

§ 164.410 Notification by a business associate.

(a) *Standard—(1) General rule.* A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

(b) *Implementation specifications: Timeliness of notification.* Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

[74 FR 42767, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]