February 20, 2009

HEALTH INDUSTRY ALERT

AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009: STIMULUS LEGISLATION OVERHAULS AND EXPANDS THE REACH OF THE FEDERAL HIPAA REGIME GOVERNING HEALTH INFORMATION PRIVACY AND SECURITY

On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act of 2009 (Recovery Act), which includes provisions making major changes to the federal health information privacy and security regime established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This legislation substantially broadens the scope and expands the reach of requirements concerning the privacy and security of health information. These changes will have a major impact on many health sector participants, including individuals and entities currently treated as "Covered Entities" (defined as including certain health care providers, as well as health plans and health care clearinghouses) and the "Business Associates" that perform functions or services on their behalf.

Key changes to the existing HIPAA privacy and security regime enacted through the stimulus legislation include, but are not limited to, the following—

- **Expanding obligations—and exposure—of Business Associates.** Under existing federal law, Business Associates only need to comply with a discrete list of privacy and security obligations that can be enforced by the Covered Entity through contract. Not only has this list of obligations expanded, but in a sea change for Business Associates, the Recovery Act creates direct, statutory obligations for Business Associates. The stakes are high, as the Recovery Act applies civil and criminal penalties to Business Associates.

- **Establishing a federal breach notification requirement.** While many states have adopted security breach notification laws, existing federal law does not require notice of data breaches involving protected health information (PHI). The Recovery Act establishes an

expansive protocol for providing notice in the event that an individual's unsecured PHI has been (or is reasonably believed to have been) accessed, acquired or disclosed as a result of a data breach. This new federal regime is more prescriptive and onerous than data breach notification laws presently in place in many states. For example, the legislation goes so far as to require that in addition to notifying individuals, both the Secretary of the U.S. Department of Health and Human Services (Secretary) and prominent local media outlets must be notified of data breaches under certain circumstances.

- **Calling for refinement of the "minimum necessary" standard.** Covered Entities are presently required to use, disclose and request only the "minimum necessary" PHI in many situations. The Recovery Act calls for new regulations on what constitutes "minimum necessary" for purposes of the HIPAA privacy provisions, and establishes a transitional standard that will remain in effect until the Secretary issues the required guidance.

- **Expanding the types of disclosures subject to accounting requirements.** Individuals currently have the right to receive an accounting of disclosures of their PHI made by a Covered Entity in the past six years, with certain exceptions. One important exception is for disclosures to carry out treatment, payment and health care operations. The Recovery Act eliminates this exception for Covered Entities using electronic health records. The legislation requires such Covered Entities to account for these types of disclosures, to the extent they are made through an electronic health record, for the three years preceding the date of the accounting request.

- **Limiting the sale of protected health information.** Existing privacy regulations do not provide extensive guidance concerning situations in which the sale of PHI would be prohibited without authorization. The Recovery Act expressly prohibits Covered Entities and Business Associates from directly or indirectly receiving remuneration in exchange for PHI without the individual's authorization, subject to several exceptions. Specifically, the legislation carves out exceptions for public health activities, treatment, the merger or acquisition of the Covered Entity, research (if remuneration is limited to the cost of preparation and transmittal of data) and certain Business Associate functions, as well as for the purpose of allowing individuals to copy their PHI when exercising their access rights. The legislation allows the Secretary to create additional exceptions that are similarly necessary and appropriate.

- **Restricting marketing communications.** HIPAA regulations currently carve out commercial communications related to treatment and certain health care operations from the definition of "marketing," thus allowing these communications to be conducted without authorization from the individual. The Recovery Act adds a new degree of complexity to

the marketing analysis, further limiting the situations in which such communications may be made without authorization. The legislation does not, however, affect communications made for treatment purposes.

- **Fine-tuning requirements concerning fundraising activities.** Currently, Covered Entities may use and make limited disclosures of a restricted set of PHI for their own fundraising purposes, without authorization, provided that any fundraising materials sent to an individual expressly describe how the individual may opt out of receiving further fundraising communications. While Congress considered changes that would have required authorization for all uses and disclosures of PHI for fundraising purposes, the Recovery Act, in its final form, instead only clarifies the existing regime. Specifically, the Recovery Act calls for regulations requiring that written fundraising communications provide, in a clear and conspicuous manner, an opportunity for the recipient of the communication to elect not to receive any further such communications. The Recovery Act also provides that an individual's exercise of the opt-out right will be treated as a revocation of authorization.

- **Enhancing penalties and strengthening enforcement of privacy and security requirements.** HIPAA enforcement efforts to date have been weak, with far fewer Covered Entities being penalized for compliance lapses than anticipated. The Recovery Act takes numerous steps to reverse this trend, including allowing state attorneys general to file suit on behalf of their residents for violations of HIPAA, requiring the Secretary to conduct audits of Covered Entities and Business Associates to ensure compliance with privacy and security requirements, calling for a mechanism to allow individuals harmed by a privacy or security violation to receive a percentage of any civil monetary penalties or settlement amounts collected in connection with the offense, clarifying that criminal penalties established by HIPAA may apply to employees of a Covered Entity or Business Associate, and creating a tiered civil monetary penalty system based on the level of intent or neglect (with penalties ranging from $100 to $50,000 for each individual violation, subject to various caps).

- **Contemplating expanding the HIPAA regime to apply privacy and security standards to additional types of entities.** Existing law focuses primarily on health care providers, health plans and health care clearinghouses, bringing certain service providers into the fold through the Business Associate contracts. The Recovery Act looks beyond Covered Entities and Business Associates. Specifically, the legislation requires the Secretary, in consultation with the Federal Trade Commission, to study and report on the extent to which privacy and security requirements should apply to entities that are not currently considered Covered Entities or Business Associates, including vendors of personal health records and other such entities.

Many stakeholders in the health care industry are still grappling with HIPAA's already arduous rules, and fear that adding a fresh layer of complexity through statutory changes and new rulemakings could negate some of the positive benefits of health information technology (HIT) adoption. Covered Entities and Business Associates will need to devote time and resources to bringing their operations into compliance with the new privacy and security regime. All Business Associate agreements will need to be amended, policies and procedures will need to be created or updated, and current patterns of use and disclosure will need to be reassessed to ensure compliance. The landscape is likely to continue shifting as the Secretary develops and implements the myriad regulations permitted or required by the law.

CONTACT INFORMATION

If you have any questions regarding the implications of the privacy and security provisions of the Recovery Act for your business, please contact—

Jorge Lopez, Jr.	jlopez@akingump.com	202.887.4128	Washington, D.C.
Jo-Ellyn Sakowitz Klein	jsklein@akingump.com	202.887.4220	Washington, D.C.
Kelly Maxwell	kmaxwell@akingump.com	202.887.4385	Washington, D.C.
Kelly Cleary	kcleary@akingump.com	202.887.4329	Washington, D.C.