Overview of the Proposed Rule:
Modifications to the HIPAA Privacy, Security, and Enforcement Rules
Under the Health Information Technology for Economic and Clinical Health Act
August 2010

[AHIMA has developed this summary to be of help to the healthcare industry as it considers this important proposal on revisions to the HIPAA Privacy and Security Rule. AHIMA will be publishing its comments and recommendations at a later date and this summary should not be viewed as AHIMA's position on the adoption of modifications to the HIPAA rules.]

On July 8, 2010, the Department of Health and Human Services (HHS) announced a proposed rule for the adoption of modifications to the Health Insurance Portability and Accountability Act of 2010 which has seen several modifications since first proposed in 2000. Many of the modifications in this notice were based on the American Recovery and Reinvestment Act (ARRA) of 2009's Title XIII – the Health Information Technology for Economic and Clinical Health Act (HITECH). HHS notes that these rules are part of the overall goal of HITECH – the adoption, implementation, and meaningful use of electronic health records (EHRs) and electronic health information exchange (HIE). On Wednesday, July 14, 2010, the official notice of proposed rulemaking was published in the *Federal Register* by the HHS Office of Civil Rights (OCR). The proposed rule modifies 45 CFR Parts 160 and 164.

An electronic copy of this Proposed Rule can be found on the electronic web pages of the *Federal Register* at http://www.access.gpo.gov/su_docs/fedreg/a100714c.html . Look for "Health and Human Services Department Proposed Rule."

KEY HIGHLIGHTS OF THE PROPOSED RULE

- The proposed rule updates the HIPAA privacy, security, and enforcement regulations with changes from ARRA-HITECH as well as other changes needed to update the previous requirements.
- **Comments** on the July 14, 2010 proposed rule **are due to HHS-OCR no later than September 13, 2010.**
- Once the final rule is posted, those HIPAA Covered Entities (CE) and their Business Associates (BAs) will have 180 days to comply. There will be an exception for the updating of Business Associate Agreements (BBAs) under certain circumstances.
- Many of the changes are technical to bring BAs under direct HIPAA privacy, security, and enforcements as required under HITECH.
- Subcontractors of BAs also fall under the proposed regulations.

- New definitions of "marketing" and "fund raising" provide new requirements for these activities as they relate to protected health information (PHI).
- The definition of electronic media has been expanded.
- The definition of PHI is changed when related to individuals who have been deceased for 50 or more years. There are also other changes to PHI related to deceased.
- The proposed rule covers investigations, and the application of civil money penalties.
- The proposed rule changes authorization requirements related to research.
- The proposed rule raises specific issues and requests comments including for:
    - The right of individuals to request information not be sent to their health plans for payment or operations;
    - The right of individuals to access their electronic PHI and request release of their electronic PHI to third parties;
    - Minimum Necessary and Limited Data Sets; and
    - Revisions to the Notice of Privacy Practices (NPP).

This HHS proposal for modifications to HIPAA privacy, security, and enforcement has a proposed compliance date of 180 days after the final rule is published in the *Federal Register*. There is an exception to this compliance period for requirements relating to business associate agreements (BAAs).

Comments on this proposed rule must be submitted on or before September 13, 2010. Instructions for submitting comments can be found on page 75FR40868. Comments must have the file code RIN: 0991-AB57.

Questions on the proposed rule can be directed to Andra Wicks at OCR at (202) 205-2292.

AHIMA has followed the ARRA HITECH and HIPAA Privacy and Security regulations closely and additional information can be found on the AHIMA web site at www.ahima.org.

NOTICE: ***This review of the "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act" is intended as an overview and not as a complete analysis of the rule. Readers seeking to comment on the proposed rule to the Department of Health and Human Services Office of Civil Rights are encouraged to read the entire rule and not rely on this or any other summary of the rule.***

I. Statutory and Regulatory Background (75FR40868)

This perfunctory section reviews the statutory and regulatory background for HIPAA Administrative Simplification as well as the statutory background for the HITECH Act and the recent history of regulations associated with HITECH including:

- On April 27, 2009, guidance was released (74FR19006) related to specifications for technologies and methodologies that render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals.

- On August 24, 2009, interim final regulations (IFR) on breach notification (74FR42740) were released. These regulations became effective September 23, 2009, although OCR permitted an extended period of compliance up until February 22, 2010. OCR has not issued a final rule on breach notification and recently pulled the proposed final rule from review by the Office of Management and Budget (OMB). There is no indication of when the final rule will be published.
- On October 30, 2009, OCR issued an IFR (74FR56123) on new additions to the Enforcement Rules, which included a new tiered and increased civil money penalty structure. This IFR became effective November 30, 2009.

II. General Issues (75FR408710)

A. Effective and Compliance Dates

OCR notes that many of the sections covered in the proposed rule were to take effect on February 18, 2010. OCR "recognize[s] that it will be difficult for covered entities and business associates to comply with the statutory provisions until after [it has]…finalized [its] changes to the HIPAA Rules…and [OCR] recognize[s] that covered entities and business associates will need some time beyond the effective date of the final rule to come into compliance with the final rule's provisions." Accordingly OCR has provided that covered entities (CEs) and business associates (BAs) will have 180 days beyond the effective date of the final rule to come into compliance with most of the rules provisions as generally the case under HIPAA. OCR further notes that "for purposes of this proposed rule…the 180-day compliance period would not govern the time period required to modify those BAAs that qualify for the longer transition period proposed in §164.532." OCR is seeking comments on any potential unintended consequences of establishing a 180-day compliance date as a regulatory default, with the noted exceptions.

OCR is not providing additional time for small health plans over the 180 days and indicates that in the future it does not see a reason to consider additional time for small health plans to implement changes to the rule.

B. Other Proposed Changes

OCR notes that in addition to the HITECH modifications to the HIPAA rules, OCR is also using this NPRM to clean up the language in HIPAA that has needed modification and also amending the rule to conform with the HIPAA Privacy Rule provisions of the Patient Safety and Quality Improvement Act of 2005 (PSQIA).

III. Section-by-Section Description of the Proposed Amendments to Subparts A and B of Part 160 (75FR40871)

The modifications to the HIPAA Section include new language that follows the same format as the original HIPAA rule. Many of the changes in Part 160 are made mainly to reflect the addition of BA compliance directly with the section. The overview will simply note sections and subsections and not go into further detail unless warranted.

Part 160 – General Administrative Requirements

§ 160.101 Statutory basis and purpose (75FR40872)

This section is changed to reflect the addition of Public Law 111-5 (ARRA-HITECH) sections 13400-13242 which change the HIPAA rules.

§ 160.102 Applicability (75FR40872)

This section is changed so that the original subsection (b) is changed to (c). The new subsection (b) reflects the new status of "business associate" and (b) reads:

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

§ 160.103 Definitions (75FR40872)

This section adds new definitions to HIPAA and modifies some of the existing HIPAA definitions. It is especially important to note the changes to the business associate definition and the new entities that become BAs under the HITECH revised HIPAA rule. Those added or modified include:

- *Administrative simplification provision* [modified and moved] means any requirement or prohibition established by:
    - 42 U.S.C. 1320d–1320d–4, 1320d– 7, and 1320d–8;
    - (2) Section 264 of Pub. L. 104–191;
    - (3) Sections 13400–13424 of Public Law 111–5; or
    - (4) This subchapter.
- *ALJ* [moved from §160.302] means an Administrative Law Judge.
- *Business associate:* [modified and expanded] (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

  (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

  (A) A function or activity involving the use or disclosure of protected health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

  (B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.
(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate. [*Note: this is a new section and a new concept of BA subcontractors.* OCR requests comments on the use of the term "subcontractor."]

(4) *Business associate* does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.
(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

[*Note that BAs now include Patient Safety Organizations. This is in addition to health information exchange organizations (HIEOs), HIOs, E-Prescribing Gateways and similar organizations that became effective with the signing of the ARRA-HITECH on February 18, 2009.* OCR requests comments on the names used in this section – see 75FR40873/column 1]

- *Civil money penalty* or *penalty* [moved from § 160.302] means the amount determined under § 160.404 of this part and includes the plural of these terms.

- *Compliance date* [modified] means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

- *Disclosure* [minor modification] means the release, transfer, provision of access to, or divulging in any ~~other~~ manner of information outside the entity holding the information.

- *Electronic media* [modified and expanded] means:

  (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

  (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet or intranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial- up lines, private networks, and the physical movement of removable/ transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form before the transmission.

- *Protected health information* [(2) is modified]

  Added (iv): (iv) Regarding a person who has been deceased for more than 50 years.

- *Respondent* [added] *means* a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

- *Standard* [modified (2)]means a rule, condition, or requirement:

  (2) With respect to the privacy of ~~individually identifiable~~ protected health information.

- *State* [modified (2)] refers to one of the following:

  (1) For a health plan established or regulated by Federal law, *State* has the meaning set forth in the applicable section of the United States Code for such health plan.

  (2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

- *Subcontractor* [added] means a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate.

- *Violation* or *violate* [moved from § 160.302] means, as the context may require, failure to comply with an administrative simplification provision.

- *Workforce [*expanded] means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the

direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

[*A new section 160.105 is added to HIPAA to accommodate the HIPAA changes.*]

§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.(75FR40874)

- In accordance with § 160.104, with respect to new standards and implementation specifications or modifications to standards and implementation specifications in this subchapter that become effective after July 14, 2010 except as otherwise provided, covered entities and business associates must comply with the applicable new standards and implementation specifications or modifications to standards and implementation specifications no later than 180 days from the effective date of any such standards or implementation specifications.

[*Section 160.201 is revised to reflect HITECH.]*

§ 160.201 Statutory basis.(75FR160.201)

The provisions of this subpart implements section 1178 of the Act, as added by section 262 of Public Law 104–191, section 264(c) of Public Law 104–191, and section 13421(a) of Public Law 111–5.

[*Section 160.20, under Subpart B – Preemption of State Law is revised to handle changes in the definitions to accommodate business associates*.]

§ 160.202 Definitions.(75FR40875)

- *Contrary,* [modified] when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

  (1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

  (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104–191, or sections 13400–13424 of Public Law 111–5, as applicable.

- *More stringent* [modify 1 (i.)]
  (1) * * *
  (i) Required by the Secretary in connection with determining whether a covered entity or business associate is incompliance with this subchapter; or…

IV. Section-by-Section Description of the Proposed Amendments to Subparts C and D of Part 160 (75FR40875)

§ 160.300 Applicability [*sections modified to reflect the revision to BA requirements*]
[Section 160.302 is removed and the definitions are now in 160.103.]

§ 160.302 [Removed and Reserved]

§ 160.304 Principles for achieving compliance. (75FR40875) **[***modified to include business associates***]**

§ 160.306 Complaints to the Secretary. (75FR40876)

Right to file a complaint. [*modified to reflect the revision to BA requirements*]

- (b) [*Requirements for filing complaints remain the same*.]

- (c) *Investigation* [modified and expanded].

  (1) The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.

  (2) The Secretary may investigate any other complaint filed under this section.

  (3) [*modified to reflect the revision to BA requirements*]

  (4) [*modified to reflect the revision to BA requirements*]

§ 160.308 Compliance reviews (75FR40876) [*modified and expanded*].

- The Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

- (b) [*sections modified to reflect the revision to BA requirements*]

§ 160.310 Responsibilities of covered entities and business associates.(75FR40876) [*sections modified to reflect the revision to BA requirements*]

§ 160.312 Secretarial action regarding complaints and compliance reviews. (75FR40876) [*sections modified to reflect the revision to BA requirements*]

§ 160.316 Refraining from intimidation or retaliation. (75fR40876) [*section modified to reflect the revision to BA requirements*]

[Subpart D – Imposition of Civil Money Penalties adds to the sections changed in the November IFR.]

§ 160.401 Definitions (75FR40877)

- *Reasonable cause* [*modified to cover business associate; however, OCR goes into a long discussion (40877-40879) of the legal aspects and liabilities established by this section even though the definition has only minor changes. This discussion in addition to reasonable cause also covers knowledge and reasonable diligence, willful neglect and correction of willful neglect violations.*]

§ 160.402 Basis for a civil money penalty. (75FR40879) [*while the section essentially adds business associate to the existing language, it is worth noting the section at this time for it adds some clarity to OCR's approach.*]

- *General rule.* Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision.

- (b) *Violation by more than one covered entity or business associate*.

  (1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate.

  (2) A covered entity that is a member of an affiliated covered entity, in accordance with § 164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter based on an act or omission of the affiliated covered entity, unless it is established that another member of the affiliated covered entity was responsible for the violation.

- (c) *Violation attributed to a covered entity or business associate.*

  (1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.

  (2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

§ 160.404 Amount of a civil money penalty**.** [*sections modified to reflect the revision to BA requirements*]

§ 160.406 Violations of an identical requirement or prohibition. [*section modified to reflect the revision to BA requirements*]

[*Subpart D – Imposition of Civil Money Penalties* begins with § 160.l408]

§ 160.408 Factors considered in determining the amount of a civil money penalty. (75FR40880)
[*We are showing this section to point out the changes in the language as well as the inclusion of BAs. The OCR discussion includes the determination of penalties after HITECH; the nature and extent of the violation as they impact penalties; the nature and extent of the harm resulting from the violations, and the history of prior compliance with the administrative simplification provisions. It should be noted that this proposed rule does not address "harm" as raised in the risk assessment necessary for breach notification.*]

In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:

- The nature and extent of the violation, consideration of which may include but is not limited to:

  (1) The number of individuals affected; and (2) The time period during which the violation occurred;

- (b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

  (1) Whether the violation caused physical harm;

  (2) Whether the violation resulted in financial harm;

  (3) Whether the violation resulted in harm to an individual's reputation; and

  (4) Whether the violation hindered an individual's ability to obtain health care;

- (c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

  (1) Whether the current violation is the same or similar to previous indications of noncompliance;

  (2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

  (3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

  (4) How the covered entity or business associate has responded to prior complaints;

- (d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

  (1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

(3) The size of the covered entity or business associate; and [*the size issue is interesting in this context since it is not unusual for a small covered entity to be working with a large business associate. The potential liability for the BA could be cause for requested changes in BAAs.*]

- (e) Such other matters as justice may require.

§ 160.410 Affirmative defenses.(75FR40881) [*There are a number of changes to this section underlined below. This extends through § 160.412 and § 160.418.*.]

- The Secretary may not:

  (1) Prior to February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that the violation is punishable under 42 U.S.C. 1320d–6. [*Several of these sections merely set the parameters for the various civil money penalties as established by HITECH.*]

  (2) On or after February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that a penalty has been imposed under 42 U.S.C. 1320d-6 with respect to such act.

- (b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:

  (1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or

  (2) The violation is—

  (i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated and is not due to willful neglect; and

  (ii) Corrected during either:
  (A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or
  (B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

- (c) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of the Secretary that the violation is—

  (1) Not due to willful neglect; and

  (2) Corrected during either:

  (i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or

  (ii) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

§ 160.412 Waiver

- For violations described in § 160.410(b)(2) or (c) that are not corrected within the period specified under such paragraphs, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation.

§ 160.418 Penalty not exclusive

- Except as otherwise provided by 42 U.S.C. 1320d–5(b)(1) and 42 U.S.C. 299b–22(f)(3), a penalty imposed under this part is in addition to any other penalty prescribed by law.

V. Section-by-Section Description of the Proposed Amendments to Subparts A of Part 164 and the Security Rule in Subpart C of Part 164 (75FR40881)

PART 164 – SECURITY AND PRIVACY

[*Authority is modified to include HITECH*]

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d—1320d–8; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320– 2(note)); and secs. 13400—13424, Pub. L. 111–5, 123 Stat. 258–279.

§ 164.102 Statutory basis.(75FR40881] [*Modifying for HITECH*]

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104– 191, and sections 13400—13424 of Public Law 111–5.

§164.104 Applicability (75FR40881) [*modify (b) to accommodate BA addition*]

§ 164.105 Organizational requirements (75FR40881) [*Several modifications are made to accommodate changes with the addition of HITECH. These need close reading and comment. Changes are in part caused by the breach notification requirements effective September 2009 and by the newly identified "subcontractors." This is again an area that could impact BAAs and other contracts among CE, BA, affiliated CEs, subcontractors, and some hybrid entities.*]

- (a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this part ~~subparts C and E~~, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

- (2) *Implementation specifications:*

  (i) *Application of other provisions.* In applying a provision of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

  [*A,B,C, and D remain the same under 2 (i*)]

  (ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

  (A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

  (B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

  (C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

  (iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

  (A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

  (B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with § 164.314 and § 164.504 regarding business associate arrangements and other organizational requirements.

(1) Covered functions; or

(2) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

- (b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.

(2) *Implementation specifications.*

(i) *Requirements for designation of an affiliated covered entity.*

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

[*The standard for documentation and implementation specifications for retention period remains as it was in HIPAA.*]

§ 164.106 Relationship to other parts. (75FR40882) [*section modified to reflect the revision to BA requirements*]

Subpart C – Security Standards for the Protection of Electronic Protected Health Information

§ 164.302 Applicability (75FR40882) [*section modified to reflect the revision to BA requirements*]

§ 164.304 Definitions (75FR40882 [*Two definitions changed to cover BAs. What is not known at the present time is the status of BA with the security administrative and physical safeguards. While the BA will be responsible to OCR under the revised HIPAA regulations it may not protect CEs from some liability if a BA fails to safeguard PHI.*]

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

§ 164.306 Security standards: General rules. (75FR40882) [*section modified to reflect the revision to BA requirements*]

§ 164.308 Administrative safeguards. (75FR40882) [*With one exception the changes only add BAs. The exception is in termination procedures. Beginning with (b) (1) the BAAs are modified.*

- (C) *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

- (b)(1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. [*While this statement is understandable under the proposed rule, it does not necessarily hold true for all cases and will require a legal risk analysis.*]

  (2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

  (3) *Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

[*It appears that (4) Implementation specifications: Written contract or other arrangement has been removed.*]

§ 164.310 Physical safeguards. [*section modified to reflect the revision to BA requirements*]

§ 164.312 Technical safeguards. [*section modified to reflect the revision to BA requirements*]

§ 164.314 Organizational requirements. (75FR40883) [*This section covers BAAs and subcontractors which is new with HITECH – see below.*]

- (a)(1) *Standard: Business associate contracts or other arrangements.* The contract or other arrangement required by § 164.308(b)(4) must meet the requirements of paragraph (a)(2)(i),(a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications* (Required).

(i) *Business associate contracts.* The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

[(D) *Termination of contract has been eliminated.*]

(ii) *Other arrangements.* The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

(iii) *Business associate contracts with subcontractors.* The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

- (b) [*Standard: Requirements for group health plans* remains the same.]

(2) [*Implementation specifications* for group health plans remains the same.]

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

§ 164.316 Policies and procedures and documentation requirements. (75FR40883)
[*Introductory text is changed to include business associates. The requirements remain the same.*]

VI. Section-by-Section Description of the Proposed Amendments to the Privacy Rule

Subpart E --- Privacy of Individually Identifiable Health Information

[*Authority is changed to reflect HITECH*]

Authority: 42 U.S.C. 1320d–2 and 1320d–4; sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)); and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279.

§ 164.500 Applicability. (75FR40883) [*A new subsection has been added to address BAs*]

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

§ 164.501 Definitions.

[*Definitions modified or new in this section include the following*:]

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to coved functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

[*All other subsections of "health care operations" remain the same.*]

[*The definition of marketing allows for the stricter interpretation from HITECH which Congress intended to stop certain current marketing processes. OCR is requesting comments – see pages 40884-40887for the rationale behind OCRs proposal.*]

Marketing:

(1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual, provided, however, that if the communication is in writing and the health care provider receives financial remuneration in exchange for making the communication, the requirements of § 164.514(f)(2) are met.

(ii) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(iii) For the following health care operations activities, except where the covered entity receives financial remuneration in exchange for making the communication:

(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 entity 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 case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) *Financial remuneration* means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

[*The original paragraph (2) has been removed from this definition*.]

C. Business Associates

§ 164.502 Uses and disclosures of protected health information: General rules. (75FR40887)
[*Given the context we are displaying the revised language in this section and as discussed on 40887and 40888.*]

- *Standard.* A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

  (1) *Covered entities: Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:
  (i) To the individual;
  (ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;
  (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;
  (iv) Pursuant to and in compliance with a valid authorization under § 164.508;
  (v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and
  (vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).

(2) *Covered entities: Required disclosures.* A covered entity is required to disclose protected health information:
(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and
(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

(3) [*Reserved]*

(4) *Business associates: Permitted uses and disclosures.* (i) A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e), or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(5) *Business associates: Required uses and disclosures.* A business associate is required to disclose protected health information:
(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.
(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

- (b) *Standard: Minimum necessary* [*There was an expectation that OCR would provide a revised standard, however this section calls for comments or recommendations and, of course BAs will now come under the Minimum necessary requirements.*]

  (1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

  [*(b) stays as stated; however, comments are requested…*]

  [*Subsections (c) and (d) remain as stated*]

- (e)(1) *Standard: Disclosures to business associates.* [*Changes are made due to the changes brought about by the status change for BAs. This is an extensive session and should be read carefully. The language here also addresses breach notification activities in part.*]

  (i) A covered entity may disclose protected health information to a BA and may allow a BA to create or receive PHI on its behalf, if the covered entity obtains satisfactory assurance that the BA will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. [*Note: This is stated as "not required." Some CEs might desire to have more detail in a contract or BAA.*]

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create or receive protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information. [*CEs might desire to also address the use of subcontractors in a contract or BAA.*]

(2) *Implementation specification: Documentation.* The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

- (f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

[Subsections *(g), (h), (i), and (j) remain as stated*.]

§ 164.504 Uses and disclosures: Organizational requirements. [*Again, changes are made in subsection (e) to reflect the BA changes and breach is discussed.*]

- (e)(1) *Standard: Business associate contracts.*

(i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible. [*This is a slight change from previous language in HIPAA.*]

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and
(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:
(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;
(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;
(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;
(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create or receive protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;
(E) Make available protected health information in accordance with § 164.524;
(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;
(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;
(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.
(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and
(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

[*This next section is mainly referencing changes in other sections – no content change per se.*]

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:
(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains

terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of *business associate* in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.*

[*No changes in (4).*]

(5) *Implementation specifications: Business associate contracts with subcontractors.* The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

[*Subsection (f), the* Standard: Requirements for group health plans *remains as written; however, subsection (2) under (f) Implementation specifications: Requirements for plan documents section (ii)(B) is revised.*]

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

[Further sections (C) – (J) remain as stated, as does (g) *Standard: Requirements for a covered entity with multiple covered functions.*]

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

[*The section below has been added to (c)* Implementation specifications: Treatment, payment, or health care operations.]

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

§ 164.508 Uses and disclosures for which an authorization is required.

[*The authorizations associated with uses and disclosures general rule and those associated with psychotherapy notes do not change. Changes begin with the Authorization required with Marketing and also cover the Sale of PHI (all new language), compound authorizations related to research - all changes that come from the HITECH legislation*

- (3) *Authorization required: Marketing*

  (i) [No change]

  (ii) If the marketing involves direct or indirect financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

- (4) *Authorization required: Sale of protected health information.*

  (i) Notwithstanding any provision of this subpart, a covered entity must obtain an authorization for any disclosure of protected health information for which the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the protected health information. Such authorization must state that the disclosure will result in remuneration to the covered entity.

  (ii) Paragraph (a)(4)(i) of this section does not apply to disclosures of protected health information:

  (A) For public health purposes pursuant to § 164.512(b) or § 164.514(e);

  (B) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

  (C) For treatment and payment purposes pursuant to § 164.506(a);

  (D) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

  (E) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate for the performance of such activities;

  (F) To an individual, when requested under § 164.524 or § 164.528;

(G) Required by law as permitted under § 164.512(a); and

(H) Permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

(b) *Implementation specifications: General requirements*

[*This specification is added to include the changes above.*]

(1) *Valid authorizations:*
(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(i), (c)(1), and (c)(2) of this section, as applicable.

(2) *Defective authorization:* [*No changes.*]

[*The section below addresses some of the issues related to the research community and the need for compound authorization (see OCR discussion on 40892). New language has been added as a result of HITECH.]*

- (3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

  (i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

  (ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

  (iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section

does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

[(b) (4), (5), and (6) along with (c) *Implementation specifications: core elements and requirements* remain the same.

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

[*Entry paragraph remains as written. (a) has only minor changes .]*

(a) Standard: Use and disclosure for facility directories
(1) Permitted uses and disclosure.
(i) [Entry remains as written.]
(ii) Use or disclose for directory purposes such information:

[(a) (2) *and* (a) (3*) remain as written*. (b) *had minor changes under (1) to reflect a new paragraph (b)(5) below. (b) has changes to referenced (b)(5), but note the added language in (3)and the new paragraph (b)(5)which referenced PHI related to deceased.*]

- (b) Standard: Use and disclosures for involvement in the individual's care and notification purposes:

  (3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes.

  (4) *Uses and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information … The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures …

  (5) *Uses and disclosures when the individual is deceased.* If the individual is deceased, a covered entity may disclose protected health information of the individual to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. [*As this is written there still could be state law considered more stringent. Also, the CE would have to keep the minimum necessary requirements in mind.*

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

[Entry paragraph and (a) *Standard: Uses and disclosures required by law* remain as written.]

- (b) *Standard: Uses and disclosures for public health activities.*
  (1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

[*Subsections(b)(1)(i) through (1)(iv) remain as written.*]

- (v) An employer, about an individual who is a member of the workforce of the employer, if;

  (A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

[*The remaining portion of (A) as well as (B), (C), and (D) remain as written. A new section (vi) is added to cover immunization records associated with school requirements. The OCR has a discussion on the release to schools (see 40895-40896) and requests comments. Issues with problems getting immunization records were raised in a number of National Committee on Vital and Health Statistic hearings and these proposed regulations are meant to alleviate the problems.*]

- (vi) A school, about an individual who is a student or prospective student of the school, if:

  (A) The protected health information that is disclosed is limited to proof of immunization;
  (B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and
  (C) The covered entity obtains the agreement to the disclosure from either:
  (*1*) A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or
  (*2*) The individual, if the individual is an adult or emancipated minor.

  [*Sections (c) and (d) remain as written*.]

- (e) *Standard : Disclosures for judicial and administrative proceedings.*

  (1) *Permitted disclosures.* A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:
  [*Subsections (i) and (ii) remain as written.]*

  (iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

  [*The remainder of subsection (iii) remains the same as do subsections (iv) and (v).]*

  (vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a

qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section.

[*Sections (f) through (j) while emphasized by OCR have no material changes (k) is changed to reflect the Department of Homeland Security which now includes the Coast Guard and Secret Service.*]

- (k) *Standard: Uses and disclosures for specialized government functions*

(1) *Military and veterans activities*

[*Section (i) remains as written.*]

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

[*The remainder of § 164.512 remain as written.*]

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

[*OCR uses this section to solicit comments (see discussion on 40896) with regard to minimum necessary. HITECH suggests that when possible a limited data set should be used. HITECH also requires that OCR issue guidance on the use of minimum necessary. To date ONC has not issued this guidance. Sections (a) through (d) remain as written.*]

- (e) (1) *Standard: Limited data set.*

[*Sections (e)(1) through (e)(3) remain as written; however (e)(4)(ii)(C)(4) is changed*.]

(*4*) Ensure that any agents to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

[*There are no changes to the remainder of (e)(4) or (e)(5).*]

[*(f) has some substantial changes to reflect the HITECH requirements to tighten fundraising use of PHI and the need for authorizations* .]

- (f) *Fundraising and remunerated treatment communications.*

(1)(i) *Standard: Uses and disclosures for fundraising.* Subject to the conditions of paragraph (f)(1)(ii) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose

of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:
(A) Demographic information relating to an individual; and
(B) Dates of health care provided to an individual.

(ii) *Implementation specifications: Fundraising requirements.*
(A) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1)(i) of this section unless a statement required by § 164.520(b)(1)(iii)(B) is included in the covered entity's notice of privacy practices.
(B) With each fundraising communication sent to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.
(C) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.
(D) A covered entity may not send fundraising communications to an the individual has elected not to receive such communications under paragraph (f)(1)(ii)(B) of this section.

(2) *Standard: Uses and disclosures for remunerated treatment communications.* Where a covered health care provider receives financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, in exchange for making a treatment communication to an individual about a health-related product or service, such communication is not marketing and does not require an authorization meeting the requirements of § 164.508, only if the following requirements are met:

(i) The covered health care provider has included the information required by § 164.520(b)(1)(iii)(A) in its notice of privacy practices; and

(ii) The communication discloses the fact that the covered health care provider is receiving financial remuneration in exchange for making the communication and provides the individual with a clear and conspicuous opportunity to elect not to receive any further such communications. The method for an individual to elect not to receive further such communications may not cause the individual to incur an undue burden or more than a nominal cost.

[(*iii) remains as written*.]

[*(g) and (h) remain as written*.]

§ 164.520 Notice of privacy practices for protected health information.

[*The notice of privacy practices (NPPs) has a number of changes to reflect the new requirements for authorizations and the disclosure of information as well as access. In its discussion (40897 – 40898) OCR discusses and requests comments on just how new NPPs might be written and distributed to the affected individuals, since the changes proposed here and elsewhere in the modified rule will require CEs to issue new NPPs at some point in time. Readers are reminded*

that this will also mean following the required steps to receive individual attestation that the new NPPs was received.]

[(a) Standard: notice of privacy practices *remains as written. (b) Implementation specifications: Content of Notice remains as written up until (ii)(E).]*

- (E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)–(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

- (iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:
  (A) In accordance with § 164.514(f)(2), the covered health care provider may send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, in exchange for making the communications, and the individual has a right to opt out of receiving such communications;
  (B) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications; or
  (C) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

- (iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:
  (A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under §164.522(a)(1)(vi);

[*The remainder of § 164.520 remains as written. Note: the accounting for disclosures changes required by HITECH will be addressed in a separate NPRM scheduled for August 2010.*]

§ 164.522 Rights to request privacy protection for protected health information.

[*This section is being changed to recognize the HITECH allowance for further restrictions on the disclosure of information by the individual. This is probably the most perplexing requirement in this set of modified requirements. OCR discusses this section's changes at 40899-40900 and acknowledges the problems that it presents to covered entities on a number of fronts including the administration associated with working with individuals. Comments are requested.*]

(a)(1) *Standard: Right of an individual to request restriction of uses and disclosures.*

(i) A covered entity must permit an individual to request that the covered entity restrict:

[*(i)(A) and (B) remain as written.*]

- (ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

[(iii) remains as written.]

- (vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:
(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

[*(a)(1 (v) remains as written.*]

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate a restriction, if:

[*(2)(i) and (ii) remain as written.*]

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:
(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and
(B) Only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.

[*The remaining sections under § 164.522 remain as written.*]

§ 164.524 Access of individuals to protected health information.

[*Subsections (a) through (b) remain as written.*]

(c) *Implementation specifications: Provision of access.* If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

[*(c)(1) remains as written.*]

(2) *Form of access requested.* (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

[*Section (ii) reflects new HITECH requirements related to PHI in electronic format or media. Note the negotiation issues between the individual and the CE.*]

- (ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

  (iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:
  (A) The individual agrees in advance to such a summary or explanation; and
  (B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.
  [*This next section addresses sending of copies of electronic records or PHI to third parties. This requirement raises previous issues of charging for copies to third parties.*]

- (3) *Time and manner of access.* (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

  (ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

[*There was some initial belief that OCR might address the cost of retrieval of PHI; however, this appears not to be the case.*]

- (4) *Fees* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

  (i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

  (ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

[*It appears that the original (ii) and (iii) are to be renumbered (iii) and (iv) respectively. The remainder of § 164.524 remains as written.]*

[As noted, Section 164.528 Accounting *for Disclosures* will be proposed separately from this NPRM per the HITECH legislation.]

§ 164.532 Transition provisions.

[*Subsections (a) through (c) remain as written. The remaining sections cover the transition now required to implement the above changes.*]

- (d) *Standard: Effect of prior contracts or other arrangements with business associates.*

  Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

- (e) *Implementation specification: Deemed compliance.*

  (1) *Qualification.* Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

  (i) Prior to [DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER], such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and

  (ii) The contract or other arrangement is not renewed or modified from [DATE THAT IS 60 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER], until [DATE THAT IS 240 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER].

  (2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

  (i) The date such contract or other arrangement is renewed or modified on or after [DATE THAT IS 240 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE FEDERAL REGISTER]; or

(ii) [DATE THAT IS ONE YEAR AND 240 DAYS AFTER DATE OF PUBLICATION OF THE FINAL RULE

VII. Regulatory Analyses and VIII. Collection of Information Requirements (75FR40904)

This is a required section, which begins on 75FR40904, for all NPRMs in which HHS must discuss the relationship of this regulation with other regulations, the estimated impact of this regulation on CEs and BAs, as well as other entities that may be involved. Since the estimates are made subject to change in the final rule at this time OCR estimates that over 700,000 NPPs will need to be distributed by a host of CEs. OCR also estimates burden hours across all affected groups will be 3,733,833 hours with the bulk, 2,000,000 hours dedicated to distribution of NPPs. BAs come in next with some 1,500,000 hours, however it is not clear whether this number takes into account all the potential BAs. It is also difficult to determine the demand that will be made from individuals as a result of the new HITECH requirements. Information from CEs and BAs during the comment period will provide additional information, but since these changes are required by law, they may modify some of OCR's approaches but will not stop these regulations from becoming final. Readers are urged to comment wherever possible.

List of Subjects (75FR40911)

This section lays out the changes as they would be made to HIPAA. We have attempted to replicate this outline in our analysis above.

– – –