

HITECH Act: New Security Breach Notification Requirements

Prior to the HITECH Act, HIPAA only required a covered entity to account for any unauthorized disclosure of an individual's protected health information ("PHI"), (i.e., record information in a log or similar format describing the PHI disclosed, to whom and when the PHI was disclosed, etc.). Thus, a covered entity was not required to provide an individual with notice that his or her PHI was the subject of a security breach or otherwise unauthorized disclosure. The HITECH Act creates new security breach notification requirements.

- **Breach Notification Required:** Section 13402(a) of the HITECH Act requires a covered entity to notify individuals whose "unsecured" PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a "breach." Section 13400(1) of the HITECH Act defines "breach" as the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, subject to certain exceptions. In addition, business associates must notify covered entities of any breaches of PHI of which they become aware. See Section 13402(b) of the HITECH Act.

No later than 60 days after the enactment of the HITECH Act, the Secretary of the Department of Health and Human Services ("Secretary") must issue guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

- **Timeliness of Notification:** Notice of a breach must be provided to an individual without unreasonable delay and in no case later than 60 days after the discovery of the breach. A breach shall be treated as discovered by a covered entity or business associate as of the first day on which such breach is known, or should have been known, to the covered entity or business associate. The knowledge of any person, other than the individual committing the breach, that is an employee, officer, or other agent of a covered entity or business associate shall be imputed to the entity or associate for the purpose of establishing compliance with the 60-day requirement. See Section 13402 of the HITECH Act.

- **Methods of Notice:**

Individual Notice: Notice to the individual whose PHI is the subject of a breach must be made in writing, via first-class mail, to his or her last known address (or by electronic mail if the individual has expressed a preference). Where there are 10 or more individuals for which there is insufficient or out-of-date contact information, the covered entity must post a conspicuous notice on its website or in major print or broadcast media in geographic areas where the individuals affected by breach likely reside. Such notice must include a toll-free number where an individual can learn whether his or her's PHI is included in the breach. See Section 13402(e)(1) of the HITECH Act.

Media Notice: Where the unsecured PHI of more than 500 residents of any state is reasonably believed to have been accessed, acquired, or disclosed during a breach, the covered entity must provide notice of the breach to prominent media outlets serving the state. See Section 13402(e)(2) of the HITECH Act.

HHS Notice: Notice must be provided by a covered entity to the Secretary of unsecured PHI that has been accessed, acquired, or disclosed during a breach. If the breach was with respect to 500 or more individuals, such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the covered entity may maintain a log documenting these breaches. This log must be submitted to the Secretary annually. The Secretary will post on the website of the Department of Health and Human Services a list that identifies each covered entity involved in a breach in which the unsecured PHI of 500 or more individuals is accessed, acquired, or disclosed. See Section 13402(e) of the HITECH Act.

- **Notice Content:** Regardless of the method, notice of a breach must include: (1) a brief description of what happened, including the date of the breach and the date

of the discovery of the breach, (2) a description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code), (3) the steps individuals should take to protect themselves from potential harm resulting from the breach, (4) a brief description of what the covered entity is doing to investigate the breach, to mitigate losses, and to protect against any further breaches, and (5) contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an electronic mail, web site, or postal address. See Section 13402(f) of the HITECH Act.

- **Effective Date:** The Secretary must promulgate interim final regulations within 180 days of the enactment of the HITECH Act. These new security breach notification requirements will become effective 30 days after publication of the regulations. See Section 13402(j) of the HITECH Act.

Breach Notification Requirement For Vendors of Personal Health Records ("PHR") and Other Non-HIPAA Covered Entities

Each vendor of personal health records ("PHR"), following the discovery of a breach of security of unsecured PHR identifiable health information that is in a PHR maintained or offered by such vendor, must notify: (1) each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such breach of security, and (2) the Federal Trade Commission. This notification requirement also applies to: (1) entities that offer products or services through the website of a vendor of PHR; (2) entities that are not covered entities and that offer products or

services through the websites of covered entities that offer individuals PHR; and (3) entities that are not covered entities and that access information in a PHR or send information to a PHR, if the breach of security is through a product or service provided by such entity. See Section 13407(a) of the HITECH Act.

A third party service provider that provides services to a vendor of PHR, or to other entities referenced above, in connection with the offering or maintenance of a PHR or related product or service must notify the vendor or entity of a breach of security that results from such services. Such notice must include the identification of each individual whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. See Section 13407(b) of the HITECH Act.

This provision shall apply to breaches of security discovered on or after 30 days after promulgation by the Federal Trade Commission of interim final regulations.

For more information, please contact **Nestor J. Rivera** at 404.815.2702 or **nrivera@carltonfields.com**. For more information about Carlton Fields' Health care practice, please visit **www.carltonfields.com/healthcare**



Nestor J. Rivera

This publication is not intended as, and does not represent, legal advice and should not be relied upon to take the place of such advice. Since factual situations will vary, please feel free to contact a member of the firm for specific interpretation and advice if you have a question regarding the impact of the information contained herein. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you free written information about our qualifications and experience.