HUNTON& WILLIAMS

CLIENT ALERT

February 2009

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Aaron P. Simpson
200 Park Avenue
New York, NY 10166
(212) 309-1126
asimpson@hunton.com

Elizabeth H. Johnson
One Bank of America Plaza
Suite 1400
421 Fayetteville Street
Raleigh, NC 27601
(919) 899-3073
ehjohnson@hunton.com

Additional Lawyers
Cédric Burton
Purdey Castle
Jörg Hladjk
Natalie Hunt
Christopher Kuner
Ryan P. Logan
Manuel E. Maisog
Melinda L. McLellan
Olivier Proust
Boris Segalis
Rachel M. St. John
Bridget C. Treacy
Mason A. Weisz
John W. Woods, Jr.

Centre for Information Policy Leadership
Martin E. Abrams*
Paula J. Bruening
Fred H. Cate
Orson Swindle*

*Not a lawyer

Stimulus Package Includes Breach Notice Obligations and Substantial Changes to HIPAA

Provisions of the economic stimulus legislation (known as the American Recovery and Reinvestment Act ("ARRA")), recently passed by the U.S. House of Representatives, require certain entities to notify affected individuals, government agencies and the media of breaches of "unsecured protected health information." Additional provisions substantially revise regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). While these provisions are specifically limited to the context of health data, they have far-reaching implications for businesses across industry that manage personal information.

Breach Notification Provisions

Following the trend at the state level where there are now more than 45 security breach notification laws in place, the ARRA contains information security provisions that require notification of security breaches in certain instances. In many important respects, this legislation varies from the core elements of existing state security breach notification laws. The new information security breach provisions apply in the health care context, governing both HIPAA-covered entities and non-HIPAA-covered entities.

Breach Notification by HIPAA-Covered Entities

Similar to the state security breach notification laws, the new legislation requires (1) HIPAA-covered entities that experience an information security breach to notify affected individuals and (2) business associates of HIPAA-covered entities to notify the HIPAA-covered entity following discovery of a breach. Unlike the state breach notification laws, the obligation to notify as a result of an information security breach under the new legislation falls on any HIPAA-covered entity that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information." This expands dramatically the concept currently in place at the state level, which ambiguously places the notification burden on "data owners." Under the new legislation, any HIPAA-covered entity that *processes* "unsecured protected health information" must notify affected individuals in the event of a breach, whether they own the data or not.

In addition, the likelihood that a HIPAA-covered entity will experience a legally cognizable security breach under the new provisions is increased significantly by the definition of the term "protected health information" or "PHI." Incorporating the relevant definition from HIPAA, this term

encompasses all individually-identifiable health information transmitted by or maintained in electronic media *or any other form or medium*. Thus, unlike most state security breach notification laws that apply only to personal information in "computerized" form, the new legislation will require notification regardless of the medium in which the information is transmitted or maintained. Likewise, the definition of "breach" under the legislation includes "unauthorized acquisition, access, use, or disclosure of protected health information," which expands on the typical state law definitions emphasizing only "acquisition" and "access."

Once a HIPAA-covered entity determines that it has an obligation to notify under the legislation, the recipients of that notification go far beyond affected individuals, as is the standard under most state breach notification laws. To the extent the information security breach impacts 500 or more individuals, the HIPAA-covered entity is required to provide "immediate" notice to the Secretary of the Department of Health and Human Services. In addition, if more than 500 individuals are affected in a given state or jurisdiction, notice must be provided to prominent media outlets in those states or jurisdictions following the discovery of the breach. In cases where there are fewer than 500 individuals affected, the HIPAA-covered entity must maintain a log of such breaches and submit the log annually to the Secretary of the Department of Health and Human Services. The Secretary is required to publish on the Department of Health and Human Services' website a list of HIPAA-covered entities involved in a security breach impacting more than 500 individuals. These requirements will certainly serve to expand the already-heightened public awareness regarding information security breaches.

Under most of the state breach notification laws, entities experiencing breaches typically are required to notify within a reasonable period of time. The timing requirements under the new legislation are less forgiving, as they require notice not later than 60 calendar days after the discovery of the breach by the HIPAA-covered entity or its business associate. Similarly, the legislation provides little flexibility regarding the question of when the breach was discovered. To the contrary, the legislation clearly states that a breach is treated as discovered on the first day it is known to the HIPAA-covered entity or business associate or should reasonably have been known. This includes knowledge by any employee, officer or other agent of the covered entity or business associate. Given the significant amount of forensic investigation and planning that goes into the notification process, HIPAA-covered entities will need to have notification plans in place and move quickly to meet these timing requirements.

Another important point of divergence with the state breach notification laws concerns encryption of the personal information in question. Under most state breach notification laws, notification is not required if the information accessed or acquired is encrypted. Typically, the term "encrypted" is left undefined by the state laws. In the new legislation, notice is required for all breaches involving "unsecured" PHI. Unlike under the state laws, this legislation is intended to be prescriptive in this context, as it requires the Secretary of the Department of Health and Human Services to issue and annually update guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. Although directly relevant in the health data context, this guidance will likely serve as a standard across industry with respect to technologies and methodologies that render personal information unusable, unreadable or indecipherable.

In addition to these significant departures from existing state security breach notification laws, the new legislation regarding information security breaches contains other provisions of which HIPAA-covered entities and their business associates should be aware. These include (i) imposing the burden of proof on the HIPAA-covered entity or business associate suffering the breach to demonstrate that all required notifications were made, (ii) permitting notification of affected individuals by telephone in urgent cases, and (iii) specific requirements related to the content of the notice sent to affected individuals.

Breach Notification by Non-HIPAA-Covered Entities

The legislation also contains separate breach notification requirements for certain vendors of personal health records and other non-HIPAA-covered entities in the health care context. In the event of a breach, these entities are required to notify both affected individuals and the Federal Trade Commission ("FTC"), which in turn is required to notify the Secretary of the Department of Health and Human Services. In this context, violations of the notice provisions are treated as unfair and deceptive acts and the FTC is authorized to enforce under Section 5 of the FTC Act. Other provisions in this context are imported from the provisions governing HIPAA-covered entities and business associates.

Substantial Changes to HIPAA

Among the ARRA's privacy provisions are requirements that substantially affect obligations imposed on covered entities and business associates by HIPAA. For example, the ARRA applies the majority of the HIPAA Security Rule's provisions directly to business associates, including all provisions mandating specific administrative, physical and technical safeguards, including the Rule's policies, procedures and documentation requirements. In addition, all security requirements specified in the ARRA as applicable to covered entities are also applicable to business associates and must be incorporated into the business associate agreement ("BAA") with the covered entity. Under current HIPAA regulations, business associates must comply only with more generalized security requirements imposed via a BAA.

The ARRA also imposes additional privacy requirements on covered entities, providing that those same requirements will apply equally to business associates and must be incorporated into the BAA. For example, HIPAA presently requires that covered entities maintain an accounting of certain disclosures of PHI. Under the ARRA, however, the exception that allows covered entities to exclude from their accounting disclosures related to treatment, payment and health care operations would no longer apply to covered entities that use or maintain "electronic health records," as defined by the ARRA. Individuals would be able to request an accounting of such disclosures made in the prior three years. This requirement would present a substantial administrative burden for covered entities, and potentially business associates, due to the prevalence of disclosures for treatment, payment and health care operations. Industry representatives have noted that the cost of storing such data for a three-year period, not accounting for the expense of implementing technical solutions to log disclosures, will be onerous.

The HIPAA Privacy Rule also provides that a covered entity will not be in compliance if it knows of a pattern or practice by its business associate that constitutes a material breach or violation of a BAA, unless it takes steps to cure the breach or violation and, if unsuccessful, either terminates the BAA or reports to the Department of Health and Human Services. The ARRA explicitly provides that this provision would apply equally to business associates, who must similarly take steps to cure a breach or violation of a BAA by a covered entity and, if unsuccessful must terminate the BAA or report to the Department.

In addition, to be deemed in compliance with the minimum necessary provisions of the HIPAA Privacy Rule, pursuant to the ARRA, covered entities would be required to rely upon a "limited data set," to the extent practicable. A limited data set consists of PHI from which an extensive list of personal identifiers, such as name, postal address, email address, phone or fax number, Social Security number, account numbers, URL, IP address and biometric identifiers are removed.

The ARRA also limits a covered entity or business associate's ability to receive remuneration, either direct or indirect, for disclosures of PHI. These restrictions include limitations on these entities' ability to be paid in connection with marketing activities.

The ARRA requires the Secretary to revise existing HIPAA regulations to be consistent with the provisions of the new legislation, and further requires the Secretary to adopt various new rules and issue guidance. The Secretary is also directed to provide for periodic audits to ensure compliance. Effective dates vary for most of the requirements but, where not otherwise specified, the requirements are effective 12 months from the date of the ARRA's enactment.

We Can Help

The ARRA is expected to be approved by Congress and submitted to President Obama by February 16. The privacy and data security provisions of the ARRA will require substantial operational changes, particularly for business associates. Hunton & Williams' Privacy and Information Management practice has substantial experience preparing and advising on comprehensive privacy and information security programs (including those maintained by HIPAA-covered entities), and frequently assists clients in preparing for and responding to information security breaches. If you would like to discuss this legislation, or need assistance in developing, reviewing or implementing your organization's privacy or data security practices, please contact us.