

Significant Changes in the Health Data Privacy for Group Health Plans and their Business Associates

March 27, 2009 Charles Plenge

PRACTICES Health and Welfare Plans, Employee Benefits and Executive Compensation

The American Recovery and Reinvestment Act of 2009 (the "Act") broadens the HIPAA privacy and security protections that apply to protected health information ("PHI") and imposes new requirements on group health plans and their business associates. Under the Act, certain HIPAA privacy and security requirements now directly apply to business associates as if they were covered entities.

Among other things, the Act:

- Adds to the privacy and security requirements the concept of "breach" of PHI (e.g., the unauthorized access, use or disclosure of certain PHI), and imposes new reporting and notice obligations on group health plans when a breach occurs. In addition to new administrative burdens, the breach notification requirements will make such improper disclosures a public relations issue for group health plan sponsors and a potential source for government investigations, resulting in an increased risk of sanctions.
- Imposes new electronic standards on any covered entity that accesses, maintains, retains, stores, destroys or otherwise holds, uses or discloses any PHI, and modifies the privacy requirements with respect to electronic PHI.
- Expands an individual's ability to place restrictions on the use and disclosure of PHI for certain purposes. The Act, unlike the prior law, requires covered entities to comply with a requested restriction in certain instances.
- Requires all disclosures on and after February 17, 2010 and until new regulations are issued to be limited to either a limited dataset or to the minimally necessary information. Minimally necessary will no longer be determined by the plan when the Act's change is effective.
- Clarifies and modifies the requirements for tracking disclosures of PHI and the use of PHI to encourage the purchase or use of a product or service.
- Expands the disclosures and uses of electronic PHI ("E PHI") that must be recorded on the log of disclosures and uses of E PHI.
- Provides that any covered entity that maintains an electronic health record must give individuals the right to direct the covered entity to transmit a copy of such health record directly to a designated person or entity effective on and after February 17, 2010.

Plan sponsors and business associates will need to update their HIPAA privacy and security policies and procedures and will need to conduct updated HIPAA privacy and security training to ensure compliance with the new requirements. In addition, plan sponsors will need to amend plan documents and re-negotiate their business associates agreements with plan vendors and other

business associates. Plans will need to update their HIPAA privacy notices to reflect the changes once effective.

The Act also authorizes the State's Attorney General to pursue actions for HIPAA violations, requires periodic audits of covered entities and business associates to determine compliance. The Act increases the scope and amount of penalties for violations, applying penalties to any person (not just covered entities) who is considered to have obtained or disclosed PHI in violation of HIPAA if the PHI involved was maintained by a covered entity. If there is willful neglect of the HIPAA privacy protections, then the Secretary is required to impose a civil penalty. Plan sponsors will need to communicate the extension of the liability to the covered entity's employees and individuals to the persons involved with the health plan who have access to PHI.

While many of the requirements do not become effective until issuance of final regulations, group health plans should monitor the guidance in this area to determine when each of the new requirements will first apply to them and require changes in their plan documents, privacy notices and privacy and security policies and procedures.

For more information on the Employee Benefits and Executive Compensation group and its members, go to [Employee Benefits and Executive Compensation](#).