enforcement, but the grace period has come to pass and it is time to make certain the breach notification regulations are being followed.

2 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html