

Mailing Address
P.O. Box 6133
Williamsburg VA 23188



Office Location
325 McLaws Cr. Suite 2
Williamsburg VA 23185

Courtesy of:
Peter Mellette, Esq.
peter@melletpc.com

Client Advisory

Modification of the Health Insurance Portability and Accountability Act (“HIPAA”) Business Associate Agreement Requirements by 2009 Stimulus Package

The recent Federal Stimulus Bill, the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 (“Stimulus Package”) included many substantive changes for healthcare providers. One such change is to the agreements such providers maintain with others.

As you may know, HIPAA standards require health care providers to enter into a written contract with an organization that performs certain functions or activities that involve the creation, use, or disclosure of protected health information (PHI) for, or on behalf of, the healthcare provider or other covered entity. These contracts, known as “business associate agreements”, establish the permitted and required uses and disclosures by the business associate of the patient PHI maintained by the healthcare provider, also referred to in HIPAA as the “covered entity”. The 2009 Stimulus Package, specifically Title IX (Health Information Technology), Subtitle D (Privacy), requires certain modifications of business associate agreements. Below are some suggestions for altering your business associate agreements accordingly.

- **Definitions:** As many health records are now electronic, a definition of “electronic health record” should be included in most agreements. The definition should read: “An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized healthcare clinicians and staff.” Additionally, a definition of “unsecured protected health information” should be added to read: “Protected health information that is not secured through the use of a technology or methodology specified by the Secretary of Health and Human Services.” The Secretary should be issuing guidance as to technologies and methodologies that render PHI secure.
- **Responsibilities of Business Associate:** Business Associate agreements should already have a provision that compels business associates to immediately report any unauthorized use or disclosure of PHI to the covered entity. Added to this should be a statement that notifications should be made no later than 60 days after the discovery of a breach, and that when the business associate is the breaching party, it bears the burden of proving that it has notified the covered entity. The method of notice depends on the number of affected individuals, requiring a publicized notice of over 10 individuals with unauthorized PHI have PHI released.

- **Minimum Necessary:** Again, agreements should already have a provision stating that covered entities and business associates must limit use and disclosure of PHI to the minimum necessary to achieve the services being rendered. The Stimulus Bill states that within the next 18 months, the Secretary shall issue guidance on what exactly constitutes the minimum necessary. Until that time, the business associate or covered entity should use its best judgment.
- **Electronic Health Records:** Important provisions regarding electronic health records should be added to most business associate agreements. 45 CFR 164.528(a)(1)(i) provides that an individual does not have a right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested, when the disclosure is to carry out treatment, payment, and health care operations.

The Stimulus Bill makes clear that the treatment, payment and healthcare operations exception does NOT apply to disclosures made through an electronic health record. In these cases, an individual DOES have a right to receive an accounting of disclosures made during the **three** years prior to the date on which the accounting is requested. The provision could read as follows: “If a covered entity uses or maintains an electronic health record with respect to PHI, the exception under 45 CFR 164.528(a)(1)(i) shall *not apply* to disclosures made through an electronic health record. When disclosures are made through an electronic health record, an individual shall have a right to receive an accounting of disclosures made during only the *three* years prior to the date on which the accounting is requested. If a covered entity has acquired an electronic health record as of January 1, 2009, the above shall apply to the covered entity with respect to disclosures made by the entity from that record on and after January 1, 2014. If a covered entity acquires an electronic health record after January 1, 2009, the above shall apply to the entity with respect to disclosures made on and after the later of the following: (a) January 1, 2001, or (b) the date that it acquires an electronic health record.” This may require additional recordkeeping to identify all disclosures made through an electronic health record.

- **Prohibition on Sale of Electronic Health Records:** Another clause to add to business associate agreements under a provision concerning electronic health records should state that business associates and covered entities shall not receive remuneration in exchange for any PHI of an individual unless the covered entity obtained a valid authorization from the individual specifying whether the PHI can be further exchanged for remuneration.

The Stimulus Bill provides certain exceptions to this prohibition, and they can be placed verbatim in business associate agreements: “Exceptions: (a) The purpose of the exchange is for research or public health activities (as described in 45 CFR 164.501, 164.512(i), and 164.512(b)) and the price charged reflects the costs of preparation and transmittal of the data for such purpose; (b) The purpose of the exchange is for the treatment of the individual and the price charged reflects not

more than the costs of preparation and transmittal of the data for such purpose; (c)The purpose of the exchange is the health care operation specifically described in subparagraph (iv) of paragraph (6) of the definition of health care operations in section 45 CFR 164.501; (d) The purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities involving the exchange of PHI that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement; (e)The purpose of the exchange is to provide an individual with a copy of the individual's PHI.”

- ***Business Associate Agreements Required for Certain Entities:*** You should be aware that certain organizations and vendors that deal with you, the covered entity, and/or your business associates are required to be treated as business associates themselves. These include organizations that provide data transmission of PHI to you or your business associates and that require access on a routine basis to such PHI, and vendors that contract with you to allow you to offer a personal health record to patients as part of your electronic health record. You should know that you are required to enter into written business associate agreements with these entities.
- ***Penalties:*** Business Associate Agreements should also state that if a business associate violates any of the Agreement's provisions, sections 1176 and 1177 of the Social Security Act shall apply to the business associate in the same way they would apply to the covered entity.

Many of the HIPAA changes apply to healthcare providers and other covered entities. These include the notice provisions and the discovery provision. Please let us know if you have any questions or if we can assist you further in redrafting your business associate agreements.

Mellette PC acknowledges with gratitude the assistance of Caitlin A. Parker, Marshall-Wythe School of Law, Class of '10, in the preparation of this client advisory.