



Upcoming Annual Deadline for HIPAA Breach Reporting: February 29, 2016

H. Carol Saul and Madison M. Pool

HIPAA covered entities should note the looming February 29, 2016 reporting deadline for breaches of unsecured protected health information that occurred in 2015 and involved fewer than 500 individuals. This Alert provides a summary of the legal requirements related to reporting such breaches.

I. Background

HIPAA requires covered entities to notify the Secretary of the U.S. Department of Health and Human Services (the Secretary) following the discovery of a breach of unsecured protected health information (PHI).¹ All covered entities should be alert to the likelihood of such a breach occurring and to the attendant reporting requirements. Breaches happen with marked frequency and to covered entities of all sizes. Even a cursory review of the Secretary's website listing "Breaches Affecting 500 or More Individuals" reveals that new entries are posted weekly if not daily.² Data on breaches involving fewer than 500 individuals is less readily available, but experience and sources suggest they occur in even greater numbers than those above the 500 individual threshold.³ A misdirected fax or medical record involving even a single patient's PHI must be reported to the Secretary.

II. Reporting Requirement

There are different timing requirements for reporting breaches involving fewer than 500 individuals versus those involving 500 or more individuals.⁴ For breaches of unsecured PHI that involve fewer than 500 individuals, HIPAA requires a covered entity to maintain a log or other documentation of such breaches and to notify the Secretary no later than 60 days after the end of the calendar year in which such breaches were discovered.⁵ (Keep in mind that the requirement to notify the Secretary is separate from the requirement to notify individuals of a breach of their unsecured PHI, which involves different timelines and additional requirements.)⁶ For breaches of unsecured PHI discovered in 2015 and involving fewer than 500 individuals, the deadline to notify the Secretary is February 29, 2016.

A breach is considered "discovered" as of the first day on which the breach is known to the covered entity, or would have been known by exercising reasonable diligence.⁷ Knowledge of the breach will be imputed to the covered entity if any workforce member or agent of the covered entity (other than the person committing the breach) knows of the breach or would have known by exercising reasonable diligence.⁸

¹ 45 C.F.R. § 164.408(a).

² U.S. Dept. of Health & Human Services, *Breaches Affecting 500 or More Individuals*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Feb 10, 2016).

³ See, e.g., U.S. Department of Health and Human Services Office for Civil Rights, *Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2011 and 2012 at 18*, available at <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf>.

⁴ 45 C.F.R. § 164.408

⁵ 45 C.F.R. § 164.408(c).

⁶ 45 CFR § 164.404.

⁷ 45 CFR § 164.404(a)(2).

⁸ *Id.*

Covered entities are also responsible for logging and notifying the Secretary of breaches that are discovered by their business associates and reported to the covered entity.⁹ Although HIPAA establishes the general requirement to report breaches of unsecured PHI to the Secretary, it does provide one narrow exception if “a law enforcement official states to a covered entity or business associate that [notification] would impede a criminal investigation or cause damage to national security.”¹⁰ In such a unique situation, some flexibility is afforded in the reporting requirement.¹¹

A covered entity is not required to wait until the deadline to report breaches, and may report prior to the deadline after a breach is discovered if the covered entity so chooses.¹² In addition, the Secretary has posted guidance on its website stating that a covered entity “may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity must complete a separate notice for each breach incident.”¹³ If the covered entity is unsure of the number of individuals affected at the time it submits the notification to the Secretary, the Secretary has clarified that “the covered entity should provide an estimate, and, if it discovers additional information, submit updates” as discussed below.

III. Reporting Procedures

The Secretary maintains a web portal and requires that the portal be used for the submission of all breach notifications required to be submitted to the Secretary.¹⁴ The link for the web portal is provided at the end of this Alert, as is a link to a website summarizing the process for submitting notice of a breach to the Secretary for both categories of breach reports (i.e. those involving fewer than 500 individuals and those involving 500 or more individuals).

The web portal may be used to submit an “Initial Breach Report” or an “Addendum to Previous Report.”¹⁵ The Secretary’s website explains that if the covered entity “discovers additional information that supplements, modifies, or clarifies a previously submitted notice,” the covered entity may submit an Addendum to the previously filed Initial Report, using the transaction number provided for each initial breach report submitted after January 1, 2015.

Thus, covered entities should be prepared to submit notice to the Secretary through the web portal no later than February 29, 2016 of any breach of unsecured PHI discovered in 2015 which involved fewer than 500 individuals.

While this Alert focuses on the upcoming February 29, 2016 deadline for reporting breaches affecting fewer than 500 individuals, covered entities should also be aware of the differences in reporting a breach affecting 500 or more individuals. These differences include required reporting to the Secretary no later than 60 calendar days after discovery of a breach, being listed on the Secretary’s website of “Breaches Affecting 500 or More Individuals,” and possibly having to notify the media of the breach.¹⁶

IV. Links

[Web Portal](#)

[Submitting Notice of a Breach to the Secretary](#)

[Breaches Affecting 500 or More Individuals](#)

⁹ See 45 CFR § 164.404(a)(1) and § 164.410(1).

¹⁰ 45 C.F.R. § 164.412.

¹¹ 45 C.F.R. § 164.412(a)–(b).

¹² U.S. Dept. of Health & Human Services, *Submitting Notice of a Breach to the Secretary*, <http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html> (last visited Feb 10, 2016).

¹³ *Id.*

¹⁴ *Id.*

¹⁵ Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true (last visited Feb 10, 2016).

¹⁶ U.S. Dept. of Health & Human Services, *Breaches Affecting 500 or More Individuals*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Feb 10, 2016); 45 C.F.R. 164.406; 45 C.F.R. 164.408(b).

Authors and Contributors

H. Carol Saul

Partner, Atlanta Office
404.873.8694
carol.saul@agg.com

Madison M. Pool

Associate, Atlanta Office
404.873.8514
madison.pool@agg.com

not *if*, but *how*.[®]

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a “business sensibility” approach, developing a deep understanding of each client’s industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal’s prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief “not if, but how.” Visit www.agg.com.

Atlanta Office

171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office

1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: <http://www.agg.com/subscribe/>

©2016. Arnall Golden Gregory LLP. This legal insight provides a general summary of recent legal developments. It is not intended to be, and should not be relied upon as, legal advice. Under professional rules, this communication may be considered advertising material.