HITECH/HIPAA Breach Notification Regulations

This summary was prepared by the New Jersey Department of Human Services Privacy Officer on February 24, 2010 for distribution at the Division of Addiction Services Quarterly Provider Meeting on February 25, 2010.

The following is a summary of the Breach Notification for Unsecured Protected Health Information Interim Final Rule (IFR) published on August 24, 2009 in the Federal Register. This IFR was required to be issued by Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA). These rules apply to breaches occurring on and after September 23, 2009. This Summary does not constitute legal advice – Providers must consult their own Privacy Officers and/or legal counsel for implementation and legal advice.

Definitions: 45 CFR § 164.402

As used in this subpart, the following terms have the following meanings:

**Breach** means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1)(i) For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

(2) **Breach excludes:**

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

**Unsecured protected health information** means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS Web site.
Notification to individuals: 45 CFR § 164.404

(a) Standard—(1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity 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) Elements. The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number, an e-mail address, Web site, or postal address.

(2) Plain language requirement. The notification required by paragraph (a) of this section shall be written in plain language.

(d) Implementation specifications: Methods of individual notification. The notification required by paragraph (a) of this section shall be provided in the following form:

(1) Written notice.

(i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been
withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) **Substitute notice.** In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

   (i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

   (ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

   (A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

   (B) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual’s unsecured protected health information may be included in the breach.

(3) **Additional notice in urgent situations.** In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

**Notification to the media:** 45 CFR § 164.406

(a) **Standard.** For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.

(b) **Implementation specification: Timeliness of notification.** Except as provided in § 164.412, a covered entity 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.** The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).

**Notification to the Secretary:** 45 CFR § 164.408
(a) **Standard.** A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

(b) **Implementation specifications: Breaches involving 500 or more individuals.** For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site.

(c) **Implementation specifications: Breaches involving less than 500 individuals.** For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

**Notification by a business associate: 45 CFR § 164.410**

(a) **Standard.** (1) 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 (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.

**Law enforcement delay: 45 CFR § 164.412**

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made
orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

**Administrative requirements and burden of proof: 45 CFR 414**

(a) **Administrative requirements.** A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.

(b) **Burden of proof.** In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.

**Administrative requirements: 45 CFR § 164.530**

(b)(1) **Standard: Training.** A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) * * * (i) * * *(C) To each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(d)(1) **Standard: Complaints to the covered entity.** A covered entity must provide a process for individuals to make complaints concerning the covered entity’s policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

(e)(1) **Standard: Sanctions.** A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part.

(g) **Standard: Refraining from intimidating or retaliatory acts.** A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

(h) **Standard: Waiver of rights.** A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) **Standard: Policies and procedures.** A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part.

**procedures.**
(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

(j)(1) **
(iv) Maintain documentation sufficient to meet its burden of proof under § 164.414(b).