Privacy HIPAA Update: Changes to Notice of Privacy Practices and New Requirements for Analyzing Breaches

H. Carol Saul, R. Michael Barry and Diane Lukin

HIPAA[1] compliance is an important part of every health care practice. The failure to provide a timely and compliant HIPAA Notices of Privacy Practices (NPP) or recognize when your health care practice may have a possible breach of protected health information (PHI) under HITECH[2] may result in costly government investigations and penalties. To assist you with ensuring timely compliance, this article addresses the new NPP content and breach risk assessment standard adopted under the final Omnibus Rule issued on January 25, 2013 by the Department of Health and Human Services (HHS), which requires health care providers to bring their NPPs into compliance and change the manner in which they analyze PHI breaches on September 23, 2013.

Notices of Privacy Practices

To assist health care providers with updating their NPPs, the following provides practical pointers on what health care providers need to do to bring their NPPs into compliance with the 2013 Omnibus Rule. Also addressed are the changes that are required for handling of the NPP. In addition to revising their NPPs, health care providers should also review and revise any HIPAA compliance policies and training materials that address the requirements for content and dissemination of NPPs. The eight changes that the 2013 Omnibus Rule requires for the content of NPPs are:

1. The NPP must include a description of the types of uses and disclosures which require an authorization in the following three areas: i) disclosure of psychotherapy notes ii) disclosures for marketing purposes and iii) disclosures that constitute a sale of PHI. The NPP also must state that other uses and disclosures not described in the NPP will not be made unless an individual provides an authorization and that authorizations may be revoked prospectively at any time by written revocation.

2. The NPP must explain the right of an individual to restrict disclosures of PHI to a health plan for payment or health care operation purposes (but not for treatment purposes) for items or services which an individual has paid for in full and out-of-pocket. Providers will also need to adopt some method to flag in the record any such mandatory restrictions.

3. If a provider intends to use PHI for fund-raising purposes, it must inform the individual of such intent and of the individual's right to opt out of receiving fundraising communications.

4. The NPP must inform the individual of the right to be notified following a breach of the individual's unsecured PHI.

5. The NPP must advise the individual that PHI may not be sold without the individual's express written authorization.

6. One prior requirement for NPPs has been removed: NPPs should no longer include a statement that the provider may send communications regarding treatment alternatives or health-related products or services if the provider is paid by a third party to make the communication. This change is due to the fact that the Omnibus Rule treats subsidized treatment communications as marketing

1 Health Information Portability and Accountability Act of 1996.
2 Health Information Technology for Economic and Clinical Health Act of 2009.

and requires an individual's authorization before such communications can be made.

7. A health care provider who maintains a physical service delivery site must make the NPP available at the site for individuals to take with them, and also must post the NPP in a "clear and prominent" location where individuals will be able to read it.
8. When an NPP is revised – as it must be by September 23, 2013 – a health care provider is not required to mail out the new NPP, but rather to make the new NPP available to individuals upon request on or after the effective date of the revision, and to follow Step 7 above, if applicable. Of course, any new patient encounter after revision will require delivery of the revised NPP and an attempt to have the patient acknowledge receipt of the revised NPP.

The New HITECH Breach Risk Assessment Standard

Recognizing and evaluating when a breach of PHI may exist can be invaluable to your health care practice. To assist you in making these assessments, this section reviews the 2013 Omnibus Rule's modifications to the definition of breach and the risk assessment standard originally adopted under HITECH and implemented under the HHS interim final rule effective September 23, 2009 (the 2009 Interim Final Rule). The following explains the former and new risk assessment standard so that you understand how it makes a difference in analyzing possible and actual breaches of the PHI you handle. Health care providers must implement the 2013 Omnibus Rule's new risk assessment standard for breaches that occur on or after September 23, 2013.

Under both the 2009 Interim Final Rule and 2013 Omnibus Final Rule, the term "breach" means the impermissible acquisition, access, use or disclosure of unsecured PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of PHI.[3] If a breach occurred under the 2009 Interim Final Rule, health care providers were required only to determine and document whether there was a significant risk of financial, reputational, or other harm to the individual who was the subject of the PHI.

Unlike the 2009 Interim Final Rule, the 2013 Omnibus Rule deletes the significant risk of harm test. Instead, the risk assessment standard has been revised to include a four-prong test.

Under the 2013 Omnibus Rule, unless the health care provider can demonstrate there is a low probability that the PHI was compromised, a breach is presumed to have occurred. Therefore, the health care provider must complete the risk assessment analysis by considering the following four factors to determine if a breach occurred:[4]

1. The nature and extent of the PHI involved, including the types of individual identifiers included in the PHI and possibility of re-identification;

2. The unauthorized person who received the PHI;

3. Whether the PHI was actually acquired or viewed by an unauthorized person; and

4. The extent the health care provider, business associate, or other recipient mitigated the breach.

For purposes of the first factor, health care providers should consider any financial and clinical information involved. Sensitive financial information may include credit card numbers, Social Security numbers, or information that increases the individual's risk of identity theft and financial fraud. Clinically sensitive information may involve the type of medical services and/or detail of medical services that are impermissibly disclosed. The health care provider must consider

3 The 2009 Interim Final Rule and 2013 Omnibus Rule continue to exclude the following three types of incidents from the definition of breach: (1) unintentional access by an employees and others acting under the healthcare provider's authority, provided access was in good faith and within the scope of employment (or the professional relationship) (For purposes of the "good faith" standard, employee snooping would be in bad faith and not covered by this exception); (2) inadvertent disclosure between employees or persons authorized to access PHI at the same health care provider (e.g., an employee authorized to review a patient's general health status factors receives information on a patient's major medical treatment or condition); and (3) unauthorized disclosures to a person that would not reasonably be able to retain the information (e.g., an employee without authorization picks up a report with PHI but does not otherwise read it and the authorized employee retrieves the report).

4 The health care provider may also consider other factors as appropriate.

whether re-identification could occur based on the breach and the unauthorized person's access to the identifiers.

When analyzing the second factor, the health care provider should consider whether the unauthorized person also has an obligation to comply with the HIPAA Privacy and Security Rules and whether the unauthorized person has the ability to re-identify the individual to his or her PHI. For purposes of the third factor, whether the PHI was actually acquired or viewed will be based on the facts and circumstances of the unpermitted disclosure. The fourth prong requires consideration of whether appropriate action was taken to mitigate potential risk and damage due to the PHI being breached. Favorable consideration might include, for example, the unauthorized person, who is also subject to HIPAA, returning the PHI or agreeing to destroy it without replicating it before returning it. Other opportunities to mitigate any potential breach will depend on the facts and circumstances of the breach under the first three factors. In all situations, the health care provider must conduct a thorough, good faith analysis of potential risk. If the health care provider believes the PHI has been compromised, breach notification will be required.

Summary

Timely compliance with the 2013 Omnibus Rule requires health care providers to review their NPPs and use the new breach risk assessment standard beginning on or after September 23, 2013.

Authors and Contributors

H. Carol Saul
Partner, Atlanta Office
404.873.8694
carol.saul@agg.com

R. Michael Barry
Partner, Atlanta Office
404.873.8698
michael.barry@agg.com

Diane Lukin
Associate, Atlanta Office
404.873.8516
diane.lukin@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 Ave., NW,
Suite 1000
Washington, DC 20006

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