

Employee Benefits and Executive Compensation

Significant Changes to HIPAA Will Affect Employer-Provided Group Health Plans

By V&E lawyers David D'Alessandro, Dorene Cohen, and Ron Bradshaw

FEBRUARY 2, 2010



Significant Changes to HIPAA Will Affect Employer-Provided Group Health Plans

By V&E lawyers David D'Alessandro, Dorene Cohen, and Ron Bradshaw

The Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), which is part of the American Recovery and Reinvestment Act of 2009 (ARRA), enacted significant changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Most of the changes apply beginning February 17, 2010, but there are some other effective dates that apply to specific provisions as addressed below. Employer-provided group health plans (Plans) will need to take various measures to comply with these new HIPAA requirements, including:

1. *Obtain assurances from the Plan’s business associates (both current business associates, as well as entities that will be treated as business associates under the expanded definition of a business associate (see Item 3 below) or that are expected to become business associates in 2010) that they will timely comply with the heightened HIPAA requirements.* Effective February 17, 2010, all business associates will be directly responsible for complying with many HIPAA requirements that currently apply only to HIPAA covered entities (*i.e.*, compliance with certain of HIPAA’s privacy and security standards such as developing policies and procedures, staff training, and other activities).
2. *Amend existing business associate agreements.* The existing business associate agreements should be amended to reflect these new HIPAA obligations.
3. *Review relationships with third-party vendors to determine whether any other business associate agreements are required.* The HITECH Act clarifies that effective February 17, 2010, each organization that provides data transmission of protected health information (PHI) to a covered entity or its business associates and that requires access to PHI on a routine basis is a business associate of the covered entity. This includes a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, and vendors that contract with a covered entity to allow it to offer a personal health record to patients as part of its electronic health record. Therefore, Plans should review their relationships with third-party vendors and verify that no other business associate agreements are required in light of this clarification. If additional entities are to be treated as business associates under the new law, Plans will need to execute business associate agreements with these new business associates.

4. *Prepare to either minimize or implement new breach notice obligations.* Under the HITECH Act, new notice obligations are associated with breaches of PHI. The breach notice obligation can be minimized, however, if certain standards for protecting PHI are observed. Although the new breach notice requirements are already effective (starting September 23, 2009), the U.S. Department of Health and Human Services (HHS) has announced that it will not enforce penalties for breaches of unsecured PHI discovered before February 22, 2010. To comply with these new provisions, a Plan can either: (a) secure its PHI pursuant to HHS guidance so that the PHI is not treated as “unsecured” PHI, thereby minimizing the notice requirement altogether or (b) be prepared to provide the required notices for breaches of unsecured PHI that are discovered (or should have been discovered if the Plan had been prudent in its HIPAA compliance efforts) on or after February 22, 2010. Note that the HHS intends to update its guidelines for securing PHI annually; therefore, review of whether the Plan’s PHI is “secured” pursuant to the HHS guidelines will be required annually if option (a) is chosen. Under the current guidance (interim final regulations issued by the HHS on August 19, 2009), either encryption or complete destruction (pursuant to certain standards issued by the National Institute of Standards and Technology) is required to satisfy the HHS’s “safe harbor” for securing PHI (including any PHI that may be transmitted in emails with both employees and vendors) and rendering it unusable, unreadable, or indecipherable to unauthorized individuals so that covered entities are relieved of the notice obligations otherwise required in response to security breaches of PHI. If encryption is used to satisfy the breach notice safe harbor, it must satisfy certain standards. For example, encryption must use “an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key,” and the decryption tools must be stored on a device or at a location separate from the encrypted data. Other standards apply as well. Note that this safe harbor regarding encryption was not intended to replace or modify HIPAA’s existing security and privacy provisions.

5. *Review and amend the Plan’s HIPAA policies and procedures to address individual rights and marketing restrictions added by ARRA.* Effective February 17, 2010, covered entities like group health plans must (a) agree to honor certain PHI restriction requests related to services for which the provider has received payment from the individual fully on an out-of-pocket basis, (b) agree to provide electronic copies of any electronic health records upon request, and (c) restrict PHI from being sold or used for marketing purposes without an individual’s HIPAA authorization, with certain exceptions. Under HITECH Act provisions that will be effective after additional guidance is issued, Plans should also become prepared to account for all electronic disclosures (including data related to treatment, payment, and healthcare operations) of electronic health records (EHRs). EHRs generally include health-related information about individuals that is created, gathered, managed, and consulted by authorized healthcare clinicians. In addition, to comply



with the “minimum necessary” HIPAA privacy rule, covered entities should limit the use and disclosure of and access to PHI to “limited data sets,” where practicable, or otherwise to the minimum necessary, in accordance with additional guidance that is yet to be issued. Policies and procedures should be revised to reflect these new rules, relevant staff should be trained accordingly, and the Plan’s privacy notice should be revised and distributed.

6. *Perform ongoing and periodic security and privacy analysis under new HHS guidance.* HHS guidance is expected to be updated on an ongoing annual basis, and covered entities will need to ensure that they remain compliant with regular HHS guidance updates. Under ARRA, heightened enforcement of violations is expected (*i.e.*, HHS is required to conduct periodic audits to measure compliance, penalties have been increased for HIPAA violations, and state attorneys general are now authorized to bring civil actions on behalf of residents who are threatened or adversely impacted by violations of HIPAA). Due to this heightened enforcement, Plans should conduct periodic HIPAA privacy and security reviews, amending policies and procedures and taking other actions, as required.

Please let us know if you would like our assistance with identifying new business associates, reviewing and drafting business associate agreements, reviewing and amending the Plan’s policies and procedures, satisfying the breach notice requirement described above, or otherwise complying with ARRA’s new HIPAA requirements. Please note that compliance with a number of the HITECH Act’s new requirements is required by February 17, 2010.

For more information, please contact Vinson & Elkins lawyers [David D'Alessandro](#), [Dorene Cohen](#), or [Ron Bradshaw](#). Visit our website to learn more about V&E's [Employee Benefits and Executive Compensation practice](#), or e-mail one of the V&E Employee Benefits and Executive Compensation [practice contacts](#).

This paper is intended for educational and informational purposes only and does not constitute legal advice or services. If legal advice is required, the services of a competent professional should be sought. These materials represent the views of and summaries of the author, and do not necessarily reflect the opinions or views of Vinson & Elkins LLP or of any of its other attorneys or clients. It is not guaranteed to be correct, complete, or current, and it is not intended to imply or establish standards of care applicable to any attorney in any particular circumstance. Prior results do not guarantee a similar outcome.