Arnall Golden Gregory LLP

Client Alert

Contact Attorneys Regarding This Matter:

Jennifer D. Burgar
404.873.8194 - direct
jennifer.burgar@agg.com

Neil W. Hoffman
404.873.8594 - direct
neil.hoffman@agg.com

Arnall Golden Gregory LLP
Attorneys at Law

171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031

Two South Biscayne Boulevard
One Biscayne Tower 2690
Miami, FL 33131

1775 Pennsylvania Avenue NW
Suite 1000
Washington DC 20006

www.agg.com

HHS Releases Final HIPAA Omnibus Rule: A Summary of the Changes

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) released its final omnibus rule to increase HIPAA privacy and security protections by implementing provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and Genetic Information Nondiscrimination Act of 2008 (GINA). Among these changes is an expansion of liability under the HIPAA Privacy and Security Rules to business associates of covered entities and to subcontractors of business associates. The final omnibus rule also increases penalties for noncompliance based on levels of negligence, with a maximum annual cap of $1.5 million for violations of identical standards. The final omnibus rule also changes the standard under HITECH Breach Notification requirements for determining whether there has been a breach of unsecured protected health information. The new standard will make it harder to rationalize that no breach has occurred. The final omnibus rule also expands certain individual rights under HIPAA.

- **Expansion of the Privacy and Security Rules with regard to Business Associates**

One of the more significant changes in the final omnibus rule is the modification of the definition of business associate to include subcontractors. Previously, if a business associate engaged a subcontractor to assist in the performance of the business associate's services, then the business associate merely had to "ensure" that the subcontractor would comply with the terms of the business associate's business associate agreement with the covered entity. The final omnibus rule expanded the definition of business associate to include directly such subcontractors. The definition of business associate was also revised to include health information organizations, e-prescribing gateways, and other entities that provide data transmission services and that require access to protected health information (PHI) on a routine basis, as well as entities that offer a personal health record product.

In addition to expanding the definition of business associate, the rule also made directly applicable to business associates many of the requirements of the privacy and security regulations. Whereas before, business associates were bound only by the terms of their business associate agreements, now business associates (the definition of which now includes subcontractors) must comply with parts of the regulations in their own right, and are subject to enforcement along with covered entities. This will require business

associates to implement HIPAA compliance initiatives and measures.

- **Other Modifications to the Privacy and Security Rules**

The final omnibus rule included several other noteworthy changes to the privacy and security regulations, including:

  - Sale of PHI. Under the final rule, a covered entity or business associate must obtain an authorization for any disclosure of PHI that would be considered a "sale" of PHI, and the authorization must expressly state that the disclosure is part of a sale. The "sale" of PHI means a disclosure of PHI by a covered entity or business associate in exchange for direct or indirect remuneration. There are a number of exceptions to this rule.

  - Individual Right to Limit Certain Disclosures of PHI to Health Plans. Previously, HIPAA permitted an individual to request restrictions on the disclosure of the individual's PHI, but the covered entity was not required to agree to implement the restriction. However, the final omnibus rule now requires a covered entity healthcare provider to agree to an individual's request to restrict disclosure of PHI to health plans under the following circumstances: (1) the request is to restrict disclosures to a health plan for payment or health care operations purposes; (2) the disclosure is not otherwise required by law; and (3) the PHI relates solely to a health care item or service for which payment has been made in full by the individual or a third party other than the health plan (e.g., the patient paid out of pocket.

  - Changes to the Notice of Privacy Practice. The final omnibus rule requires a number of changes to the Notice of Privacy Practices (Notice) published by covered entities. Notices must now include a general statement that the covered entity is required by law to notify affected individuals following a breach of unsecured PHI. The Notice must be revised to describe certain types of uses and disclosures that require an authorization, including disclosures of psychotherapy notes, marketing communications and the sale of PHI. The Notice must state that other uses and disclosures not described in the Notice will be made only with the individual's authorization. The Notice must make individuals aware that they can restrict certain disclosures to health plans (described above).

- **Change to the HITECH Breach Notification Rule**

The final omnibus rule makes important changes to the standard for determining whether there has been a breach of unsecured PHI that would require notification. Previously this determination required an analysis of the risk of financial, reputational, or other harm to an individual. Under the final omnibus rule, however, a breach will be presumed unless it can be determined through risk assessment that there is a low probability that PHI has been compromised by the unauthorized use or disclosure. This is set forth in a new paragraph (2) of 45 C.F.R. § 164.402 as follows:

Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

HHS stated its expectation that such risk assessments be thorough and completed in good faith, and that the conclusions reached be reasonable. Such risk assessments should also be documented. Where an assessment results in a determination that a breach of unsecured PHI has occurred, all required notifications must be made. HHS also indicated that, in the future, it will issue additional guidance in performing risk assessments with respect to frequently occurring scenarios.

- **Strengthening Enforcement**

The final omnibus rule incorporated the tiered civil money penalty structure set forth in the HITECH Act, whereby different ranges of civil monetary penalties are tied to different levels of culpability. The tiers, which are equally applicable to covered entities and business associates, are as follows:

- If the covered entity or business associate did not know and could not have known of the violations, then the penalty range is $100 - $50,000 per incident.

- If the covered entity or business associate acted with "reasonable cause," that is, the covered entity or business associate knew or would have known through reasonable due diligence that an act or omission would violate the rules but did not act with willful neglect, then the penalty range is $1,000 - $50,000 per incident.

- If the covered entity or business associate acted with willful neglect but instituted successful corrective measures within 30 days, then the penalty range is $10,000 - $50,000 per incident.

- If the covered entity or business associate acted with willful neglect and did not institute

successful corrective measures within 30 days, then the penalty is $50,000 per incident.

All levels include an aggregate annual cap of $1.5 million for violations of identical provisions.

- **Protections for Genetic Information**

In addition to its prohibition of discrimination based on an individual's genetic information in health coverage and employment contexts, GINA contains privacy protections for genetic information requiring revisions to the Privacy Rule. Accordingly, the final omnibus rule revises the Privacy Rule to clarify that genetic information is health information and to prohibit health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes. New paragraph (5)(i) to 45 C.F.R. § 164.502(a) sets forth the following:

> (i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling under paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(1) of this section, underwriting purposes means, with respect to a health plan:
>
> (A) Except as provided in paragraph (a)(5)(i)(B) of this section:
>
> (1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
>
> (2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
>
> (3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and
>
> (4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.
>
> (B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

For now, long-term care plans are exempted from this underwriting prohibition, pending further information for HHS to consider in determining "the proper balance between the individual's privacy interests and the industry's concerns about the cost effects of excluding genetic information."

- **Compliance Deadlines**

The final omnibus rule is effective on March 23, 2013 and covered entities and business associates have 180 days to comply with most of the rule – meaning compliance initiatives must be in place by September 23, 2013. However, the changes to the enforcement provisions are effective on March 23, 2013.

The scope and anticipated effect of the final omnibus rule is summarized in a January 17, 2013 press release by HHS. In the press release, HHS Office for Civil Rights Director Leon Rodriguez is quoted as follows: "This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."

Click here[1] for final omnibus rule and HHS press release.

1 http://www.hhs.gov/ocr/privacy/hipaa/understanding/omnibus/index.html