Arnall Golden Gregory LLP

Client Alert

Contact Attorneys Regarding This Matter:

Meredith Mlynar Burris
404.873.8164 - direct
404.873.8165 - fax
meredith.burris@agg.com

Jennifer D. Burgar
404.873.8194 - direct
404.873.8195 - fax
jennifer.burgar@agg.com

Stimulus Package Includes Significant Expansion of HIPAA

On February 17, 2009, President Obama signed into law the federal stimulus package, officially known as the American Recovery and Reinvestment Act of 2009. While this law will significantly affect a number of industries, its Health Information Technology for Economic and Clinical Health Act ("HITECH Act") contains provisions that will impact the health care industry by substantially expanding the reach of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA was enacted to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers, and to help covered entities address the security and privacy of health data. The new legislation includes provisions intended to shore up public confidence in the use of electronic health records ("EHR"s) and personal health records ("PHR"s) by beefing up enforcement of HIPAA and expanding the scope of businesses covered by the Act. The provisions of the HITECH Act will, inter alia: (1) authorize state attorneys general to file suit on behalf of affected patients for entity HIPAA non-compliance; (2) increase current civil penalties and make criminal penalties applicable to persons, including covered entity (e.g., hospitals, doctors, insurers, employer plans) employees who obtain protected health information ("PHI") without authorization; (3) extend the HIPAA security provisions to business associates; (4) require entities to notify patients if the security of "unsecured PHI" has been breached; (5) prohibit the use of PHI for fundraising purposes, absent express authorization from patients; (6) require covered entities to make an electronic copy of electronic health records available to assist patients and/or plan participants in building their personal EHRs; (7) prohibit the sale of electronic PHI, with limited exceptions, including patient authorization; (8) allow patients to restrict access to their PHI; (9) require that covered entities "account for" routine disclosures of PHI, including those related to treatment, payment and healthcare operations, for disclosures dating back up to three years from the patient's request; and (10) heighten the burden on covered entities to use only the minimum necessary PHI.

The HITECH Act creates a private cause-of-action for HIPAA non-compliance, which could be brought by state attorneys general to seek injunctions and/or monetary damages on behalf of patients whose health privacy or security has been compromised. Courts will be able to awards costs and attorneys' fees in successfully prosecuted cases. The Act also delineates a tiered penalty system, where violators of HIPAA shall be fined different amounts depending on whether the violation was made without knowledge (starting at $100 per violation), due to reasonable cause (starting at $1,000 per violation) or due to willful neglect (starting at $10,000 for violations that are corrected, or $50,000 for violations that are not corrected).

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

One of the most significant expansions of HIPAA under the HITECH Act is that business associates are now subject to the same HIPAA requirements applicable to covered entities. Business associates, which include, but are not limited to, those companies that have access to protected health information to perform legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and/or financial services for covered entities, will now need to implement policies and procedures that establish administrative, physical, and technical safeguards for PHI. The Secretary of Health and Human Services ("HHS") is required to issue guidance on these safeguards annually and compliance with these new requirements will need to be incorporated into existing business associate agreements. Like covered entities, business associates now will be subject to direct penalties for violations of HIPAA's security provisions, including civil and criminal penalties.

Another substantive expansion of HIPAA under the HITECH Act is the requirement that entities now must notify patients if the security of their "unsecured PHI" has been breached. The Act specifies that the Secretary of HHS shall be responsible for defining "unsecured PHI" within 60 days of the law's enactment; if the Secretary fails to provide this guidance, the default definition shall be "protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute." The Act requires notification by business associates to covered entities and covered entities to individuals of any unauthorized access, acquisition, or disclosure of their "unsecured PHI" that compromises the patient's privacy and the integrity of the information. Notification must be given to both patients and the Secretary of HHS no later than 60 days from when the breach is discovered, and if more than 10 patients are involved, the entity must post news of the breach on its website; notification must be given immediately to both patients and prominent media outlets serving the area if the breach involves 500 or more individuals. Additionally, vendors that provide or maintain PHR are required to notify both the affected patients and the Federal Trade Commission in the event of any breach arising from their products or services.

A number of additional provisions included in the stimulus package will significantly impact the way health care providers and their business associates handle PHI and that will require modification of these entities' patient record privacy and security policies and procedures. AGG will continue to update our clients with information on compliance, guidance issued by the Secretary of HHS, and relevant implementation dates in the coming months.

The full text of the American Recovery and Reinvestment Act of 2009 can be found here: http://www.govtrack.us/congress/bill.xpd?bill=h111-1