

Checklist for Covered Entities

HIPAA HITECH

ADMIN 0101-12

[Unless otherwise specified below, effective date is February 17, 2010]

Covered Entities Must Notify Individual of Breach of re: Unsecured PHI [§13402]
[Effective for breaches occurring on or after September 23, 2009].

_____ **1. Process for notification to individuals and media and Secretary of HHS of breach of unsecured PHI. Process will include:**

A. Notice to Individuals

_____ Notice without unreasonable delay and not later than 60 days after discovery of breach;

_____ Notice by:

_____ First Class mail (or e-mail, if requested), or,

_____ If no current mailing information via substitute form of notice including conspicuous posting on entity's website (required if 10 or more individuals with insufficient contact information), or notice in major print or broadcast media that includes toll-free number.

_____ In urgent cases, because of possible imminent misuse of unsecured PHI, Covered Entities may provide notice by phone or other appropriate means. Notice by mail is still also required.

_____ Notice will include:

_____ Description of what happened, including date of breach and date of discovery;

_____ Description of the types of unsecured PHI that were involved (e.g., name, SS#, DOB, address, etc.);

- _____ Steps individuals should take to protect themselves;
- _____ Brief description of steps Covered Entities are taking to investigate and protect against future breaches; and,
- _____ Contact procedures for individuals to get more information, including toll-free number, email address, website, or postal address.

B. Notice to Media

- _____ Notice to prominent media outlets serving state or jurisdiction in case of breach of unsecured PHI if more than 500 involved.

C. Notice to HHS Secretary

- _____ Notice to HHS Secretary of unsecured PHI that has been acquired or disclosed in a breach.
- _____ If 500 or more individuals involved, notice must be provided immediately.
- _____ If less than 500 individuals involved, Covered Entities may maintain a log of breach and submit log annually to HHS of breaches.

Must Grant Individual's Request to Limit Disclosure of PHI in Some Cases
[\$13405].

_____ **2. Process for Handling Individual's Request to Restrict Disclosure by:**

- _____ Granting requests to limit uses and disclosures of PHI for payment or health care operations if the disclosure is to a health plan for purposes of carrying out payment or health care operations (e.g., not for treatment) and the PHI pertains solely to a health care item or service for which the health care provider has been paid in full. (So, if individual requests no disclosure to health plan for health care operations or payment and health care provider has been paid in full, must grant request).

_____ **3. Limit disclosure or use of PHI to minimum necessary to accomplish purpose by, to the extent possible, limiting use/disclosure to "limited data set" (defined by 164.514(e)(2)), i.e. delete 16 identifiers. (Sunsets once Secretary issues guidance (no later than August 2010) on what is minimum necessary.) Need to make minimum necessary determination for each time disclose. Exceptions to minimum necessary requirements in 165.502(b)(2) still apply.**

Increased Accounting Obligations if Covered Entities Use Electronic Health Record. [§13405(c)] [Effective 1/1/14 if Covered Entities got EHR as of 1/1/09; effective later of 1/1/11 or date Covered Entities get EHR if got EHR after 1/1/09].

- ___ 4. If Covered Entities use electronic health record, Covered Entities must include disclosures made through an EHR for payment/treatment/health care operation on the accounting and the individual can get an accounting of payment/treatment/health care operation disclosures made during past 3 years.

Covered Entities Must Make Accounting Available to Individual [§13405(c)].

- ___ 5. Process to allow individual to obtain an accounting of disclosures made by Covered Entity & Business Associates or an accounting of disclosures by Covered Entity and a list of Business Associates with contact information. Business Associates must give individuals an accounting of PHI disclosures.

Subject to Exceptions, Covered Entities Cannot Get Remuneration for PHI Absent a Signed Authorization From Individual Expressly Allowing Remuneration in Exchange for PHI [§13405(d)] [Effective 6 months after final interim regulations, i.e. 2/2011].

- ___ 6. A Covered Entities may not receive remuneration in exchange for PHI unless the purpose of the exchange is for:
 - ___ Public health activities; or,
 - ___ Research; or,
 - ___ Treatment of the individual; or,
 - ___ A “health care provider” as defined in 6(iv) of health care provider under 164.501; or,

- ___ payment to a business associate for activities involving the exchange of PHI at the specific request of and on behalf of the Covered Entities pursuant to the Business Associates' agreement; or,
- ___ Giving the individual copy of PHI; or,
- ___ Purposes described in regulations.

Limitations on Marketing

- ___ **7. Communications about a product or service encouraging recipients to purchase/ use a product are not health care operations unless the communication is made:**
 - a) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in, a plan of benefits of the Covered Entities making the communication, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or,
 - b) For treatment of the person; or,
 - c) For case management/care coordination or to direct/recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

Communications described above are in the definition of "marketing" in (1) (i-iii) of 164.501 defining marketing.

Furthermore, such communications are not health care operations if the Covered Entities receive payment for such communication unless:

- a) The communication describes a drug/biologic that is currently being prescribed for the recipient of the information and any payment is reasonable; or,
- b) The communication is by the Covered Entities and the Covered Entities obtain an authorization from the individual; or,
- c) The communication is by Business Associates on behalf of the Covered Entities and the communication is consistent with the Business Associates' contract.

Covered Entities HITECH

Payment as used in this section does not mean payment for treatment.

- _____ **8. If Covered Entities have EHR, individual has right to get copy of PHI in electronic format and to direct Covered Entities to transmit copy to individual or third person. Cost cannot exceed Covered Entities' labor costs. [§ 13405(e)].**