OUTLINE: 45 CFR PARTS 160 AND 164 MODIFICATIONS TO THE HIPAA PRIVACY, SECURITY AND ENFORCEMENT RULES UNDER THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT; PROPOSED RULE

Published in Federal Register: August 24, 2009

NOTE: This outline is provided for reference only; no legal advice or analysis should be construed by or from its content.

Summary
a. Proposed rulemaking
b. Published in Federal register on July 14, 2010
c. Comments due in 60 days

I. Statutory and Regulatory Background
a. HIPAA Administrative Simplification – Statutory Background
   i. National standards for electronic transmission of certain health information
      1. health care transactions
      2. code sets
      3. unique health care identifiers for providers and employers
   ii. privacy and security protections
   iii. civil money and criminal penalties for violations
b. HIPAA Administrative Simplification – Regulatory Background
   i. Privacy Rule
      1. issued December 28, 2000
      2. amended August 14, 2002
   ii. Security Rule
      3. issued February 20, 2003
   iii. Enforcement Rule
      4. interim final rule April 17, 2003
      5. revised as final rule February 16, 2006
      6. governs investigations by Department
         a. investigation of complaints
         b. conduct of compliance reviews
         c. procedures for hearings and appeals
c. The HITECH Act – Statutory Background
   i. Designed to promote widespread adoption and standardization of health information technology (HIT)
   ii. Extends applicability of certain privacy and security rule requirements to business associates
   iii. Breach notification rules
   iv. Limits on marketing and fundraising
   v. Prohibition on sale of PHI (without specific Authorization)
   vi. Consideration of LDS as minimum necessary
   vii. Expands individuals’ rights
   viii. Strengthens and expands enforcement
   ix. Etc.
x. Not discussed in this proposed rulemaking:
   1. Breach notification provisions (subject to previous rulemaking)
   2. Modified civil money penalty structure (previous rulemaking)
   3. Accounting for disclosures requirement (tied to adoption of standard under HITECH Act)
   4. Penalty distribution methodology (based on recommendations to be developed at later date by GAO)
   5. New authority of State Attorneys General
   6. Studies, reports, guidance, audits or education efforts required by HITECH

d. HITECH Act – Regulatory Background
   i. Breach notification provisions
   ii. FTC final regulations on breach notification for Personal Health Records (PHRs)
   iii. Technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals
   iv. New tiered and increased CMP structure

II. General Issues
   a. Effective and Compliance Dates
      i. Most HITECH provisions took effect 2/18/2010
      ii. Exceptions:
         1. day after enactment (2/18/09) – tiered and increased CMPs for violations occurring after date of enactment
         2. breach notification IFR required within 180 days of enactment; effective date 30 days after publication
         3. on or after 2/18/11 – Secretary’s authority to impose CMP only barred to extent criminal penalty has been imposed rather than in cases in which offense in question merely constitutes offense criminally punishable
      iii. HHS will provide CEAs and BAs with 180 days beyond effective date of Final Rule to come into compliance with its provisions
         1. This will become new regulatory default time frame for compliance with standards or implementation specifications (proposed160.105)
      iv. additional 1 year to modify business associate agreements
   b. Other Proposed Changes
      i. Improving workability and effectiveness of all 3 sets of HIPAA rules; HHS has learned a lot since Rules went into effect!
      ii. Conforming HIPAA Privacy Rule to provisions in 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
      i. Adding reference to HITECH Act
   b. Subpart A – General provisions, Section 160.102 – Applicability.
      i. Make clear that standards, requirements and implementation specifications apply to business associates.
   c. Subpart A – General Provisions, Section 160.103 – Definitions
      i. Moving definitions of ALJ, CMP and violation/violate; reserving 160.302 from where they were moved
      ii. Replacing “IIHI” with PHI” in definition of “standard”
      iii. Definition of “administrative simplification provision”
      iv. Definition of “business associate”
- propose many modifications to definition of business associate

1. inclusion of PSOs as BAs
   a. added to list of functions and activities a person may undertake on behalf of a CE that give rise to BA relationship.

2. Inclusion of Health Information Organizations (HIOs), E-Prescribing Gateways, and Other Persons that Facilitate Data Transmission; as well as Vendors of Personal Health Records
   a. All are business associates!
   b. Data transmission organizations that do not require access to PHI on routine basis would not be business associates (as previously under HIPAA)

3. Inclusion of Subcontractors
   a. Those persons that perform functions for or provide services to a business associate other than in the capacity as a member of the BA’s workforce, are also business associates to the extent that they require access to PHI
   b. Definition added to HIPAA
   c. Definition would apply to any agent or other person who acts on behalf of the BA, even if no BAA in place.
   d. Goal is to protect downstream PHI
   e. Covered entity not required to have contract with subcontractor; obligation lies with business associates

4. Exceptions to Business Associate
   a. Treatment exception remains; added to definition of business associate

5. Technical Changes to the Definition
   a. IIHI changed to PHI in current definition of business associate
   b. BA has no obligation to IIHI that is not PHI

6. Definition of “Compliance Date”
   a. Add application of compliance date to BAs

7. Definition of “Electronic Media”
   a. Desire to clarify that physical movement of electronic media from place to place is not limited to magnetic tape, disk or compact disk. Removes a restriction as to what is considered to be physical electronic media, thereby allowing for future technological innovation.
   b. Transmission of information not in electronic form before the transmission, for example, paper or voice, is not covered by this definition.
   c. Revise definition to conform it to current usage – as set forth in Guidelines for Media Sanitization (Definition of Medium, NIST SP 800-88, Glossary B, p. 27)
   d. Add a reference to intranets to definition to clarify that intranets come within the definition
   e. Change word “because” to “if” in final sentence to encompass transmissions made by voice via telephone that exist in electronic form before transmission – some voice technology is digitally produced from an information system and transmitted by phone so would be encompassed in above definition.

External commentary: “The original definition became outdated quickly. The new one does allow for ongoing technological innovation and changes to be covered. Pointing to a NIST definition is a good way to have it more consistent with other laws and regulations that also use this definition.”
v. Definition of “Protected Health Information”
   1. PHI – HIPAA does not apply to IIHI of persons who have been deceased for more than 50 years.

   External commentary: According to the proposed rule, this change will reduce the burden on both covered entities and on those seeking the protected health information (PHI) by eliminating the need to search for and find the decedent’s personal representative to authorize the disclosure. HHS believes this change will benefit family members and historians who want access to this medical information for personal and public interest reasons.

vi. Definition of “Respondent”
   1. Moved definition from 160.302 to 160.103 and add reference to business associate to recognize potential liability imposed on BAs for violations of certain provisions of HIPAA

vii. Definition of “state”
   1. Add reference to American Samoa and the Commonwealth of the Northern Mariana Islands

viii. Definition of “workforce”
   1. Make clear that this includes employees, volunteers, trainees and other persons whose conduct, in performance of work for BA, is under direct control of BA.

d. Subpart B – preemption of State Law, Section 160.201 – Statutory Basis
   i. Add reference to section 264(c) of HIPAA which contains statutory basis for exception to preemption at 160.203(b) for state laws that are more stringent than HIPAA Privacy Rule.
   ii. Add reference to section 13421(a) of HITECH to apply HIPAA’s preemption rules to HITECH Act’s privacy and security provisions.
   iii. Re-title provision to read “Statutory basis” instead of “applicability”.
   iv. Make clear that section 264(c)(2) of HIPAA and 160.203(b) do not create federal evidentiary privilege.
   v. Make clear neither HIPAA statute nor implementing regulations give effect to state physician-patient privilege laws or provisions of state law relating to privacy of IIHI for use in Federal court proceedings.
   vi. Key: any state law that was preempted prior to HIPAA is still preempted (consistent with Supremacy Clause)

e. Subpart B – Preemption of State Law, Section 160.202 – Definitions
   i. Definition of “contrary”
      1. insert references to business associates
      2. expand reference to encompass all sections of subtitle D of HITECH (rather than only 13402 – breaches)
   ii. Definition of “more stringent”
      1. amend definition to add reference to business associates

IV. Section-by-Section Description of the Proposed Amendments to the Enforcement Rule – Subparts C and D of Part 160

➢ Interim Final Rule for Enforcement; effective February 18, 2009
   ▪ four categories of violations that reflect increasing levels of culpability and corresponding tiers of CMP amounts
(i) for violations in which CE did not know and by exercising reasonable diligence would not have known: amount not less than $100 or more than $50K for each violation
(ii) for violations due to reasonable cause and not willful neglect, an amount not less than $1000 or more than $50,000 for each violation
(iii) for violations due to willful neglect and that are timely corrected (30 days), amount not less than $10,000 or more than $50,000 for each violation
(iv) for violations due to willful neglect and that are not timely corrected, an amount not less than $50,000 for each violation

- A penalty for violations of same requirement or prohibition under any of these categories may not exceed $1.5M in a CY
- HITECH Sections 13401 and 13404 impose direct civil money penalty liability on business associates for violations of HITECH Act and certain Privacy & Security Rule provisions (effective 2/18/10)
- Term “business associate” added to 160.300, 160.304, 160.306(a) and (c), 160.308, 160.310, 160.312, 160.316, 160.401, 160.402, 160.404(b), 160.406, 160.408(c) and (d), and 150.410(a) and (c).
- Paragraph added 160.402(c)(2) – describes BA’s liability for actions of its agents in accordance with Federal common law of agency.
- Removed covered entity’s lack of knowledge as affirmative defense
- Provides for affirmative defense when violations not due to willful neglect are corrected within 30 days
- Added a requirement that notice of proposed determination also references the applicable category of violation (pursuant to 160.402)

a. Subpart C – Compliance and Investigations, Section 160.304 – Principles for achieving compliance
   i. Principle of cooperation – in 160.304(a) –“Secretary will to extent practicable seek the cooperation of CEs in obtaining compliance with applicable administrative simplification provisions.”
   ii. New subsection – Noncompliance due to willful neglect
       1. Secretary must impose a penalty if violation due to willful neglect
       2. Secretary must formally investigate any complaint if preliminary investigation of the facts indicates possibility of willful neglect.
       3. Willful neglect provisions effective February 18, 2011
       4. Secretary may seek to proceed directly to formal enforcement instead of seeking to correct noncompliance through voluntary corrective action

b. Subpart C – Compliance and Investigations, Section 160.306(c) - Complaints to the Secretary.
   i. Willful neglect – Secretary will investigate
   ii. Already conducting preliminary review of every complaint received and proceeding with investigation if indication of violation of HIPAA rules, but - this will make clear their intention to pursue investigations where possibility of willful neglect exists

c. Subpart C – Compliance and Investigations, Section 160.308 – Compliance Reviews
   i. Secretary may conduct compliance reviews if there is no indication of willful neglect
   ii. If preliminary review indicates possible violation due to willful neglect, Secretary WILL conduct compliance review
   iii. Brings consistency to investigations whether or not initiated by complaint
   iv. If Secretary initiates complaint investigation because preliminary review of facts indicates possible willful neglect violation, not also required to initiate compliance review (since duplicative)
d. Subpart C – Compliance and Investigations, Section 160.310 – Responsibilities of covered entities
   i. CE is responsible for making information available to Secretary and to cooperate with Secretary during complaint investigation or compliance review
   ii. Secretary allowed to disclose PHI if required by law
   iii. Secretary allowed to disclose PHI if permitted under Privacy Act (5 USC 552a(b)(7)) to another agency or instrumentality of any governmental jurisdiction within or under control of US for civil or criminal law enforcement activity if activity authorized by law and agency makes written request.
   iv. So – Secretary may now release PHI to cooperate with other law enforcement agencies:
      1. State Attorneys General pursuing HIPAA actions on behalf of state residents
      2. FTC pursuing remedies under other consumer protection authorities

e. Subpart C – Compliance and Investigations, Section 160.312 – Secretarial action regarding complaints and compliance reviews
   i. Clarifying – Secretary is not required to attempt to resolve cases of noncompliance due to willful neglect by informal means
   ii. If HHS makes finding of violation involving willful neglect – Secretary required to impose CMP.
   iii. Secretary could proceed directly to notice of proposed determination without having to attempt to resolve matter informally
   iv. However, CE or BA would be made aware of and have opportunity to address HHS’s compliance concerns

f. Subpart D – Imposition of Civil Money Penalties, Section 160.401 – Definitions
   i. Definitions of ‘reasonable cause’, ‘reasonable diligence’ and ‘willful neglect’ moved to signify broader application to entirety of subpart D of part 160. HHS worried some violations may not fit squarely into a penalty tier, therefore, they are amending definition of reasonable cause to clarify scope of violations fitting into this category
   ii. Worried that it would be difficult to determine mens rea (state of mind) for category II violations (reasonable cause); therefore
      1. reasonable cause = an act or omission in which a CE or BA knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the CE or BA did not act with willful neglect.
      2. Definition will recognize circumstances that would make it unreasonable for CE or BA to comply with HIPAA despite exercise of ordinary business care and prudence.
         a. example: patient requests access to file, CE doesn’t respond within timeframe but investigation reveals that CE had compliant policies in place but had unusually high volume of requests for access within time period in question. CE had knowledge of violations but circumstances existed that would make it unreasonable for CE to be able to comply with HIPAA. CE also:
            - acted in good faith by having p&p in place
            - responded to majority of access requests in timely manner
            - otherwise responded to subsequent requests as required
      3. Definition will also apply if CE or BA has knowledge of violation but lacks conscious intent or reckless indifference associated with willful neglect
a. example: authorization form presented to patient without all core elements required – CE aware of requirement and had attempted to draft compliant authorization but had mistakenly not done so.

iii. Knowledge and Reasonable Diligence
1. knowledge has to be that violation has occurred, not just knowledge of facts constituting violation
2. CE or BA cannot assert affirmative defense if doesn’t know – if lack of knowledge resulted from its failure to inform itself as to obligations
   a. Example: physician fails to provide patient with complete NPP but CE has good notice and procedures for giving it out and appropriate training of its workforce – but printing error was cause.
   b. Example: BA failed to terminate former employee’s access privileges -- but BA attempted to terminate access but terminated access of a different employee with same name instead.
3. Knowledge of employee or agent will generally be imputed to its principal
   a. Example: hospital employee accesses medical record of ex-spouse; CE had appropriate safeguards and training, so CE couldn’t have known. So, act attributed to employee but knowledge cannot be.

   “The Federal common law of agency does not permit the imputation of knowledge to the principal where the agent consciously acts in a manner that is adverse to the principal.”

iv. Willful Neglect
1. defined – conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated
2. presumes active or constructive knowledge as well as conscious intent or degree of recklessness with regard to compliance obligations.
3. HITECH Act does not revise the definition.
4. Examples:
   a. CE disposes of hard drives in unsecured dumpster; no policies/procedures, etc.
   b. CE fails to respond to request for restriction of disclosures of PHI. CE has no policies/procedures for consideration of this request.
   c. CE’s employee losses unencrypted laptop, CE doesn’t tell anyone fearing loss of reputation.
5. Correction of willful neglect
   a. Correction will not bar imposition of CMP, however, may allow Secretary to impose penalty from lower penalty tier
   b. “Correction” could include correction of CE’s noncompliant procedures by making the procedure compliant

    g. Subpart D – Imposition of Civil Money Penalties, Section 160.402 – Basis for a CMP
       i. CMP may be levied against CE for acts of its agent
       ii. Adding parallel provision so that CMPs may be levied against a BA for acts of its agent
       iii. Proposing to remove: exception for CE for the acts of its agent in cases where the agent is a business associate, the relevant contract requirements have been met, the CE did not know of a pattern or practice of the BA in violation of the contract and the CE did not fail to act as required by the Privacy or Security Rule with respect to such violations.
          1. Covered entity remains liable for acts of its BA, regardless of whether CE has compliant BAA in place
2. CE remains liable for the failure of its BA to perform that obligation on behalf of the CE
3. Don’t see this as undue burden since CEs are liable for acts of their agents under agency common law
4. Does not create liability for CEs with independent contractors; this will be based on facts of relationship – i.e. level of control CE has over entity’s conduct.

h. Subpart D – Imposition of Civil Money Penalties, Section 160.408 – Factors Considered in Determining the Amount of a CMP
i. Determination of Penalty Amounts Prior to the HITECH Act
   1. Secretary must take into account:
      a. Nature of claims and circumstances under which they were presented
      b. Degree of culpability, history of prior offenses and financial condition of person presenting the claims
      c. Such other matters as justice may require
      d. Specific to HIPAA –
         - Nature of violation in light of purpose of Rule
         - Circumstances, including consequences of violation
         - Degree of culpability of CE
         - History of prior compliance with administrative simplification provisions including violations by CE
         - Financial condition of CE
         - Such other matters as justice may require

ii. Determination of Penalty Amounts after HITECH Act
   1. requires Secretary to consider nature and extent of violation as well as nature and extent of harm resulting from violation
   2. excludes degree of culpability of CE as is redundant now with tiers
   3. Secretary’s consideration of all specific circumstances is optional
   4. “prior violations” – changed to “indications of noncompliance”
      a. Nature and Extent of the Violation
         - 1st factor Secretary must consider in determining amount of CMP
         - Includes time period during which violation occurred
         - Number of individuals affected
      b. Nature and Extent of the Harm Resulting from the Violations
         - 2nd factor Secretary must consider in determining amount of CMP
         - HHS adding reputational harm to make clear that this is as cognizable a form of harm as physical or financial harm
      c. The History of Prior Compliance with the Administrative Simplification Provisions
         - Violation normally reserved for formal findings of violation
         - CE’s general history of HIPAA compliance is relevant
         - Changing this to make regulatory language consistent with HHS’ policy of considering a CE’s general history of compliance.

i. Section 160.410 – Affirmative Defenses
   i. Effective February 18, 2011 – replaces “if the act constitutes an offense punishable under section 1177” with “if a penalty has been imposed” under 1177.
   ii. Prior to February 18, 2011 – affirmative defense of criminally “punishable” is applicable to penalties
iii. After February 18, 2011 – Secretary’s authority to impose CMP only barred to extent CE or BA can demonstrate that penalty has been imposed
iv. Replacing term “reasonable cause” with unrevised text of its current definition to ensure that current definition is applied to violations occurring prior to February 18, 2009 (conforming change)

j. Section 160.412 – Waiver
i. Aligning cross-references to 160.410 with proposed revisions to that section discussed above.

k. Subpart D – Imposition of Civil Money Penalties, Section 160.418 – Penalty Not Exclusive
i. Adding reference to Patient Safety and Quality Improvement Act of 2005 that provides that penalties are not to be imposed under both acts for the same violation.

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

i. Section 164.102 – Statutory Basis
   1. include reference to provisions of sections 13400 through 13424 of HITECH

ii. Section 164.104 – Applicability
   1. standards, requirements and implementation specifications of HIPAA Privacy, Security and Breach Notification Rules apply to BAs
   2. health care clearinghouse not required to comply with 164.105

iii. Section 164.105 – Organization Requirements
   1. Section 164.105
      a. Breach notification requirements apply here!
   2. Section 164.105(a)(2)(ii)(C)-(E)
      a. Removing paragraphs C and D pertaining to obligation of CE to ensure component that performs BA-like activities to be in compliance with HIPAA (when dealing with hybrid entities)
      b. BAs now directly liable for compliance provisions – should HHS require, rather than permit, CE that is a hybrid entity to include component that performs BA-like activities within its health care component so that such components are directly subject to the Rules? (requesting comment)
   3. Section 164.105(a)(2)(iii)(C)
      a. With respect to hybrid entity, CE itself, not merely health care component, remains responsible for 164.314 and 164.504 regarding BA arrangements and other organizational requirements
      b. Intended to recognize that hybrid entities may need to execute legal contracts and conduct other organizational matters at level of legal entity, rather than at level of health care component
   4. Section 164.105(b)(1)
      a. Fixing typo error
   5. Section 164.105(b)(2)(ii)
      a. Collapsing subparagraphs A, B and C into one provision

iv. Section 164.106 – Relationship to Other Parts
   1. add reference to business associates

b. Modifications to the HIPAA Security Rule in Subpart C
i. References to Business Associates
   1. Security Rule’s administrative (164.308), physical (164.310) and technical (164.312) safeguards requirements as well as its policies and procedures and documentation requirements (164.316) shall apply to BAs in same manner as to CEs
   2. BAs civilly and criminally liable for penalties for violations of these provisions
   3. Reference to BAs added to 164.302 (applicability), 164.304 (definitions), 164.308, 164.310, 164.312 and 164.316

ii. Section 164.306 – Security Standards: General Rules
   1. also adding reference to BAs in 164.306 – general rules
   2. CEs and BAs must review and modify security measures and update to be in compliance with 164.308, 164.310 and 164.312.

iii. Section 164.308 – Administrative Safeguards
   1. include volunteers in security termination procedures
   2. treatment exception to BAA going to be part of definition of BA – so removing reference to those exceptions from this subsection
   3. added to definition of business associate -- subcontractors that create, receive, maintain or transmit protected health information on behalf of a business associate
      a. so subcontractors are business associates!
   4. CE not required to have contract with subcontractor; i.e. not required to obtain satisfactory assurances in the form of a contract or other arrangement with a business associate that is a subcontractor of CE’s business associate.
   5. BA responsible to obtain required satisfactory assurances from subcontractor to protect ePHI
   6. Removing provision (164.308(b)(3)) where CE that violates satisfactory assurances it provides as a BA of another CE will be in noncompliance with Security Rule since CEs actions as a BA of another CE are now directly regulated by Security Rule’s provisions which apply to BAs.

iv. Section 164.314 – Organizational Requirements
   1. Agreements between BAs and subcontractors that create, receive maintain or transmit ePHI must contain all required elements as for agreements between CEs and BAs.
   2. removing 164.314(a)(1)(ii) – steps CE must take if it knows of material breach/violation by BA – parallel provision exists in Privacy Rule’s BA contract provisions (164.504), so this is redundant
   3. removing contract provision at 164.314(a)(2)(i)(D) authorizing termination of contract by CE if determines BA has violated material term of contract. Also redundant.
   4. removing specific requirements for other arrangements - such as MOU – when both CE and BA are governmental entities; instead referring to requirements of 164.504(e)(3); redundant also.
   5. BUSINESS ASSOCIATE CONTRACT MUST PROVIDE THAT THE BA WILL REPORT TO THE CE BREACHES OF UNSECURED PHI AS REQUIRED BY 164.410 OF BREACH NOTIFICATION RULES.
6. BA contract between BA and BA subcontractor must provide that subcontractor report any security incident of which it becomes aware, including breaches of unsecured PHI to BA.

7. So, subcontractor notifies BA which notifies CE which notifies affected individuals, Secretary and if applicable, the media of a breach of unsecured PHI.

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

a. Section 164.500 – Applicability

i. Where provided, standards, requirements and implementation specifications of the Privacy Rule apply to BAs.

b. Section 164.501 – Definitions

i. “health care operations” – amend to include reference to patient safety activities as defined in the PSQIA implementing regulation at 42 CFR 3.20.
   1. even though activities of PSO already encompassed within paragraph 1 of definition, HHS wants to expressly include patient safety activities to conform definition to PSQI and eliminate any confusion.

ii. “marketing” –
   1. propose changes to definition:
      a. revise exceptions to marketing to better distinguish exceptions for treatment communications from those made for healthcare operations
      b. add definition of financial remuneration; align with congressional use of term “direct or indirect payment” in HITECH
      c. provide that health care operations communications for which financial remuneration is received are marketing and require individual authorization
      d. provide that written treatment communications for which financial remuneration is received are subject to certain notice and opt out conditions
      e. provide limited exception from remuneration prohibition for refill reminders
      f. remove paragraph regarding arrangement between CE and another entity in which CE receives remuneration in exchange for PHI – as this now constitutes “sale of PHI” (addressed separately)
   2. propose to include notice and opt out conditions that would attach to written treatment communications (to revise 164.514(f)(2) and 164.520(b)(1)(iii)(A))
   3. propose to make conforming change to authorization requirements for marketing at 164.508(a)(3)(ii)

4. **marketing** = to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service

5. Three (3) exceptions:
   a. Certain health care operations communications if CE receives financial remuneration in exchange for making the communication
      - “direct or indirect payment” is wording from HITECH law; HHS substituting with term: “financial remuneration” to avoid confusion
b. **Financial remuneration = direct or indirect payment from or on behalf of a third party whose product or service is being described**
   - does not include any direct or indirect payment for the treatment of an individual
   - Only receipt of financial remuneration in exchange for making communication (as opposed to any other type of remuneration) is relevant for purpose of definition of marketing
   - Adding “financial” before “remuneration” for consistency with HITECH (payment)
   - Financial remuneration for purposes of marketing MUST be in exchange for making the communication itself and be from or on behalf of the entity whose product or service is being described
     1. example: authorization required prior to CE making communication to patients regarding acquisition of new state of art medical equipment if equipment manufacturer paid CE to send the communication to patients
     2. example: authorization not required if local breast cancer charitable organization foundation funded CE’s mailing to patients about availability of new state of art medical equipment such as mammography screening – since CE not receiving remuneration by or on behalf of entity whose product/service was being described.
     3. example: authorization not required if hospital sends flyers to patients announcing opening of new wing where funds for new wing were donated by 3rd party, since financial remuneration to hospital from third party was not in exchange for mailing of flyers.

c. **Statutory exception**– for communications regarding refill reminders or otherwise about a drug/biologic that is currently being prescribed for individual if financial remuneration received by CE for making communication is reasonably related to CE’s cost of making the communication.
   - Requesting comment on this exception as to types and amount of costs that should be allowed

d. **Must meet certain notice and opt out conditions for marketing treatment communications about health related products/services by health care provider to an individual including communications for case management or care coordination for individual or to direct or recommend alternative treatments, therapies, health care providers or settings of care to individual.**
   - Note: other non-treatment communications per above would be considered marketing.
   - Unclear how Congress wanted this treated regarding treatment communications, so:
     - NPP will require statement when provider intends to send subsidized treatment communications to an individual, as well as the opportunity for the individual to opt out of receiving such communications.

(Note: THIS WILL REQUIRE NOTICE OF PRIVACY PRACTICES [NPP] AMENDMENT)
- So, CE can send subsidized treatment communications if CE NPP includes following: 1) informs individuals that provider may send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remunerations from a third party in exchange for making the communication; 2) individual has right to opt-out of receiving communications; and 3) the treatment communication itself must disclose the fact of remuneration and provide individual with clear and conspicuous opportunity to elect not to receive any further such communications.

- Opt-out method may not cause individual to incur undue burden or more than nominal cost.

- Consider use of toll-free number, email address, similar opt-out mechanism for simple, quick inexpensive way to opt-out.

- Having individuals write and send in a letter is NOT ok; too burdensome.

- Request comments on:
  1. how opt out should apply to future subsidized tx communications (i.e. should opt out prevent all future subsidized treatment communications or just those dealing with particular product/service in current communication?)
  2. workability of requiring providers that intend to send subsidized tx communications to provide individual with opportunity to opt-out of receiving such communications prior to individual receiving first communication.

- Clarification: communications by health plan concerning health-related products or services included in plan of benefits or for case management or care coordination NEVER considered treatment communications – would be considered health care operations and would require authorization if financial remuneration involved.

- For subsidized communications by healthcare provider about health related products/services for case management or care coordination or to recommend alternative treatments or settings of care, whether communication would require authorization or statement in NPP and opportunity to opt out depends on -- to what extent provider is making communication in population-based fashion (health care operations) or to further tx of particular individual based on that individual’s health care status or condition (treatment).

- Example: pregnant patient gets brochure recommending specific birthing center suited to patient’s particular needs – treatment
  1. if provider receives financial remuneration for this -- required to: 1) include in NPP and 2) offer opportunity to opt out and 3) disclose the fact of remuneration with the communication and 4) provide information on how to opt out of receiving future such communications.
- Example: if provider sends blanket mailing to all patients with information about new affiliated physical therapy practice – is health care operations communications and if remuneration involved = marketing; if not remuneration involved = healthcare operations

- Face-to-face communications and promotional gifts of nominal value still exempt from marketing.

- Communications made to promote health in general – i.e. maintaining healthy diet or getting annual physical - still not marketing.

- Communications about government and government-sponsored programs do not fall within definition of marketing as there is no commercial component to communications about benefits available through public programs.

- No longer marketing: arrangement between CE and any other entity in which CE discloses PHI to other entity in exchange for remuneration, for the other entity or its affiliate to make communication about its own product or service that encourages recipients of communication to purchase or use that product/service
  1. This is SALE OF PHI now and requires specific authorization.

### c. Business Associates

i. Section 164.502 – Uses and Disclosures

1. BA must not use or disclose PHI except as permitted or required by Privacy Rule or Enforcement Rule

2. 164.502(a)(1) – applies only to CEs
   a. To individual
   b. TPO
   c. Incidental disclosure
   d. With authorization
   e. Pursuant to agreement under 164.510 (uses/disclosures requiring individual to agree or object – facility directories, involvement in care, etc.)
   f. As permitted by and in compliance with 164.512 (uses/disclosures for which opportunity to agree or object not required) and 514 e-g (limited data set, fundraising, underwriting & related purposes)

3. CE required to disclose PHI to Secretary to determine compliance with any of HIPAA Rules (not just Privacy Rule).

4. BAs only allowed to use or disclose PHI as permitted or required by their BAAs (referred to as “business associate contracts or other arrangement”) or as required by law.
   a. If no BAA then BA may use or disclose PHI only as necessary to perform its obligations for CE or as required by law; any other use/disclosure would violate Privacy Rule.
b. BA would not be permitted to use/disclose PHI in manner that would violate Privacy Rule except that BA may use PHI for proper management and administration of the BA, and the provision of data aggregation services for CE, if permitted by BA contract or other arrangement.
c. BAs required to disclose PHI when required by Secretary to determine BA’s compliance with HIPAA and to CE, individual or individual’s designee as necessary for access provisions to electronic PHI.

5. Minimum necessary standard applies to BAs when they use, disclose or request PHI – must limit PHI to minimum necessary to accomplish intended purpose of the use, disclosure or request.

6. CEs are not required to obtain satisfactory assurances from business associates that are subcontractors
   a. BAs must obtain satisfactory assurances, through written contract or other arrangement, from subcontractors that provide that subcontractor will comply with all applicable requirements of the Rules.

7. BAs may disclose PHI to BA that is a subcontractor and allow subcontractor to create or receive PHI on behalf of the BA if BA obtains satisfactory assurances that subcontractor will appropriately safeguard the information
   a. Required to enter into contract or other arrangement with subcontractor (same requirements as CE to BA contract)
   b. HHS believes that Bas are in best position to ensure that subcontractors comply with requirements of Privacy Rule

8. Direct liability attaches regardless of whether contractor and subs have entered into BAAs or not

9. Removing 164.502(e)(1)(iii) – CE that violates satisfactory assurances it provided as BA of another CE will be in noncompliance with Privacy Rule’s BA provisions – because new regulations covering BAs make this redundant

ii. Section 164.504(e) – Business Associate Agreements
   1. References HITECH Act Section 13404 – proposing number of modifications to this section to reflect “Department’s new regulatory authority with respect to business associates as well as to reflect a covered entity’s and business associate’s new obligations under subpart D to provide for notification in the case of breaches of unsecured PHI”.
   2. Revising 164.504(e)(1)(ii) – removing requirement that CEs report to Secretary when termination of BA contract not feasible - due to BA’s direct liability for CMPs for violations of HIPAA Rules and obligations to report breaches of unsecured PHI to CE, so HHS will find out about these instances in other ways now.
   3. Add new provision at 164.504(e)(1)(iii) applicable to BAs with respect to subcontractors to mirror requirements on CEs in 164.504(e)(1)(ii) – minus requirement to report to Secretary if termination of contract not feasible. If BA knew of pattern or practice of activity of its BA subcontractor that constituted material breach or violation of the subcontractor’s contract or other arrangement, BA must take reasonable steps to cure the breach of the subcontractor or to terminate the contract, if feasible.
   4. This implements intent of section 13404(b) of HITECH and aligns requirements for BAs with regard to BA subcontractors with requirements for CEs with regards to their BAs.
a. “A business associate that is aware of noncompliance by its business associate subcontractor must respond to the situation in the same manner as a CE that is aware of noncompliance by its business associate.”

5. BAs still contractually liable to CEs pursuant to their business associate contracts, however business associate contract requirements will now include:
   a. Requirement that business associates comply, where applicable, with Security Rule with regard to ePHI
   b. Requirement that business associates report breaches of unsecured PHI to CEs
   c. Requirement that BAs must ensure that any subcontractors that create or receive PHI on behalf of the BA agree to same restrictions and conditions that apply to the BA with respect to such information
   d. HHS: these revisions align requirements for BA contract with requirements in HITECH Act and elsewhere within HIPAA

6. New requirement – BA is contractually liable not only for uses and disclosures of PHI, but also for all other requirements of the Privacy Rule as they pertain to the performance of the BA’s contract
   a. Example: TPA fails to distribute plan’s NPP on timely basis, TPA not directly liable under HIPAA Rules but contractually liable for the failure. CE remains directly liable for failure to provide NPP in timely manner because its CE’s ultimate responsibility.

7. Business associate required to enter into business associate contracts or other arrangements that comply with the Privacy and Security Rules with their BA subcontractors in same manner that CEs must enter into contracts with their BAs

8. Removing reference to subcontractors to avoid confusion with use of the term (not substantive).

iii. Section 164.532 – Transition Provisions
   1. grandfathering certain existing contracts for specified period of time to prevent rushed and hasty changes to existing BA agreements
   2. CEs and BAs may continue to operate under certain existing contracts for up to one year beyond the compliance date of the revisions to the Rules if already existing contract or other written arrangement in place.
   3. if renewed or modified between effective date and compliance date of modifications to the Rules – grandfathering period would expire at end date of written contract
   4. would grandfather existing written agreements between BAs and subcontractors
      a. deemed in compliance with modifications until either CE or BA renews or modifies contract following compliance date of modifications or until date is one year after compliance date – whichever is sooner.
      b. If evergreen contract – eligible for extension; deemed compliance would not terminate when these contracts automatically roll over
      c. ONLY applies to written contracts or arrangements, not to ORAL agreements.
      d. This only affects the contracts – not the obligations of BAs, subcontractors under HIPAA.

   d. Section 164.508 – Uses and Disclosures for Which an Authorization is Required
      i. Sale of PHI
         1. authorization required under HIPAA for 1) psychotherapy notes and 2) uses and disclosures for marketing purposes
         2. HITECH adds third circumstance – sale of PHI
a. Exceptions:
   - Public health activities
   - Research purposes
   - If price charge for information reflects costs of preparation and transmittal of data
   - Treatment
   - Sale, transfer, merger or consolidation of all or part of CE and for related due diligence
   - Services rendered by BA pursuant to BAA and at specific request of CE
   - Providing an individual with access
   - Other purposes as Secretary determines necessary and appropriate

b. Effective 6 months after date of final regulations

3. To implement:
   a. CE must obtain authorization for any disclosure of PHI in exchange for direct or indirect remuneration
   b. Authorization must state that disclosure will result in remuneration to the CE. “CE is receiving direct or indirect remuneration in exchange for the PHI”
      - Allows individuals to make informed decision when deciding whether to sign form
   c. Exceptions included (from above and others):
      - For public health activities to public health authority
         1. if LDS – also excepted from authorization requirement
         2. HITECH allows Secretary to require that price charged for data reflects only costs of preparation and transmittal – Secretary not proposing this at this time but requesting public comment.
      - Research
         1. as long as remuneration received is reasonable, cost-based fee to cover cost to prepare and transmit information
         2. request public comment on types of costs that should be permitted
         3. also applies to disclosure of LDS of PHI
      - For treatment and payment purposes
         1. Act only addressed treatment
         2. HHS added disclosures for payment purposes
         3. excepting disclosures made for payment for health care from remuneration limitation to make clear that HHS doesn’t consider exchange of PHI to obtain payment to be sale of PHI!
      - For sale, transfer, merger or consolidation of all or part of CE with another CE or entity that will become CE (& related due diligence)
      - To or by a business associate for activities that BA undertakes on behalf of a CE
         1. Exempts disclosure of PHI by CE to BA or by BA to 3rd party on behalf of the CE as long as remuneration received by BA was for payment for activities performed pursuant to BA contract.
- To an individual
  1. excluding general access and accounting of disclosures
     provisions because:
     - CE may charge reasonable, cost-based fee for
       provision of access to individual’s PHI
     - accounting of disclosures = one without charge in
       any 12-month period but reasonable, cost-based fee
       for each subsequent request

- Disclosures that are required by law as permitted under
  164.512(a) (ADDED BY SECRETARY UNDER HER AUTHORITY)
  1. this way CE can continue to disclose PHI where required
     by law even if CE receives remuneration for the disclosure
     (requesting comment)

- Disclosures of PHI for any other purpose permitted by and in
  accordance with applicable requirements of subpart E. (ADDED
  BY SECRETARY UNDER HER AUTHORITY)
  1. Remuneration received MUST be reasonable, cost-based
     fee to cover cost to prepare and transmit PHI…
  2. or is fee otherwise expressly permitted by other law (state)
  3. Exception would not apply if CE received remuneration
     above actual cost to prepare, produce or transmit PHI
     (unless permitted by other law)
  4. So, if CE charging fees that conform to applicable State
     law, exception would apply (i.e. no authorization required)
   d. Applies to business associates as well
   e. Do not need to include statement that information disclosed by CE for
      remuneration can be further exchanged for remuneration by entity
      receiving information
       - However, if being disclosed to CE or BA – recipient CE or BA
      could not redisclose that PHI without another valid authorization.
      (requesting comment)

ii. Research
  1. compound authorizations
   a. 164.508(b)(4) – prohibits CEs from conditioning T, P,
      enrollment in a health plan, or eligibility for benefits on provision of an authorization
   b. Intended to prevent CEs from coercing individuals into signing
      authorization for use or disclosure not necessary to carry out services
   c. However, CE may condition provision of research-related treatment on
      obtaining individual’s authorization in limited situations - such as for
      clinical trials.
   d. Compound authorizations for research generally not allowed; HHS has
      received comments that this creates multiple forms, hassles, etc. and
      recruitment into clinical trials has been hampered by multiplicity of forms.
   e. Propose to allow CE to combine conditioned and unconditioned
      authorizations for research if: 1) authorization clearly differentiates
      between the two and 2) clearly allows individual the option to opt in to the
      unconditioned research activities.
   f. Gives CEs flexibility as to how they meet authorization requirements – i.e.
      use different pages for conditioned and unconditioned activities, cross-
      reference relevant sections, use separate check-box for unconditioned
research activity to signify whether individual has opted-in to unconditioned research activity, could have one signature line only or two distinct signature lines. (requesting comment)

2. Authorizing Future Research Use or Disclosure
   a. Currently, authorizations for research need to be study-specific and not look into the future
   b. However, HHS has gotten feedback that this encumbers secondary research, also diverges from current practice under Common Rule which allows consent to future research
   c. Requesting comment:
      - Should Privacy Rule permit authorization for uses and disclosures of PHI for future research purposes to extent they are adequately described in authorization?
      - Should it permit authorization for future research only to extent description included certain elements or statements specified by Rule?
      - Should it permit option #1 as general rule but require certain disclosure statements on authorization in cases where future research may encompass certain types of sensitive research such as involving genetic analyses or mental health research?
   d. Note: this would not alter individual’s right to revoke authorization for future research at any time! Authorization would still have to explain how an individual may revoke.

e. Protected Health Information about Decedents
   i. Section 164.502(f) – Period of Protection for Decedent Information
      1. Currently -- CE allowed to disclose PHI only if authorization from decedent’s personal representative
         a. personal rep = executor, administrator or other person who has authority under applicable law to act on behalf of decedent or decedent’s estate.
      2. Proposed – CE required to comply for period of 50 years following date of death
      3. Propose to modify definition of PHI to align with this – i.e. if date of death more than 50 years ago, not considered PHI.
      4. Note: doesn’t affect CE’s permitted disclosures for law enforcement purposes, to coroners or medical examiners and funeral directors, research activities solely for decedents or organ procurement organizations or others engaged in procurement, banking or transplantation of cadaveric organs, eyes, or tissue for purpose of facilitating organ, eye or tissue donation and transplantation.
   ii. Section 164.510(b) – Disclosures about a Decedent to Family Members and Others Involved in Care
      1. many people who have had access to health information of loved one prior to death have difficulty obtaining access after death because he/she doesn’t qualify as personal representative
         a. HHS proposes to allow CEs to disclose decedent’s information to family members and others involved in care or payment for care of decedent prior to death, unless doing so is inconsistent with any prior expressed preference of individual known to CE.
         b. Note: permitted -- not required
         c. Requesting comment on unintended consequences of this permissive proposal
d. Would not change authority of decedent’s personal representative to access or get accounting of PHI, etc.

f. Section 164.512(b) – Disclosure of Student Immunizations to Schools
   i. Currently, CEs may disclose PHI to: 1) public health authority for purpose of preventing or controlling disease, injury, etc.; 2) public health authority or other appropriate government authority to report child abuse etc.; 3) person/entity subject to jurisdiction of FDA to FDA about quality, safety or effectiveness of FDA-regulated product; 4) notify person that he/she is at risk of contracting or spreading disease or condition as authorized by law to carry out public health intervention or investigation; and 5) employer under limited circumstances and conditions when employer needs information to comply with OSHA or Mine Safety and Health Administration (MSHA) requirements.
   ii. Privacy Rule making it difficult for schools to obtain necessary immunization documentation for students.
   iii. Add provision: CEs permitted to disclose proof of immunization to schools in states that have school entry or similar laws.
      1. CE would still be required to obtain agreement from parent, guardian, etc.
         a. Oral agreement would be ok
         b. Potential for miscommunication and later objection by parent; therefore, requesting comment on whether oral permission (& documentation of it) should be allowed
         c. Should HHS mandate that disclosure go to particular school official?
         d. Requesting comment on scope of “school” – definition needed?
         e. Expand past those schools that may not be subject to school entry laws?
   2. Note: FERPA applies once school receives records

g. Section 164.514(d) – Minimum Necessary
   i. Current minimum necessary provisions:
      1. CEs must limit uses and disclosures of and requests for PHI to minimum necessary to accomplish intended purpose.
      2. exceptions apply
      3. CEs must identify workforce members who need access to PHI to identify categories and conditions of access and make reasonable efforts to limit access consistent to such policies
      4. CEs must adopt policies and procedures addressing minimum necessary – including regarding uses and disclosures that occur routinely.
   ii. HITECH – CE in compliance with requirements only if limits such PHI – to extent practicable – to LDS, or if needed, to minimum necessary.
   iii. Secretary to issue guidance on what constitutes minimum necessary within 18 months of enactment
      1. must consider:
         a. de-identification of PHI
         b. information necessary to improve patient outcomes and to detect, prevent and manage chronic disease.
      2. Secretary requesting guidance….

h. Section 164.514(f) – Fundraising
   i. HIPAA allows CE to use or disclose to BA or institutionally related foundation for its own fundraising purposes (without authorization) only 2 pieces of information without individual authorization:
      a. demographic information relating to individual
b. dates of health care provided to individual

1. CEs that do this must inform individuals of this in NPP and state that the CE may contact them to raise funds for the CE
2. CEs must also include opt out description in fundraising materials and must make reasonable efforts to ensure that individuals who do opt out are not sent future fundraising communications.

ii. Proposed regulations:

1. Require CE to provide “clear and conspicuous” (vs. “must include”) opportunity for individual to elect not to receive further fundraising communications with each fundraising communication sent to an individual – so HITECH strengthens this already-existing HIPAA requirement
   a. Method can’t cause undue burden or more than nominal cost on individual
   b. Encourage use of toll-free number or email address
   c. Writing letters would be considered “undue burden”

2. CE may not condition treatment or payment on individual’s choice to receive fundraising communications (new wording to implement congressional intent in HITECH)

3. CE may not send fundraising communications to individual who has elected not to receive such communications. Current provision says CE must “make reasonable efforts” not to send fundraising communications after individual has elected not to receive them – so HITECH strengthens this already-existing HIPAA requirement.

4. Requesting comment on what fundraising communications should apply to opt out:
   a. i.e. if individual receives fundraising letter and opts out should this apply to all future fundraising communications or only those that apply to the particular fundraising campaign in letter?
   b. Should there be an easy way for an individual to opt back in? such as toll-free number, etc.

5. Requesting comment on expanding information CE may use or disclose for fundraising – such as adding department of service where care received, outcomes information, etc. If so, should this be added to NPP? Adequacy of minimum necessary standard to appropriately limit amount of PHI used or disclosed?
   a. Should individuals be given option to opt out of even first fundraising solicitation?

i. Section 164.520 – Notice of Privacy Practices for Protected Health Information (NPP)

i. Currently:

1. CE must include separate statements about uses and disclosures that CE intends to make for certain T, P or O activities
2. Must state that any other uses and disclosures other than permitted by Privacy Rule will be made only with written authorization and that individual may revoke authorization at any time

ii. Proposed:

1. NPP must include statement that describes uses and disclosures of PHI that require authorization and provides that other uses and disclosures not described in NPP will be made only with individuals’ authorization
   a. Purpose is to indicate to individuals that most disclosures of PHI for which remuneration is received – would require authorization.

2. NPP must explain that most uses and disclosures of psychotherapy notes and marketing purposes would require authorization.
a. HHS is worried that individuals may assume that psychotherapy notes and marketing are included in treatment, payment and operations permissions when they are not – want CEs to make clear to individuals that these two categories of disclosures require authorization

3. 164.520(b)(1)(iii) changes:
   a. Covered healthcare provider that intends to send treatment communications concerning tx alternatives or other health related products or services where provider receives financial remuneration in exchange would be required to inform individual in advance in NPP
      - Must also inform individual of their right to opt out of this
   b. If CE intends to contact individual to raise funds for CE, CE must not only inform individual of this fact, but also must inform the individual that he/she has the right to opt out of receiving fundraising communications
   c. Must notify individuals of their right to request restrictions based on new HITECH requirement of restricting PHI for P or O (not T) being sent to an individual’s health insurer if the individual pays for an item/service out of pocket and in full at the time of service and requests the restriction.
      - Currently NPPs state that the CE is not required to agree to any restrictions for the purposes of T, P or O.
   d. Requesting comment on whether breach notifications regulations should be included here in specific statement
   e. THESE ARE MATERIAL CHANGES TO NPP so CE will be required to promptly revise and distribute NPP as per 164.520(c)
      - Most CEs: “must promptly revise and distribute its Notice whenever there is a material change...”
      - Health plan requirement: “must provide notice within 60 days of a material revision to the Notice, to individuals then covered by the plan”
      1. HHS recognizes it may be costly for health plans to redistribute new NPP so HHS considering allowing plans to notify in next annual mailing to members, provide delay or extension of 60-day timeframe, retain provision but provide that Secretary will waive 60-day timeframe in cases where timing or substance of modifications call for such a waiver or make no change. Requesting comment on this.
      - Not worried about direct treatment providers as must only have available at delivery site, post new NPP and make available upon request.

j. Section 164.522(a) – Right to Request Restriction of Uses and Disclosures
   i. Add that a CE, upon request from an individual, must agree to a restriction on the disclosure of PHI to a health plan if:
      1. disclosure is for payment or healthcare operations and not otherwise required by law, and
      2. PHI pertains solely to healthcare item/service for which individual has paid the CE in full.
   ii. CE also required to restrict disclosure to a business associate of a health plan once individual has triggered above request (as it would be the same as disclosing to the CE)
   iii. CE cannot require individual to apply this restriction to all care given by the provider – i.e. can’t make individual pay for all items/services out-of-pocket and in full if and individual triggers this Right.
iv. CEs encouraged to work with individuals to determine best method for ensure this right is effectuated
   1. i.e. physician who is already restricting information to a health plan about a certain treatment should not electronically submit prescription information to a pharmacy if patient wants that restricted as well – should issue paper prescription instead.
   2. requesting comment on this
   3. requesting comment on obligation of providers that know of restriction to inform other healthcare providers downstream of this restriction.
      a. What if an individual asks the provider to send his/her information to another provider? must the provider carve out this information before sending to the other provider?

v. Provider does not have to agree to this if it is “required by law” – defined at 164.103.

vi. Not solely limited to individual as anyone may be paying for this on individual’s behalf.

vii. Note that if individual requests this restriction they should not expect that this payment will count towards any deductibles or out-of-pocket thresholds for insurance.
   1. requesting comment as to how this will work for HMOs; would the individual have to use an out-of-network provider to effectuate this Right?

viii. If an individual’s out of pocket payment is not honored (i.e. check bounces) CE may submit information to health plan for payment
     a. provider under no obligation to restrict information; however, HHS expects that CE will make some attempt to resolve payment issue with individual prior to sending info to health plan such as notifying individual of non-payment and provide them with opportunity to submit payment
     b. HHS requesting comment

ix. Follow-up treatment:
   1. If individual visits provider for follow-up treatment and asks provider to bill health plan for follow-up treatment and doesn’t request a restriction at the time, nor pays out of pocket for the tx, no restriction is in effect for this treatment episode.
   2. However, provider may need to submit original tx information to health plan to determine medical appropriateness or necessity for follow-up care.
   3. HHS considers lack of restriction for follow-up tx to extend to any PHI necessary to effect payment for such tx, even if this information was subject of previous restriction.
   4. Encourage CEs to have discussion with individuals to ensure they are aware of possible disclosure of previously-restricted information
   5. HHS requesting comment

k. Section 164.524 – Access of Individuals to Protected Health Information
   i. Individual have a right to review or obtain copies of their PHI, to extent such information is maintained in the designated record set, of a CE. (HIPAA)
   ii. Right of access exists regardless of format of PHI
   iii. HITECH allows for access to information electronically if contained within an EHR
   iv. HHS proposing to strengthen this right of access to incorporate all PHI maintained in one or more designated record sets electronically, regardless of whether the designated record set is an EHR.
   v. If PHI requested is maintained electronically in one or more DRSs, CE must provide individual with access to the electronic information in electronic form and format requested by individual if readily producible, or if not, in readable electronic form and format as agree to by CE and individual
vi. So, if CE maintains DRS electronically, it must provide individual with electronic copy. CE may make other agreement with individual as to alternative means to provide readable electronic copy if requested means is not readily available.
   1. example: CE requested to provide electronic access via secure web-based portal but only readily producible version of PHI in PDF, CE could provide individual with PDF copy of PHI if agreed to by CE and individual.
      a. i.e. nothing would require the CE to give an individual access to their record through a portal if CE didn’t consider this reasonable or appropriate.
   2. option of arriving at alternative agreement that satisfies both parties is already a part of HIPAA, so HHS believes that extension of this requirement to electronic access shouldn’t be problematic
   3. CEs must ensure that reasonable safeguards are in place to protect the information transferred to individuals
   4. invite public comment on this

vii. Individual may direct a CE to transmit ePHI directly to entity or person designated by individual if such choice clear, conspicuous and specific.
   1. for both paper and electronic form
   2. HHS proposing: individual’s request must be in writing, signed by the individual and clearly identify designated person and where to send the copy of PHI
      a. Individual may request electronically
      b. Individual may sign electronically – to extent valid under applicable law
      c. So, CE could employ electronic process for receiving individual’s request to transmit copy of PHI to his/her designee

viii. CE must implement reasonable policies and procedures under 164.514(h) to verify identity of any person who requests PHI, as well as implement reasonable safeguards under 164.530(c) to protect the information that is used or disclosed

ix. Currently costs for copies may only include cost of supplies for and labor of copying the PHI and postage and/or preparing a summary or explanation

x. HITECH provides that CE may not charge more than its labor costs in responding to the request for the copy.

xi. HHS:
   1. identify separately labor for copying PHI whether in paper or electronic form
   2. costs for paper copies would stay the same
      a. i.e. may not include costs associated with searching for and retrieving information
      b. reasonable cost-based fee for electronic copies includes costs attributable to labor involved to review the access request and produce electronic copy (which HHS expects to be negligible)
         - do not expect to see standard “retrieval fee” that doesn’t take into account actual labor costs associated with the retrieval of the ePHI or reflects charges unrelated to the individual’s request
         - invite public comment on this
      c. separate costs – supplies for creating paper copy or electronic media
         - if individual requests information to be provided on portable media, can charge for this (i.e. flash drive)
            1. however, if individual brings own media in and requests that information be place on it and the CE’s systems can do this – CE couldn’t require individual to buy their own media
- Cannot charge for behind the scenes costs for electronic information such as computer, scanners, or software used to generate response (unlike paper copy which you can charge for paper, wear and tear on copying machine, pro-rated toner.)

- If individual requests electronic information be sent via unencrypted email, CE should advise individual of risks associated with unencrypted email, but CE would not be allowed to require individual to instead purchase a flash drive
  
  I. Did they mean to say this?

- CE can charge for postage if individual requests that CE transmit portable media containing PHI through mail or courier

d. HHS requesting comment on timeliness of responding to access requests

  - HITECH didn’t change this; however, HHS feels electronic access can be made “without unreasonable delay and not later than 30 days”

  - HHS also requesting comments on whether extra 30-day timeframe for off-site records should be eliminated for both paper and electronic – or just electronic information

I. Other Technical and Conforming Changes

  i. Number of technical and conforming changes made to Privacy Rule to fix minor problems.

  ii. Other changes – adding ‘use’ to disclose when dealing with directory information in hospitals, changing “Transportation” with “Homeland Security” as this function was transferred to Homeland Security in 2003, etc.

VII. Regulatory Analyses

  a. Introduction

  i. Executive Order 13866

  ii. Regulatory Flexibility Act

  iii. Unfunded Mandates Reform Act

  iv. Federalism

b. Why is this Rule Needed?

c. Costs

  i. Notifying Individuals of Their New Privacy Rights

  1. $166.1 Million within 12 months of effective date

  2. This includes following additions to NPP:

  a. Addition of sale of PHI as use or disclosure that requires express written authorization

  b. Statement that provides advance notice to individual if provider receives financial remuneration from third party to send treatment communications to individual and right of individual to elect not to receive such communications

  c. Right to restrict disclosure of PHI to health plan if individual has paid out of pocket in full

  ii. Authorization and Other Requirements for Disclosures

  iii. Related to Marketing and Sale of PHI

  iv. Authorization for Compound Disclosures

  v. Uses and Disclosures of Decedents’ PHI

  vi. Uses and Disclosures for Care and Notification Purposes

  vii. Public Health Disclosures
viii. Fundraising Requirements
ix. Individuals’ Access to PHI
x. Business Associates and CEs and Their Contractual Relationships
d. Benefits
   i. To individuals
      1. added information on their rights through expanded NPP
      2. greater control over uses and disclosures of their personal health information by expanding requirements to obtain authorizations
      3. easier access to their PHI in electronic format
      4. relatives and friends of deceased persons now able to obtain person’s PHI when no personal representative exists
      5. Personal health information of decedents available to historians, researchers, family members.
      6. individuals’ rights to fundraising communications strengthened
      7. schools would have easier time obtaining immunization records
      8. individual’s PHI would be afforded greater protection due to protection of downstream PHI
e. Regulatory Flexibility Analysis
   i. Requires agencies to analyze and consider options for reducing regulatory burden if will impact substantial number of small entities
   ii. Extended BAA timeframe for compliance
   iii. Plan to provide sample language for revising contracts

VIII. Collection of Information Requirements
a. Abstract
   ii. Revisions to NPP – estimating each revision would take 20 minutes to complete (!)
   iii. Bigger burden on health plans – one hour to prepare 100 NPPs for mailing to individuals; total burden to disseminate – 200 million “burden hours”.
   iv. Assumption that BAs already in compliance with HIPAA
      1. BAs may renegotiate their contracts during compliance period
      2. subcontractors will present burden – will have to initiate BAAs with them
   v. HHS assuming majority of burden from HITECH will be for 1) NPP changes and 2) costs for business associates
b. Estimated Annualized Burden Table

PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS

160.101 Statutory basis and purpose.

160.102 Applicability.

(a) Where provided, the standards, requirements and implementation specifications of this subchapter apply to business associates.

160.103 Definitions.
**Administrative simplification provision** = any requirement or prohibition established by: (1) 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** = Administrative Law Judge

**Business associate:**

(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 health care 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.

(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.

**Civil money penalty or penalty** – amount determined under § 160.404 of this part and includes the plural of these terms.

**Compliance date** - 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** - the release, transfer, provision of access to or divulging in any manner of information outside the entity holding the information.
**Electronic media:** (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) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.

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

**Standard** - a rule, condition, or requirement: (1) Describing the following information for products, systems, services, or practices: (i) Classification of components; (ii) specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of protected health information.

**State** - 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** 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** (as the context may require), failure to comply with an administrative simplification provision.

**Workforce** - 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.

160.104 Compliance dates for new or modified standards and implementation specifications
   i. 180 days after publication of the Final Rule in the Federal Register

160.201 Statutory basis.

160.202 Definitions

**Contrary,** 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 (I)*** (i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or ****

160.300 Applicability

160.302 [Removed and Reserved]

160.303 Principles for achieving compliance.

(a) Cooperation.

(b) Assistance.

160.306 Complaints to the Secretary.

(a) Right to file a complaint
(b) ***
(c) Investigation
   i. 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.

160.308 Compliance reviews.

(a) Secretary to conduct compliance review to determine whether CE or BA is complying with applicable administrative simplification provisions when preliminary review of facts indicates possible violation due to willful neglect.

(b) Secretary may conduct compliance review to determine whether CE or BA is complying with applicable administrative simplification provisions in any other circumstance.

160.310 Responsibilities of CEs and BAs

(a) Provide records and compliance reports
(b) Cooperate with complaint investigations and compliance reviews
(c) Permit access to information

160.312 Secretarial action regarding complaints and compliance reviews

(a) Resolution when noncompliance is indicated.
   a. Secretary may attempt to reach resolution by information means
      i. Demonstrated compliance
      ii. Complete corrective action
      iii. Other agreement
   b. If resolved informally, Secretary will inform CE or BA and complainant (if involved)
   c. If matter not resolved informally, Secretary will:
      i. Give CE or BA opportunity to submit written evidence of mitigating factors or affirmative defenses
      ii. Must submit evidence to Secretary within 30 days
      iii. If CMP to be imposed, Secretary will inform BA or CE in notice of proposed determination.

(b) Resolution when no violation is found.
   a. Secretary will inform CE or BA and/or complainant in writing
160.316 Refraining from intimidation or retaliation
(1) CE or BA may not threaten, intimidate, coerce, harass, discriminate against or take any other retaliatory action against any individual or other person for …

160.401 Definitions.

**Reasonable cause** – an act or omission in which a CE or BA knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the CE or BA did not act with willful neglect.

160.402 Basis for a civil money penalty.
(a) Secretary will impose CMP on CE or BA if determines violation of administrative simplification provision
(b) Violation by more than one CE or BA
   a. CMP against each CE or BA responsible for violation
   b. CE that is member of affiliated CE jointly and severally liable for CMP for violation based on act or omission of affiliated CE unless another member of affiliated CE was responsible for violation.
(c) Violation attributed to a CE or BA.
   a. CE is liable (federal common law of agency) for CMP for violation based on act/omission of any agent of CE including workforce member or BA, acting within the scope of the agency.
   b. BA is liable (federal common law of agency) for CMP for violation based on act or omission of any agent of the BA including a workforce member or subcontractor acting within scope of agency.

160.404 Amount of a civil money penalty.

160.406 Violations of an identical requirement or prohibition.

160.407 Factors considered in determining the amount of a civil money penalty.
(a) The nature and extent of the violation, consideration of which may include but is not limited to the number of individuals affected; and the time period during which the violation occurred;
(b) The nature and extent of the harm resulting from the violation…
(c) The history of prior compliance with the administrative simplification provisions, including violations, by the CE or BA…
(d) The financial condition of the CE or BA…
(e) Such other matters as justice may require.

160.410 Affirmative defenses.

160.412 Waiver.

160.418 Penalty not exclusive.
(a) penalty imposed under this part is in addition to any other penalty prescribed by law

**PART 164 – SECURITY AND PRIVACY**

164.102 Statutory basis.

164.103 Applicability
164.104 Organizational requirements

(a) Standard: health care component.
   a. if hybrid entity, requirements of this part only apply to healthcare component
   b. CE that is hybrid entity must ensure that health care component of the entity complies with this part
      i. healthcare component cannot disclose PHI to another component if circumstances would prohibit such disclosure if they were separate and distinct legal entities
      ii. healthcare component protects ePHI with respect to another component of the CE to same extent it would if component and other component were separate and distinct legal entities.
      iii. if person performs duties for both parts, workforce member cannot use/disclose PHI created or received in the course of or incident to the member’s work for healthcare component in away prohibited by subpart E.
   c. CE that is hybrid entity must:
      i. implement policies and procedures to ensure compliance including safeguard requirements
      ii. must be in compliance with business associate arrangements and other organizational requirements.

(b) Standard: Affiliated covered entities.
   a. Legally separate CEs that are affiliated may designate themselves as a single CE for purposes of this part.
   b. If under common ownership or control
   c. Designation must be documented and maintained.

164.106 Relationship to other parts.

164.304 Applicability.

164.304 Definitions.

Administrative safeguards = administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect ePHI and to manage the conduct of the CEs or BAs workforce in relation to the protection of that information.

Physical safeguards = physical measures, policies, and procedures to protect a CE’s or BA’s electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

(a) CEs and BAs must do the following:
   a. ensure confidentiality, integrity and availability of all ePHI the CE or BA creates, receives, maintains or transmits.
   (b) CE and BAs may use any security measures that allow the CE or BA to reasonable and appropriately implement the standards and implementation specifications as specified in this subpart.
      a. CE or BA must take into account
         i. Size, complexity and capabilities of CE or BA
         ii. CE or BA’s technical infrastructure, hardware and software security capabilities.
   (c) Standards – CE or BA must comply with applicable standards for all ePHI.
Maintenance – CE or BA must review and modify security measures implemented to continue provision of reasonable and appropriate protection of ePHI and update security measures as necessary.

164.308 Administrative safeguards.
(a) Risk analysis (Required). – conduct accurate and thorough assessment of potential risks and vulnerabilities to confidentiality, integrity and availability of ePHI held by CE or BA.
(b) Sanction policy (Required). – apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the CE or BA.
(c) Standard: Assigned security responsibility.
(d) Termination procedures (Addressable).
   a. Implement procedures for terminating access to ePHI when the employment of or other arrangement with a workforce member ends
(e) Access establishment and modification (Addressable). Implement p&p that establish, document, review and modify a user’s right of access to a workstation, transaction program or process.
(f) Implementation specification: Response and Reporting (Required).
   a. Identify and respond to suspected or known security incidents; mitigate, to extent practicable, harmful effects of security incidents known to the E or BA and document security incidents and their outcomes.
(g) Standard: evaluation.
   a. Perform a periodic technical and nontechnical evaluation based initially upon standards implemented under this rule and subsequently in response to environmental or operational changes affecting the security of ePHI that established the extent to which a CE’s or BA’s security P&P meet the requirements of this subpart.
(h) Business associate contracts and other arrangements.
   a. CE doesn’t have to make subcontractors a BA
   b. BAs must ensure subcontractor will appropriately safeguard information given to it.
   c. Implementation specifications: Written contract or other arrangement (Required.)
      i. Document satisfactory assurances through written contract with BA

164.310 Physical Safeguards.
   (includes reference to business associates)

164.312 Technical Safeguards.
   (includes reference to business associates)

164.314 Organizational requirements.

164.316 Policies and procedures and documentation requirements.

164.500 Applicability.

164.501 Definitions.
(a) Health care operations
(b) Marketing
(c) Financial remuneration means direct or indirect payment form 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

164.502 Uses and disclosure of PHI: General rules.

164.504 Uses and disclosures: Organizational requirements
164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(4) Authorization required: Sale of PHI
   “Must obtain an authorization for any disclosure of PHI for which the disclosure is in exchange for direct or indirect remunerations from or on behalf of the recipient of the PHI. Such authorization must state that the disclosure will result in remuneration to the CE.”

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

(5) Uses and disclosures when the individual is deceased
   “If the individual is deceased, a CE may disclose PHI 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 CE.”

164.514 Other requirements relating to uses and disclosures of PHI

f. Fundraising and remunerated treatment communications.

164.520 Notice of privacy practices for PHI.

164.522 Rights to request privacy protection for PHI.

164.524 Access of individuals to PHI.

164.532 Transition provisions.