Analysis of Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules

January 25, 2013

On Tuesday, February 17, 2009, President Barack Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA), also known as Public Law 111-5. Within that Act was Title XIII, the Health Information Technology for Economic and Clinical Health Act (HITECH). Included in this Title were a number of sections addressing the promotion and incentives for adopting, implementing, and using electronic health records; however, Subtitle D – "Privacy" – included sections that address requirements significantly revising the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA – Public Law 104-191) regulations (45 CFR Parts 160-164) that had not been fundamentally changed for almost a decade. This analysis covers these new requirements.

With the adoption of HITECH, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) quickly published two interim final rules addressing HITECH privacy requirements for Breach Notification and Enforcement. The 2013 final rule includes provisions that make those "interim final" rules final. This omnibus rule, however, does not address all of the Congressional HITECH Privacy requirements, including the provision for the Accounting of Disclosure, which OCR indicates will be released at a later date.

Included in this final rule are requirements that have been added to the HIPAA requirements related to the Genetic Information Nondiscrimination Act of 2008 (GINA – Public Law 110-233). The GINA requirements added here apply to the genetic information that a health plan might use in underwriting and other activities.

This analysis describes a review of the January 25, 2013 *Federal Register*, Part II, 45 CFR Parts 160 and 164 Rules and Regulations. The American Health Information Management Association (AHIMA) intends this information to provide health information management professionals, including HIPAA privacy or security officers, insight into these new rules and regulations and their requirements. This analysis does not take the place of an individual reading the actual *Federal Register* publication for more detail than can be provided here, but is intended to aid in an entity's steps to become compliant with the HITECH-HIPAA requirements.

Electronic copies of the final rule published on January 25, 2013 can be found at the Government Printing Office website at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

AHIMA fully expects that over time, there will be additional information coming from the OCR, the entity to which these regulations have been designated for oversight and enforcement, at its website

http://www.hhs.gov/ocr/privacy/. AHIMA will also be developing additional information on the rules, their effect, and how to address these requirements in the months to come. In addition, AHIMA will be updating the AHIMA Practice Briefs impacted by these regulations and modifications. Information from AHIMA can be found in its *Journal of AHIMA* and its website, www.ahima.org. AHIMA will also be offering a series of webinars and in-person meetings related to these final rules.

Key Highlights of the HITECH/GINA Updates to HIPAA Privacy and Security Requirements:

- Business associates must follow the Security Rule for electronic protected health information.
- Business associates have business associate agreements with their subcontractors who must also follow the security rule for electronic protected health information (PHI).
- Covered entities do not have business associate agreements with business associates' contractors.
- Marketing requires an authorization.
- Financial remuneration is defined.
- Exceptions to marketing are still in place.
- Business associates must obtain authorizations prior to marketing.
- Grandfather clause for business associate agreement transition
- Sale of PHI
- Compound authorizations for research
- Authorizing future research for use or disclosure
- Any individually identifiable health information of a person deceased more than 50 years is no longer considered PHI under the Privacy Rule.
- Covered entities are now permitted to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of a decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the CE.
- Covered entities can disclose proof of immunization to a school where state or other law requires it prior to admitting a student. Written authorization is no longer required, but an agreement must still be obtained, which can be oral.
- Covered entities must provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications and that the individual's choice to opt out is treated as a revocation of authorization under the privacy rule.
- The Notice of Privacy Practices must be revised and redistributed.
- Required restriction to health plan
- Access to electronic PHI
- Form and format of electronic copies
- Fees for paper and electronic copies
- Timeliness for paper and electronic records
- The Breach Notification Rule's "harm" threshold is removed and replaced with a more objective standard.
- Title I of GINA required the Secretary to revise the HIPAA Privacy Rule.
- Genetic information is health information.
- Genetic information may not be used or disclosed for underwriting purposes.
- Excludes long-term care plans from the underwriting prohibition

Effective and Compliance Dates [78FR5566]

The effective date for these regulations, as required by HIPAA, is March 26, 2013. The compliance date for these regulations is September 23, 2013.

Under HIPAA, the regulation's effective date is 60 days after publishing in the *Federal Register*. This was to permit Congress to intervene if it thought regulations did not comply with the intent of the legislation. There is no sign that there will be an intervention at this time. The compliance date is 180 days after the rules are effective. OCR explains in some detail (78 FR) why it chose to go with the minimum timeline under HIPAA.

Further Information from OCR [78FR5566]

The official contact for further information is Andra Wicks at (202) 205-2292. The OCR website that houses all of the privacy and security regulations and frequently asked questions (FAQs) and other information is http://www.hhs.gov/ocr/privacy/.

Supplementary Information [78FR5566]

I. Executive Summary and Background [78FR5566]

A. Executive Summary:

The rule begins with an Executive Summary that includes:

- The purpose (and need for this regulatory action;
- The legal authority for the regulation:
  - ARRA-HITECH, 2009
  - The Genetic Information Nondiscrimination Act (GINA) of 2008;
- A summary of major provisions:
  - Final modifications of HIPAA by HITECH and certain modifications proposed in July 14, 2010. These modifications:
    - "Make business associates of covered entities directly liable for compliance with certain HIPAA Privacy and Security requirements;
    - Strengthen the limitations on the use and disclosures of protected health information (PHI) for marketing and fundraising purposes and prohibit the sale of PHI without individual authorization;
    - Expand individuals' rights to receive electronic copies of their health information (HI) and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full;
    - Require modification to, and redistribution of, a covered entity's notice of privacy practices (NPP);
    - Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members; and

        - Adopt the additional HITECH enhancements to the Enforcement Rule previously adopted in the October 31, 2009, interim final rule including enforcement.
    - Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increase and tiered civil money penalty structure provided by HITECH originally published as an interim rule on October 30, 2009.
    - Final rule on Breach Notification for Unsecured PHI under HITECH , which replaced the Breach Notification Rule's 'harm' threshold with a more objective standard and supplants an interim final rule published August 24, 2009.
    - Final rule modifying the HIPAA Privacy Rule as required by GINA to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009."
- Cost and benefits of the regulation

B. Statutory and Regulatory Background [78FR5567]

This section provides a brief background on HIPAA, GINA, and HITECH Acts. OCR notes that these current regulation modifications do not include rulemaking for:

- Accounting of Disclosure, originally proposed May 31, 2011, or
- Penalty distribution methodology, which will be the subject of separate regulations.

These regulations also for the first time apply not only to covered entities, but also in part to business associates and their contractors.

II. Overviews of the Final Rule [78FR5568]

Summary of the sections of the new rule

III. Effective and Compliance Date [78FR5569]

This section notes that there are a variety of effective and compliance dates associated with the original HITECH Act, even though the bulk of the act was to be effective a year after enactment (February 17, 2009) on February 18, 2010. Many of the requirements contained in this January 25, 2010 rule were to take effect on that February 18, 2010 date. OCR does not explain the delay in these regulations, now almost three years late, but also notes that these new regulations also complete several interim final rules that did become effective in or since 2009.

OCR indicates that the new regulation changes some of the HIPAA regulations to note that most compliance dates will go into effect 180 days after the effective date and exceptions will be noted. OCR discusses comments made by the public and its rationale for using 180 days.

OCR notes:

- All regulations contained in this final rule will have a 180-day compliance period, except for the requirement for business associate agreement modifications.

IV. Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the HITECH Acct Other Modifications to the HIPAA Rules [78FR5570]

A. Subparts A and B of Part 160: Statutory Basis and Purpose, Applicability, and Definitions, and Preemption of State Law [78FR5570]

In this section, OCR makes changes in the HIPAA rules to conform to the new requirements under HITECH and GINA. This requires the some movement of sections as well as new or revised definitions.

1. Subpart A – General Provisions, Section 106.101 – Statutory Basis and Purpose [78FR5570]

Technical changes for HITECH affected by GINA are described.

2. Subpart A – General Provisions, Section 160.102 – Applicability [78FR557]

Statutory references for HITECH and GINA modifications to HIPAA are identified.

3. Subpart A – General Provisions, Section 160.103 – Definitions [78FR5570]

a. Definition of "Business Associate" adds the following entities:

- Patient Safety Organizations
- Health Information Organizations (HIOs)
  - See http://www.hhs.gov/ocr/privacy/hipaa/faq/providers/business/245.html for more information.
  - OCR goes into an extended discussion of what constitutes a business associate, including the difference between an entity providing transit for PHI versus storage. The discussion also discussed the various entities that OCR believes are HIOs and notes that it will offer further guidance in the future to define who is or is not a business associate. This guidance will be outside of regulation and will occur on the OCR website. OCR also discusses the situations where a vendor of personal health records (PHR) is also a business associate.
- Subcontractors inclusion in the definition of business associate
  - There is a significant discussion as to the relationship between business associates and their subcontractors and so forth, making all of these entities dealing with PHI subject to the same requirements as subcontractors and ensuring that covered entities do not need business associate agreements for anyone other than the (prime) business associate.
- Exceptions to Business Associates
- Technical Changes to the Definition of Subcontractor
- Response to Other Public Comments – discusses comment made to clarify relationships that might be considered business associates. The discussion clarifies that researchers and institutional review boards are not business associates and suggests http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/239.html as a source for further information.

The definition of a "Business Associate" changes significantly and now reads [78FR5668]:

"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, creates, receives, maintains, or transmits PHI for a function or activity regulated by this subchapter, 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 (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 PHI 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 PHI to a covered entity and that requires access on a routine basis to such PHI. (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 PHI 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 PHI 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."

b. Definition of **"Electronic Media" [78FR5688]**

Discussion in this section addresses the changes in technology that have occurred over time and calls for the change in the definition. The discussion calls readers to look to the National Institute of Standards and Technology (NIST) (http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf) for further information and clarifies situations where fax transmissions would not come under the rule. Furthermore, the discussion notes that PHI potentially held in technical/mechanical instruments such as copiers, etc., are subject to HIPAA security rules.

The definition of "Electronic Media" now reads [78FR5688-changes]:
(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, extranet or intranet, 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 immediately before the transmission."

c. Definition of **"Protected Health Information" [78FR5576]**

The OCR notes that its proposal to modify PHI when the individual has been deceased for more than 50 year will go forward therefore changing this definition.

The definition of "Protected Health Information" now reads [78FR5689 modified in part]:
"(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."

d. Definition of "State"

America Samoa and the Northern Marian Islands have been added to the definition of "state."

e. Other changes to definitions (78FR5576)

This section notes minor changes to other definitions.

4. Subpart B – Preemption of State Law [78FR5576]

a. Section 160.201—Statutory Basis [78FR5576]
This section discusses limited discussion on comments and minor language changes to previous HIPAA rules.

b. Section 160.202 – Definitions [78FR5577]

The definition of "Contrary" was modified slightly to read [78FR5577]:
"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."

The definition of "More Stringent" was modified slightly to read [78FR5566]:
"More stringent (1) (i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter."

B. Subparts C and D of Part 160: Amendments to the Enforcement Rule [78FR5577]

This section describes modifications to the Enforcement Rule to reflect other changes occurring from HITECH.

1. Subpart C of Part 160-Complance and Investigation [78FR5578]

a. Section 160.304, 160.306, 160.308, and 160.312 – Noncompliance Due to Willful Neglect [78FR5578]

In this section, OCR describes changes necessary in its investigations of probable or possible willful neglect including compliance review. This discussion notes that the HITECH changes call for a more deliberate investigation and penalties than the previous approach for just changes that would bring the entity into compliance. The changes in the section's language signal this tougher enforcement, whether through a complaint and investigation that finds probably or possible "willful neglect," the discovery of such through a general compliance review, or identification through some other source such as a media story or similar identification. Due to the legislation, the section notes that OCR, when willful neglect is found, must proceed with civil money penalties. The section also describes the OCR's approach to initial complaints, noting that it begins an investigation on all complaints.

b. Section 160.310 – Protected Health Information Obtained by the Secretary [78FR5579]

This section describes situations where OCR (the Secretary) will provide individual PHI to other federal or state agencies under the Privacy Act. Examples given include state attorneys general who are pursuing HIPAA violations, the Federal Trade Commission, or the Federal Bureau of Investigation.

2. Subpart D – Imposition of Civil Money Penalties [78FR5579]

a. Section 160.401 – Definitions [78FR5579]

OCR notes the need to move definitions of "reasonable cause," "reasonable diligence," and "willful neglect to reflect changes necessary to implement HITECH provisions. OCR also indicates it will expand on these concepts on its web page.

OCR is modifying the definition of "Reasonable Cause" and this section describes why the definition is being change and what it means.

The definition of **"**Reasonable Cause" now reads:
"Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect."

b. Section 160.402 – Basis for Civil Money Penalty [78FR5580]

This section gets into a very long discussion on the issue of "agent" and the Federal Common Law of Agency and the impact of the culpability of a covered entity or business associate's relationships that would result in the basis for a civil money penalty due to the action of the second party depending on whether they were an agent. The section highlights the need for legal review of business associate agreements or contracts, as well as any business associate contract with a subcontractor handling PHI and whether they are acting as an agent. While the section is detailed, it does not replace the need for legal review to determine liability under the HIPAA and perhaps other obligations.

c. Section 160.404 – Amount of Civil Monetary Penalty [78FR5582]

The interim final rule established that penalties will apply to any action that occurred on or after February 18, 2009.

The new rule reminds readers of the penalty windows set in the interim final rule:

Table 2 – Categories of Violations and Respective Penalty Amounts Available

Violation Category - Section 1176 (a) (1)	**Each Violation**	**All Such Violations of an Identical Provision in a Calendar Year**
(A) Did Not Know	$100 - $50,000	$1,500,000
(B) Reasonable Cause	$1,000 - $50,000	$1,500,000
(C)(i) Willful Neglect-Corrected	$10,000 - $50,000	$1,500,000
(C)(ii) Willful Neglect-Not Corrected	$50,000	$1,500,000

OCR goes into depth to discuss how it will apply these penalties, especially the upper limits, which it notes provides the Secretary with flexibility to address the specific situation. This approach has been used by OCR and will continue to be used.

OCR also describes "affirmative defenses" that a covered entity might consider should it fall into one of the lower categories, including the taking of corrective action within the 30 days provided. OCR explains that the Secretary also has the right under HIPAA to modify civil money penalties when the prescribed penalty may not fit the violation. Therefore, it appears that OCR will continue to use its discretion even with these more defined penalties, and this section identifies the statutes under which the Secretary might act and under which a covered entity might appeal a penalty.

In response to questions related to how OCR counts violations, OCR responded: "Generally speaking, where multiple individuals are affected by an impermissible use or disclosure, such as in the case of a breach of unsecured protected health information, it is anticipated that the number of identical violations of the Privacy Rule standard regarding permissible uses and disclosures would be counted by the number of individuals affected. Further, with respect to continuing violations, such as lack of appropriate safeguards for a period of time, it is anticipated that the number of identical violations of the safeguard standard would be counted on a per day basis (i.e., the number of days the entity did not have appropriate safeguards in place to protect the protected health information)." OCR also notes "that in many breach cases, there will be both an impermissible use or disclosure, as well as a safeguards violation, for each of which the Department may calculate a separate civil money penalty. We refer readers to prior Enforcement Rule preambles for additional discussion on the counting methodology."

OCR further clarifies that the $1.5 million cap is per a type of violation and there could therefore be multiple violations that could result in a much higher amount.

d. Section 160.408 – Factors Considered in Determining the Amount of a Civil Money Penalty [78FR5584]

The section begins by reviewing the factors that the Secretary/OCR must use for determining the penalty. These include the degree of culpability, history of prior offenses, and the financial condition of the person investigated. Because the Enforcement Rule applies to a number of rules, which apply to an enormous number of entities and circumstances, the Secretary/OCR has the direction to decide whether and how to consider the factors (i.e., as either aggravating or mitigating) in determining the amount of a civil penalty. The HITECH Act added "harm" as a factor in determining civil money penalties. The interim final rule proposed to exclude "degree of culpability" since this now resides in the tiered penalties section. In updating this section to abide with HITECH, OCR also added the factors of:

- "Number of individuals involved;"
- "The time period during which the violation(s) occurred;"
- "Reputational harm;" and
- "Prior violations."

OCR also notes that in determining "harm to the individual" it will consider effects on "employment, standing in the community, or personal relationships." Also, OCR will use "prior indications of noncompliance" and compliance, rather than "history of violations" since the latter would assume previous investigations that found violations, which may not be the case. Similarly, OCR will look at its history of complaints and previous compliance or correction steps taken by the entity.

e. Section 160.410 – Affirmative Defense [78FR5585]

The affirmative defenses previously permitted in HIPAA have been modified to exclude the defense of "did not know" since this defense is no longer permitted but is included in the lowest tier of penalties. The defense of the entity having been "criminally punished" is applicable to penalties imposed prior to February 18, 2011, and on or after February 18, 2011, the Secretary's authority to impose a civil money penalty will only be barred to the extent a covered entity or business associate can demonstrate that a criminal penalty had been imposed. The modifications are for violations that occur after February 18, 2009.

f. Section 160.412 – Waiver [78FR5586]

Essentially, this section is modified to provide the Secretary with the ability to waive a penalty in whole or in part where the situation can be shown to be a violation where the covered entity was not cognizant of the violation but had also been following prudent business practices.

g. Section 160.418 – Penalty Not Exclusive [78FR5586]

This section was revised to reflect that an entity cannot be penalized under the Patient Safety and Quality Improvement Act of 2005 (PSQIA) and HIPAA for essentially the same violation.

h. Section 160.420 – Notice of Proposed Determination [78FR5586]

The Secretary/OCR, in a notice of proposed determination of a violation and penalty, will identify the applicable violation category upon which the proposed penalty amount is based.

i. Calculation of the 30-day Cure Period for Willful Neglect Violations [78FR5586]

The final rule retains the policy that the 30-day cure period for violation due to willful neglect, like those not due to willful neglect, begins on the date that an entity first acquires actual or constructive knowledge of the violation and will be determined based on evidence gathered by the HHS during its investigation on a case-by-case basis. OCR goes on to indicate that it is aware that 30 days may not be enough time for correction but notes that the statute limits the period to 30 days. OCR also notes that enforcement is for all sections of administrative simplification and not just privacy and security.

C. Subparts A and C of Part 164: General Provisions and Modifications to the Security Rule [78FR5587]

1. Technical Changes to Subpart A—General Provisions [78FR5587]

a. Section 164.102—Statutory Basis [78FR5587]

This section sets out the statutory basis to include a reference to the provisions of sections 13400 through 13424 of the HITECH Act.

b. Section 164.104—Applicability [78FR5587]

This section adds the statement that this applies to business associates.

c. Section 164.105—Organizational Requirements [78FR5588]

For hybrid entities, this outlines the organizational requirements and implementation specifications for health care components. OCR makes it clear that the provision of this section also applies to breach notification for unsecured PHI.

i. Section 164.105(a)(2)(ii)(C)–(E) – Application of other provisions [78FR5588]

The hybrid entity provision of the HIPAA rules now requires that the healthcare component of a hybrid entity include all business associate functions within the entity. The hybrid entity applies the rules to its components that perform functions that would make the component a "covered entity" if it were a separate entity. While most of the HIPAA rules' requirements apply only to the healthcare component, the hybrid entity retains certain oversight, compliance, and enforcement obligations.

ii. Section 164.105(a)(2)(iii)(C) – Responsibilities of the covered entity [78FR5589]
This section makes it clear that a hybrid entity, and not merely the healthcare component, remains responsible for the liability and business associate agreements regarding business associate arrangements and other organizational requirements. Hybrid entities may need to execute legal contracts and conduct other organizational matters at the hybrid level, rather than at the level of the healthcare component.

iii. Section 164.105(b)(1) Standard: Affiliated covered entities [78FR5589]
This section corrects a minor typographical error in the numbering of this paragraph.

iv. Section 164.105(b)(2)(ii) Safeguard requirements [78FR5589]
This provision simplifies and combines this section stating that an affiliated entity must comply with the Privacy and Security Rules.

d. Section 164.106—Relationship to Other Parts [78FR5589]

This provision adds the reference to the business associate which is consistent to the inclusion throughout the HIPAA rules.

2. Modifications to the HIPAA Security Rule in Subpart C [78FR5589]

a. Business Associates [78FR5589]

Section 164.308, 164.310, and 164.3012 modify the definitions of administrative safeguards and physical safeguards to implement the HITECH Act's provision extending direct liability for complying with the Security Rule to business associates. The requirement extends the technology-neutral and scalability requirements to all the different sizes of business associates, enabling them to reasonably implement any given standard.

b. Section 164.306—Security Standards: General Rules [78FR5589]

This section adds business associates to the provision that ensures the confidentiality, integrity, and availability of all electronic health information. Business associates must review and modify security measures as needed to ensure the continued provision of reasonable and appropriate protection of electronic PHI and update documentation of such security measures accordingly.
Business associates may go to the HHS website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule for educational papers and other guidance for compliance with the HIPAA Security Rule.

c. Section 164.308—Administrative Safeguards [78FR5590]

This provision explicitly states that a covered entity is not required to enter into a business associate agreement with the business associate's subcontractors. This section also broadens the security termination procedures for work force members to include "or other arrangements" in recognitions that not all work force members are employees. Finally, OCR removed the provision requiring a covered entity acting as a business associate to another covered entity that violated the assurances that it had provided will be in noncompliance with the Security Rule, as this is now regulated by the Security Rule's provision for business associates.

d. Section 164.314—Organizational Requirements [78FR5590]

This provision explicitly states that the business associate has the obligation to have business associate contracts with subcontractors that create, receive, maintain or transmit electronic PHI. The contract, memorandum of understanding, or other arrangements provision was removed since this is clearly defined in the HIPAA Privacy Rule. This section also ensures that business associates report to the covered entity any security incident, including breaches of unsecured PHI. Finally, the section requires that any subcontractors that enter into a contract or other arrangement must protect the security of electronic protected information and must report any security incidents or breaches of unsecured PHI to the business associate that holds its contract. So a subcontractor reports the breach to the business associate, the business associate reports the breach to the covered entity, and the covered entity reports the breach to the individuals.

D. Subpart E of Part 164: Modifications to the Privacy [78FR5591]

1. Section 164.500—Applicability [78FR5591]

The HITECH Act explicitly made business associates liable for noncompliance for specific requirements of the Privacy Rule. The Privacy Rule does not create direct liability for business associates with regard to compliance with all requirements under the Privacy Rule. A business associate is directly liable under the Privacy Rule for uses and disclosures of PHI that are not in accord with its business associate agreement or the Privacy Rule.

2. Section 164.501—Definitions [78FR5592]

a. Definition of "Health Care Operations" [78FR5592]

The Patient Safety and Quality Improvement Act of 2005 (PSQIA), 42 U.S.C. 299b–21, et seq., provides that patient safety activities of patient safety organizations (PSOs) are deemed to be healthcare operations under the Privacy Rule. Therefore, the Privacy Rule definition of healthcare operations has been modified to expressly reference the activities of the PSOs as healthcare operations.

b. Definition of **"**Marketing" [78FR5592]

The definition of "marketing" has significantly changed. Marketing means "making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." This provision requires a marketing authorization for all subsidized communications; thus the individual will be notified of this type of communication through the authorization process. This does not include financial remuneration to a covered entity to implement a program such as a disease management program, where the individuals are only encouraged to participate in the covered entity's program and not purchase products or services from the third party.

When remuneration received by the covered entity reasonably covers costs of the communication, then this is not considered marketing and a valid authorization is not needed. The notice of privacy practice covers this type of communication under treatment and healthcare operation. OCR defines reasonable costs as the cost of labor, supplies, and postage to make the communication. Financial remuneration that generates a profit or includes payments for other costs is not considered reasonable.

Exceptions to marketing communication for reasonable financial remuneration include:

- refill reminders or other communications about a drug or biologic that is currently being prescribed for the individual
- treatment of an individual by a healthcare provider:
    - including case management/care coordination
    - to direct or recommend alternative treatments, therapies, healthcare providers, or settings of care
- To describe a health-related product or service that is provided by:
    - the entities participating in a health care provider network or health plan network
    - replacement of, or enhancements to, a health plan
    - available only to a health plan enrollee that add value to, but are not part of, a plan of benefits
- 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

This provision also defines "financial remuneration" to mean "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." Direct payment is defined as financial remuneration that comes from the third party to the covered entity who is requesting their product or service to be described. Indirect payment means financial remuneration that comes from an entity on behalf of the third party to the covered entity who is requesting their product or service to be described. Financial remuneration does not include non-financial benefits such as in-kind benefits. Only payments are included.

A business associate (including subcontractors) that receives financial remuneration (instead of the covered entity) by a third party in exchange for making the communication about a product or service must also obtain an authorization from the individual prior to making the communication.

A valid authorization must be obtained from the individual prior to the communication and such authorizations must disclose the fact that the covered entity is receiving financial remuneration from a third party. Section 164.508 (a)(3) indicates that the scope may apply broadly to subsidized communications generally as long as the authorization adequately describes the intended purpose of the requested use and disclosure and must also contain the elements and statements of valid authorization. It must be clear that the individual may revoke the authorization at any time.

As a point of clarification, OCR did not modify the marketing exceptions to the authorization for treatment or healthcare operations when financial remuneration is received if the communication is:

- made face to face by the covered entity to the individual
- consists of a gift of nominal value provided by the covered entity

It is important to note that communication via phone, mail or e-mails do not constitute a face-to-face communication and therefore do not apply to the exception.

3. Business Associates [78FR5597]

The final rule clarifies that a person becomes a business associate by definition. In other words, if there is no contract or other arrangement, but the person is functioning in the role as defined by a business associate, the person is considered a business associate. Business associates are directly liable under HIPAA for:

- impermissible uses and disclosures (§ 164.502(a)(3))
- failure to provide breach notification to the covered entity (§ 164.410)
- failure to provide access to a copy of electronic protected health information either to the covered entity or individual (§ 164.502(a)(4)(ii))
- failure to disclose protected health information to the Secretary as required to investigate or determine the business associates compliance (§ 164.502(a)(4)(i))
- failure to provide an accounting of disclosures (§ 164.502 76 Fed. Reg. 31426, May 31, 2011)
- failure to comply with the Security Rule Subpart C of Part 164

a. Section 164.502(a) and (b)—Permitted and Required Uses and Disclosures and

Minimum Necessary [78FR5597]

i. Permitted and Required Uses and Disclosures [78FR5597]
The way a covered entity may use and disclose PHI now extends to a business associate. Business associates are now explicitly required to only use and disclose PHI as permitted or required by the Privacy or Enforcement Rules. This requirement also adds at § 164.502(a)(4) and (5) that a business associate may only use or disclose protected information pursuant to its business associate contract or other arrangement or as required by law. In addition, the business associate must disclose protected information when required by the Secretary to investigate or determine the business associate's compliance. Finally, a business associate must disclose protected information to the covered entity, individual, or individual's designee as necessary to meet the obligation of the covered entity when an individual requests an electronic copy of their PHI.

ii. Minimum Necessary [78FR5599]
At § 164.502(b), the minimum necessary standard is explicitly extended to businesses associates. Business associates must follow this standard when using or disclosing PHI, and the final rule makes clear that requests from the business associate to a covered entity or another business associate must also follow the minimum necessary standard. The business associate will apply the standard in way that is consistent with the covered entity's policies and procedures and as outlined in the business associate agreement. The department intends to issue future guidance on the minimum necessary standard.

b. Sections 164.502(e) and 164.504(e)—Business Associate Agreements [78FR5599]

The rule currently allows business associates to create or received PHI on behalf of the covered entity, and that the business associate will appropriately safeguard the information;
§ 164.502(e) extends the same provisions to subcontractors of the business associate. The subcontractor will also have appropriately safeguarded the information. Consistent with the Security Rule, this section clarifies that the covered entity is not required to obtain satisfactory assurances from business associates that are contractors, but rather the business associate of the covered entity is required to get these assurances from subcontractors directly. Satisfactory assurances are documented through a written agreement such as a memorandum of understanding that the business associate meets the applicable requirements of the business associate agreement.

This provision does not change the parties on the contracts. A covered entity may choose to contract with a business associate and that business associate may choose to contract with a subcontractor, who in turn may contract with a subcontractor and so on. The business associate and both contractors are all now liable under the HIPAA rules, and each is required to obtain a business associate agreement with the party with whom they have contracted for services that involve PHI. Again, even if there is no contract (as required) the business and subcontractors would still be liable under the Privacy Rule definition of business associate.

This provision removed § 164.502(d)(1)(iii) which stated that a covered entity will be in noncompliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another entity, as this is now covered under § 164.502(e).

Section 160.103 states that a business associate that is aware of noncompliance by its subcontractor is required to respond to the situation in the same manner as a covered entity that is aware of noncompliance by its business association to § 164.502(e)(1)(ii).

In § 164.504(e)(2)(ii)(B)-(D)the business associate agreement must include:

- business associates comply (as necessary) with the Security Rule in regard to electronic PHI
- business associates must report breaches of unsecured PHI to the covered entity
- business associates must ensure that their subcontractors that create or receive PHI agree to the same restrictions and conditions that apply to the business associate

Additionally in § 164.502(e)(1)(ii) business associates, as designated by the agreement, that carry out a covered entity's obligation are contractually required to comply with the requirements of the Privacy Rule in the same manner as they apply to the covered entity. In other words, the business associate would assume contractual liability for the failure to distribute the Notices of Privacy Practice, but would not be directly liable under HIPAA.

A new agreement provision was added at § 164.504(e)(1)(ii)(H) requiring that business associates who have contracted with a covered entity and then subcontract out the work must enter into a business agreement or other arrangement with the subcontractor.

For covered entities and their business associates who are both governmental agencies, section 164.504(e)(3) includes references to the Security Rule to avoid having to duplicate this provision in the Security Rule itself. OCR also added that the data use agreement may quality as a business associate's satisfactory assurance that will appropriately safeguard the covered entity's information when the PHI is used and disclosed for healthcare operations. They clarify that this is not appropriate for disclosures of a limited data set for research or public health, as these uses do not require business associate agreements.

c. Section 164.532—Transition Provisions [78FR5602]

The final rule adopts the transition provision allowing covered entities and business associates to continue to operate under existing contracts that have already have a HIPAA-compliant agreement in place before January 25, 2013, and if the agreement is not renewed between March 26, 2013, and September 2013, then they can rely on that agreement until September 23, 2014.

If the covered entities and business associates do not have a compliant agreement in place by January 25, 2013, then they will need to enter into a compliant agreement by September 23, 2013, which is a year earlier than for grandfathered agreements.

The bottom line is if an agreement is renewed between Sept. 23, 2013 and Sept. 23, 2014, it must comply with the new rule. The benefit of having a HIPAA-compliant agreement in place prior to January 25, 2013, is that if it is not due to be renewed by September 23, 2013, then the parties have until September 23, 2014, to revise it.

In contrast, if the covered entity or business associate executes the agreement on or after January 25, 2013, then the parties should either ensure that it complies with the new rule or plan to revise the agreement no later than September 23, 2013, to bring it into compliance with the new rule.

4. Section 164.508—Uses and Disclosures for Which an Authorization is Required [78FR5603]

a. Sale of Protected Health Information [78FR5604]

Sale of PHI by a covered entity or a business associate is prohibited except as pursuant in this section.

To clarify, the final rule added the definition for the sale of PHI. Sale of PHI means "disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information." This provision also clarifies that the way "remuneration" is used in this statute is *different* than how is it used in the marketing section and therefore, "remuneration" here means both financial and nonfinancial benefits (also known as in-kind benefits).
The sale of protected information does not include disclosures of protected information:

- for public health
- for research purposes where remuneration was a reasonable cost-based fee to cover the costs to prepare and transmit the information
- for treatment and payment purposes
- for a sale, transfer, merger or consolidation related to due diligence
- to a business associate (or the subcontractor) that undertakes activities on behalf of the covered entity, where the remuneration is only for the performance of those activities
- to an individual who has requested the PHI
- as required by law
- for any other purpose permitted where remuneration is a reasonable cost-based fee to cover the costs to prepare and transmit the information or where the fee is otherwise expressly permitted by law

For those sections that are allowed a reasonable cost-based fee to prepare and transmit the data, costs include both direct and indirect costs for generating, storing, retrieving and transmitting PHI:

- labor
- materials
- supplies

Any fees generated that incur a profit margin are not allowed.

This provision also clarifies that de-identified PHI is not subject to the remuneration prohibition, as it is no longer considered PHI. However, limited data sets are not completely exempt from this provision. Limited data sets that are permitted under the rule are exempt from the authorization requirements to the extent that the only remuneration received is in exchange for the data is a reasonable cost-based fee.

b. Research [78FR5609]

*i. Compound Authorizations § 164.508(b)(3)(i) and (iii) [*78FR5609]
This provision has been amended to allow compound (conditioned and unconditioned) authorizations for research. The authorization must clearly differentiate between the conditioned and unconditioned research components and clearly allow the individual to opt out of the unconditioned research activities. This provision applies to all types of research studies except when the research involves the use or disclosures

of psychotherapy notes. Psychotherapy note authorizations may not be combined with any other authorization for use or disclosure of psychotherapy notes.

Compound authorizations for research can include an authorization for use of PHI in a clinical trial and optional sub-studies or biospecimen banking that also permits future secondary use of the data (to the extent the authorization meets the future use requirements). Authorizations are still allowed to be combined with the informed consent documents for the research study.

Authorizations must give participants an opt-in option; combined authorizations that only allow the individual the option to opt out of the unconditioned research activities are not permitted (e.g. check here if you do **not** want….). The opt-out option does not give the participants a clear ability to choose to participate in the optional research activity. This provision is not required, but merely allows for the authorizations to be combined. For new studies, separate authorizations may continue to be used.

Lastly, when a revocation is requested for only one part of the compound authorization, the revocation does not invalidate the entire authorization unless it is not clear exactly which research activity the participant's revocation applies.

ii. Authorizing Future Research Use or Disclosure § 164.508(c)(1)(iv) [78FR5611]
Though the HIPAA authorization elements are still required, the "purpose" interpretation had changed for research. An authorization for uses and disclosures of PHI for future research must adequately describe what the individual is to expect that his or her PHI may be used or disclosed for future research. In addition, the description of the PHI may include information collected beyond the time of the original study.

5. Protected Health Information about Decedents [78FR5613]

a. Section 164.502 (f) – Period of Protection for Decedent Information [78FR5613]

The final rule requires covered entities to comply with the Privacy Rule regarding PHI of deceased individuals for a period of 50 years following date of death. The definition of PHI (§160.103) has been changed to reflect the new requirement that any individually identifiable health information of a person deceased more than 50 years is no longer considered PHI under the Privacy Rule.

The final rule does not override or interfere with state or other laws providing greater protections. This change has no impact on a covered entity's disclosures permitted by other provisions under the Privacy Rule (e.g. §164.512(i)(1)(iii)).

The final rule clarifies that this is not a record retention requirement.

b. Section 164.510(b)—Disclosures about a Decedent to Family Members and Others Involved in Care [78FR5614]

This provision amends §164.510(b) and now permits entities to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of a decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. For example, a healthcare provider can describe the circumstances that led to an

individual's death or provide billing information to a decedent's sibling. This does not include past unrelated medical problems.

The final rule includes a definition of "family member" under §160.103 which can also be found in the section of this analysis about GINA (see pg. 33-35).

These disclosures are permitted and not required. If the covered entity is uncomfortable or believes the disclosure to be inappropriate or doubts identity of the requestor, the final decision lies with the covered entity.

6. Section 164.512(b) – Disclosure of Student Immunizations to Schools [78FR5616]

This provision amends §164.512(b)(1) by permitting a covered entity to disclose proof of immunization to a school where state or other law requires it prior to admitting a student. Written authorization is no longer required, but an agreement must still be obtained, which can be oral. The agreement must come from a parent/guardian, or other person acting in *loco parentis*, or directly from the individual (adult or emancipated minor). Agreements for disclosure of immunization records should be obtained on a case-by-case basis as needed.

The agreement must be documented, but no signature by the parent is required. The final rule leaves it up to the covered entity about what information needs to be captured regarding the agreement to determine what is needed for their purposes. The documentation must make clear that the agreement was obtained as permitted under this provision. Written or e-mail requests suffice as documentation of the agreement. Agreements obtained under this provision are considered effective until revoked by the parent, guardian, or other person acting in *loco parentis*, or by the individual himself (adult or emancipated minor). The agreement is not to be treated the same as a HIPAA-compliant authorization.

This provision leaves it up to each individual school to determine the appropriate individual to receive and manage the receipt of immunization records at their respective locations. The final rule does not define the terms "school" or "school official."

7. Section 164.514(f)—Fundraising [78FR5618]

This provision keeps the original definition and requirements under HIPAA but makes a few changes. The final rule emphasizes that this provision only applies to covered entities using or disclosing PHI to target a fundraising communication. Example: if a covered entity uses a public directory to mail fundraising communications to residents in a particular service area, these provisions do not apply.

The final rule requires a covered entity to provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications and that the individual's choice to opt out is treated as a revocation of authorization under the Privacy Rule. Thus, treated as a revocation, a covered entity may not make further fundraising communications to an individual who has opted out. The covered entity also may not condition treatment or payment because of an individual's choice about receiving fundraising communications.

The opportunity to opt out of receiving further fundraising communications must be provided with each fundraising communication made. The scope of the opt-out is left up to the covered entity. In other words, it is up to the covered entity to decide if the opt out applies to all future fundraising communications or if

it is campaign specific. However, if an individual chooses to opt out of future fundraising communications using a mailed opt-out method, the mailed opt-out method would apply to all forms of fundraising communications (e.g., e-mail). The final rule gives covered entities the discretion to decide how to handle and manage individuals who want to opt back in.

The method for an individual to opt out may not cause the individual to incur an undue burden or more than a nominal cost. The final rule encourages the use of a toll-free number, e-mail address, or similar opt-out mechanism that provides a simple, quick, and inexpensive way to opt out. Covered entities can provide multiple opt-out methods if they choose allowing the individual to determine which method is most convenient for them.

The final rule clarifies at §164.514(f)(1)(i) that demographic information relating to an individual includes names, addresses, other contact information, age, gender, and dates of birth. Dates of birth was added instead of merely age. Insurance status remains a type of demographic information as under the Privacy Rule. Along with demographic information, health insurance status, and dates of healthcare provided, the final rule allows covered entities to use and disclose department of service (e.g. neurology, orthopedics, and cardiology), treating physician, and outcome information (e.g. death of a patient, or any sub-optimal result of treatment or services) for fundraising purposes. The final rule, in permitting its use for fundraising, intends for it to be used by the covered entities to screen and eliminate from fundraising solicitations those individual experiencing a sub-optimum outcome, and for its disclosure to a business associate or institutionally related foundation only where such screening function is done by those parties.

A statement must be included in the Notice of Privacy Practices (NPP) that a covered entity may contact them about fundraising and that individual has a right to opt out of receiving fundraising communications. The rule does not require pre-solicitation opt outs prior to the first fundraising communication.

This provision also applies to any fundraising communications made over the phone.

8. Section 164.520—Notice of Privacy Practices for Protected Health Information [78FR5622]

This section defines some new requirements for the NPP, including redistribution.

- The final rule modifies §164.520(b)(1)(ii)(E) requiring certain statements on the NPP about uses and disclosures that require authorization. The NPP must include:
  - A statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require an authorization
  - A statement that other uses and disclosures not described in the NPP will be made only with an authorization from the individual
  - The final rule does not require a description of a covered entity's psychotherapy notes recordkeeping practices to be included on the NPP.
  - Covered entities that do not record or maintain psychotherapy notes are not required to have a statement about the authorization requirement for uses and disclosures of psychotherapy notes on their NPPs.
- The NPP must include a statement about fundraising communications and an individual's right to opt out. The mechanism does not have to be included on the NPP.

- (Only applies to healthcare providers) The NPP must inform individuals of their new right to restrict certain disclosures of PHI to a health plan if they pay for a service in full and out of pocket. Other covered entities retain current verbiage as required under the Privacy Rule.
- The NPP must include a statement of an individual's right to be notified of a breach of unsecured PHI in the event they are affected.

Health Plan Redistribution of the Notice of Privacy Practices

The final rule requires a health plan that currently posts its NPP on its website in accordance with §164.520(c)(3)(i) to:

1) Prominently post the material change or its revised notice on its website by the effective date of the material change to the notice which is September 23, 2013, in this case.
2) Provide revised notice, or information about the material change and how to obtain the revised notice in its next annual mailing to individuals then covered by the plan, such as at the beginning of the plan year or during the open enrollment period.

   Health plans that do not have customer service web sites are required to provide the revised NPP or information about the material change and how to obtain it to individuals covered by the plan within 60 days of the material revision to the notice.

Healthcare Providers Redistribution of the Notice of Privacy Practices

The final rule does not modify the current requirement to distribute revisions to the NPP for healthcare providers. However:

- The final rule clarifies that providers are not required to print and hand out a revised NPP to all individuals seeking treatment.
- Providers are required to give a copy of the NPP to and obtain a good faith acknowledgement of receipt from new patients.
- The revised NPP must be posted in a clear and prominent location with copies of the NPP available for the individual to easily take one. It would not be appropriate for an individual to have to ask the receptionist for a full copy of the NPP.
- For covered entities that have already revised their NPPs, the final rule clarifies that they do not have to be revised and redistributed again as long as the NPP is consistent and compliant with this final rule.
- To comply with the Rehabilitation and Americans with Disabilities Acts, the covered entity must be made in available formats such as Braille, large print, or audio.
- The final rule clarifies that covered entities may use a "layered notice" to implement the rule's provisions, as long as the elements required under the Privacy Rule are included in the document provided to the individual.
    - Example: a covered entity may meet this requirement by providing the individual with both a short notice (brief summary of individual rights) and a longer notice layered beneath the short notice that contains all the elements required by the Rule.
- The final rule clarifies that the Privacy Rule permits covered entities to distribute their NPPs or notices of material changes by e-mail, if the individual has agreed to receive it that way.

9. Section 164.522(a)—Right to Request a Restriction of Uses and Disclosures [785626]

Covered entities must agree to an individual's request to restrict disclosure of PHI to the individual's health plan when:

- The disclosure is for the purpose of payment or healthcare operations and is not otherwise required by law
- The protected information pertains to a healthcare item or service which has been paid in full other than by the health plan

Operationalizing these provisions does not require the covered entity to segregate PHI to a restricted healthcare item or service. However, it is expected that the covered entity have a way to note that the information has been restricted and is not released to the health plan for payment or healthcare operations such as audits. The minimum necessary standard should be applied.

A covered entity is required to disclosure the restricted information to Medicare or Medicaid as required by law such as for audits. The final rule clarifies that if the information is required to be disclosed by law, then the information may not be withheld. Required by law includes following the Medicare Conditions of Participation.

For request for restriction as it applies to state law, Medicare and Medicaid that prevent providers from billing, and receiving cash payment from, an individual for covered services over and above any permissible cost sharing amounts, OCR provides the following guidance:

Providers that are required by state or other law to submit a claim to a health plan and there is no exception or procedure for individuals wishing to pay out of pocket for the service, then the disclosure is required by law and is an *exception* to an individual's right to request a restriction to the health plan.

For Medicare, when a service is covered by Medicare, then it is subject to the mandatory claim submission provisions of section 1848(g)(4) of the Social Security Act, which requires when charges or attempts to charge a beneficiary any remuneration for a service that is covered by Medicare, then a claim must be submitted to Medicare. However, there is an exception to this rule where a beneficiary refuses to authorize the submission of a bill to Medicare. Then a Medicare provider is not required to submit a claim to Medicare for the covered service and may accept an out-of-pocket payment for the service from the beneficiary. The limits on what the provider may collect from the beneficiary continue to apply to charges for the covered service, notwithstanding the absence of a claim to Medicare.

In cases where a provider is prohibited from unbundling a services or it is more costly to unbundle, OCR expects providers to counsel patients on their ability to unbundle the service and the impact of doing so, such as the health insurer being able to determine the service based on the context. If the item cannot be unbundled, the provider should inform the individual and them the opportunity to pay for the entire bundled service out of pocket. In these cases, OCR considers a group of bundled items or services is seen as one item or service for the purposes of applying the restriction.

OCR encourages providers to discuss with patients that the patients needs to request restrictions with other providers and pay out of pocket if they wish to keep information from going to the health plan from other providers and pay out of pocket for those services. For example, if the patient wants to pay for a prescription out of pocket, the provider can provide the patient with a paper prescription to allow the

individual an opportunity to request and pay for the prescription before a pharmacy submits the bill to the health plan. In addition, if the patient returns for follow-up care and the information from the original restriction are used, the patient would once again have to pay out of pocket for the current service to ensure the information is not sent. The provider would only send the information if requested by the payer, the information meets the minimum necessary policy of the provider and restriction is not requested and paid for in advance.

If the information is released after a restriction has been requested and paid for in advance, the provider may be subject to criminal penalties, civil money penalties or corrective action for making an impermissible disclosure under the Privacy Rule.

10. Section 164.524—Access of Individuals to Protected Health Information [78FR5631]

Covered entities must provide an electronic copy of protected health information that is:

- maintained electronically
- located in one or more designated record sets
- in the form and format requested

a. Form and Format - § 164.524(c)(2)(i)-(ii) [78FR5632]

The covered entity must produce a copy of the electronic record in the form and format requested by the individual. If the form and format are not readily producible, then the information must be produced in an electronic form as agreed to by the covered entity and the individual. If the individual declines any of the electronic formats that are available, the covered entity must provide a hard copy as an option to fulfill the access request.

The information, at a minimum must be in a machine-readable format. Machine-readable format means digital information stored in a standard format enabling the information to be processed and analyzed by a computer such as in MS Word, MS Excel, or PDF, among other formats.

This provision does not require covered entities to purchase new software or systems in order to accommodate electronic requests for a specific form that the covered entity does not currently possess, provided the covered entity can produce a copy of the information in an electronic form.

A covered entity may choose to require a written request; however, it may be in no way designed to discourage an individual from requesting an electronic copy. A covered entity may also chose to accept an individual's oral request for an electronic copy of their information.

If the covered entity's electronic system contains links to PHI that is part of the designated record set, and that information is requested, the electronic copy must contain a copy for that information. It is important to note that if a portion of the record is maintained in paper, this does not have to be converted to an electronic format.

This provision also clarifies that the covered entity does not have to accept external portable media from individuals if they have determined this to be an unacceptable risk; however, covered entities cannot require individuals to purchase a portable media device from the covered entity if the individual does not wish to do so.

Covered entities may also send individuals unencrypted e-mails if they have advised the individual of the risks and the individual still prefers that method of delivery.

b. Third Parties - § 164.524(c)(3) [78FR5634]

This section expressly requires when an individual requests the covered entity to transmit a copy of the PHI to another person, the covered entity must comply. Within this provision, the request must:

- be made in writing
- be signed by the individual
- clearly identify the designated person
- clearly identity where the information will be sent

If the covered entity requires all *access* requests to be in writing, the same request may be used for releasing the information electronically as long as the individual clearly designates the person, where the information is to be sent and signs the request. This written request for PHI to be sent to a designated person is distinct from an authorization form. Covered entities may rely on the information provided in writing by the individual, but must have policies and procedures in place to verify the identification of the individual making the request as well as implement reasonable safeguards to protect the information that is used or disclosed. This does not include verifying that the individual provided the correct e-mail address, but does include ensuring the e-mail address provided is entered into the system correctly.

c. Fees - § 164.524(c)(4)(i) [78FR5635]

This provision allows for identifying the labor for copying PHI, whether in paper or electronic form. Labor costs can include in a reasonable cost-based fee for skilled technical staff time spent creating and copying the electronic file such as:

- compiling
- extracting
- scanning
- burning onto media
- distributing media

This could also include the time spent preparing an explanation or summary.

Other fees include:

- cost of supplies for creating the paper copy or electronic media (if the individual requests portable media)
- postage or courier

This provision clarifies that a covered entity may not charge for a retrieval fee (whether it be a standard retrieval fee or one based on actual retrieval costs).

Finally, in regard to state laws that provide a limit on the fee that a covered entity may charge for a copy of PHI, a covered entity must be both reasonable and fee based. If the state law per page fee is 25 cents, and the covered entity can provide an electronic copy for 5 cents per page, then the covered entity may only charge 5 cents per page. If the covered entity can provide an electronic copy for 30 cents, it may only charge 25 cents per page, as this is not reasonable based on state law.

Affidavits are not considered to be a copying cost and are therefore outside of the scope of the Privacy Rule. However, an entity may not withhold the copy of the record for failure to pay for any services above the copying costs.

d. Timeliness - § 164.524(b) [78FR5636]

The final rule removes the provision that permits 60 days for retrieving and copying a record that is maintained off site. The covered entity has 30 days with one-time 30 day extension to respond to the request (with the written notice to the individual of the reasons for delay and expected completion date). This provision extends the 30-day time limit with a one-time 30-day extension to respond to requests for electronic access. This aligns the time period to respond, no matter the location or the media.

This provision clarifies that the time period for responding to a request begins on the date of the request – the time it takes to reach an agreement for the form and format of an electronic request is counted in this 30-day time frame.

11. Other Technical Changes and Conforming Changes [78FR5637]

The Privacy Rule had a number of technical and conforming changes to correct minor problems such as incorrect cross references, grammar, and typographical error.

V. Modifications to the Breach Notification Rule under the HITECH Act [78FR5638]

A. Background [78FR5638]

This section gives a brief background on the legislation and history of the Breach Notification Rule.

B. Overview of the Interim Final Rule [78FR5639]

This section provides a very brief overview of the interim final rule that was published on August 24, 2009, and the accompanying FTC rule published on August 25, 2009.

C. Section by Section Description of the Final Rule and Response to Comments

1. Section 164.402 – Definitions [78FR5639]

a. Definition of "Breach"

OCR provides a very detailed discussion of this definition arrived at after considering the public comments on the interim rule definition. The OCR in this final rule amends the definition of "breach."

OCR notes that it has added language to the definition of breach to clarify that an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

To ensure that this provision is applied uniformly and objectively by covered entities and business associates, OCR has removed the harm standard and modified the risk assessment to focus more objectively on the risk that the PHI has been compromised.

Thus, breach notification is not required under the final rule if a covered entity or business associate, as applicable, demonstrates through a risk assessment that there is a low probability that the PHI has been compromised, rather than demonstrate that there is no significant risk of harm to the individual as was provided under the interim final rule.

OCR states that the statute acknowledges, by including a specific definition of breach and identifying exceptions to this definition, as well as by providing that an unauthorized acquisition, access, use, or disclosure of PHI must compromise the security or privacy of such information to be a breach, that there are several situations in which unauthorized acquisition, access, use, or disclosure of PHI is so inconsequential that it does not warrant notification. Agreeing with some commenters, OCR also notes that it believed that the risk assessment focus on "harm to an individual" in the interim final rule was too subjective and would lead to inconsistent interpretations and results across covered entities and business associates. Now, instead of assessing the risk of harm to the individual, covered entities and business associates must assess the probability that the PHI has been compromised based on a risk assessment that considers at least the following factors:

(1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(2) The unauthorized person who used the PHI or to whom the disclosure was made;

(3) Whether the PHI was actually acquired or viewed; and

(4) The extent to which the risk to the PHI has been mitigated.

The first factor requires covered entities and business associates to evaluate the nature and the extent of the PHI involved, including the types of identifiers and the likelihood of re-identification of the information. To assess this factor, entities should consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature.

The second factor requires covered entities and business associates to consider the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made. Entities should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information.

The third factor requires covered entities and business associates to investigate an impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed.

The final factor included in the final rule requires covered entities and business associates to consider the extent to which the risk to the PHI has been mitigated.

Covered entities and business associates should attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

A covered entity's or business associate's analysis of the probability that PHI has been compromised following an impermissible use or disclosure must address each factor discussed above. Other factors may also be considered where necessary. In the future, OCR will issue additional guidance to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios.

In addition to the removal of the harm standard and the creation of more objective factors to evaluate the probability that PHI has been compromised, the rule has removed the exception for limited data sets that do not contain any dates of birth and ZIP codes.

In the final rule, following the impermissible use or disclosure of any limited data set, a covered entity or business associate must perform a risk assessment that evaluates the factors discussed above to determine if breach notification is not required.

The final rule expressly includes a factor that would require consideration of the re-identifiability of the information, as well a factor that requires an assessment of the unauthorized person who used the PHI or to whom the disclosure was made (i.e., whether this person has the ability to re-identify the affected individuals).

Covered entities and business associates are encouraged to take advantage of the safe harbor provision of the Breach Notification Rule by encrypting limited data sets and other PHI pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740, 42742). If PHI is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information.

It was suggested that covered entities be required to include in their notice of privacy practices information about how a risk assessment will be conducted or their internal policies for determining whether a breach has occurred and notification is warranted. The final rule declines to require that the covered entity's notice of privacy practices include a description of how a risk assessment will be conducted, although covered entities may include such information in their notice of privacy practices if they choose.

The Privacy Rule's minimum necessary standard requires a covered entity to make reasonable efforts to limit access to PHI to those persons or classes of persons who need access to PHI to carry out their duties and to disclose an amount of PHI reasonably necessary to achieve the purpose of a disclosure. The Privacy Rule requires covered entities to determine and define in their policies and procedures how the minimum necessary standard applies to their own uses and disclosures. Thus, covered entities are in a good position to know when such policies and procedures have been violated and to assess the probability that the incident has compromised the security or privacy of the information.

Regarding the consistent use of definitions; the Privacy Rule uses the terms "use" and "disclosure," and OCR included both "acquisition" and "access" in the regulatory text for consistency with the statutory language. OCR states: "We interpret 'acquisition' and 'access' to information based on their plain meanings and believe that both terms are encompassed within the current definitions of "use" and "disclosure" in the HIPAA Rules."

Although the FTC and HHS Breach Notification rules generally apply to different entities, HHS has worked closely with the FTC to ensure both sets of regulations were harmonized to the greatest extent possible by including the same or similar requirements within the constraints of the statutory language. In addition, in the few situations where an entity provides PHRs to customers of a HIPAA covered entity through a business associate arrangement but also provides PHRs directly to the public and a breach of its records occurs, in certain cases, the FTC will deem compliance with certain provisions of HHS' rule as compliance with FTC's rule.

b. Definition of "Unsecured Protected Health Information" [78FR5646]

The final rule amends the definition of "unsecured protected health information" to read:

"Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary in guidance."

2. Section 164.404—Notification to Individuals [78FR5647

These provisions are adopted in the final rule without any modifications from the interim final rule. Covered entities, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach.

For breaches at or by a business associate, the covered entity ultimately maintains the obligation to notify affected individuals of the breach. A covered entity is free to delegate the responsibility to the business associate that suffered the breach or to another of its business associates. Also with regards to health information organizations, the obligation to notify individuals lies with the covered entity.

Breaches Treated as Discovered
A breach will be treated as discovered by a covered entity or business associate as of the first day on which the breach is known or should reasonably have been known to the covered entity or business associate. Discovery is triggered as soon as any person, other than the individual committing the breach, who is an employee, officer, or other agent of the covered entity or business associate knows or should reasonably have known.

Timeliness
Covered entities must notify affected individuals of a breach without unreasonable delay but in no case later than 60 calendar days from the discovery of the breach, except in certain circumstances where law enforcement has requested a delay. Keep in mind that 60 days is the outer limit.

The time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete. A covered entity is expected to notify individuals as soon as

reasonably possible after the covered entity takes reasonable time to investigate and collect information to be included in the notification.

Content of the Notification
The content requirements of the notification have been adopted in the final rule without modification from the interim final rule and are as follows:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach (if known)
- A description of the types of unsecured PHI that were involved in the breach (e.g. full name, social security number, date of birth, account number, diagnosis code)
- Any steps an individual should take to protect themselves from potential harm resulting from the breach
- A brief description of what the covered entity involved is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address

The notification must be written in plain language at an appropriate reading level. Covered entities must also take appropriate steps to ensure meaningful access for Limited English Proficient persons. This also includes if steps need to be taken to include those with disabilities or who fall under the Rehabilitation Act which would include formats such as Braille, large print, or audio.

HHS anticipates providing additional guidance in the future regarding the content of notification to individuals.

Methods of Notification
The final rule requires both written notice to affected individuals as well as substitute notice if contact information is insufficient or out of date. Substitute notice should be provided as soon as reasonably possible after the covered entity is aware that it has insufficient or out-of-date information.

- Notification must be sent via first-class mail to the last known address or the individual or next of kin if the individual is deceased or by e-mail if specified as the preferred method by the individual.
- Notification can be one or more mailings as information becomes available.

If there is insufficient or out of date information for 10 or more individuals, a substitute notice must be provided in one of the following for the geographic areas where the affected individuals most likely reside:

- A posting on the home page of the covered entity's web site (can be a prominent hyperlink); or
- Notice in major print; or
- Broadcast media; and
- A toll-free number (active for 90 days) where individuals can learn if their PHI was in fact affected.

If there is insufficient or out-of-date information for fewer than 10 individuals, a substitute notice must be provided through an alternative form of written notice, by telephone, or other means.

The final rule allows a covered entity to provide notice by telephone or other means to individuals (in addition to above said requirements) in urgent situations involving possible imminent misuses of PHI.

If the affected individual is a minor or lacks legal capacity (e.g. mental condition), notice to the parent or personal representative is permitted. For deceased individuals, the notice should only be sent to the individual's next of kin or personal representative if the address of one or the other is known.

The rule does not prohibit notifications from being sent to an alternative address besides the home address (e.g. work address, post office box, e-mail) if the individual requests it. Additionally, if an individual has only agreed to receive communications orally or over the phone, a covered entity can (under the rule) call the individual and tell them to pick up the written breach notification. If the individual does not want to travel to pick it up, the provider should provide all of the information in the breach notice to the individual over the phone and documented. HHS will exercise enforcement discretion in such cases.

In the event a healthcare provider believes that the breach notification may cause anguish or distress for an individual, the provider may phone the individual ahead of time or have them come into the office to discuss. All timeframes still apply.

A covered entity is permitted to send one breach notice to a plan participant, their spouse and/or other dependent under the plan (all must have been affected by the breach). This provision only applies when all individuals are under the same plan and reside at the same address. The notice must also clearly identify to which individuals it applies.

In the event a dependent child's PHI has been breached, the notice must be addressed to the plan participant and/or participant's spouse living with the dependent child. The participant and/or spouse must be the personal representatives of the dependent child and notice must identify who it applies to. If the plan participant and/or spouse is not the personal representative of a dependent under the plan the covered entity must address the notice to the dependent.

3. Section 164.406---Notification to the Media [78FR5652]

The final rule adopts this section with one minor change. The change includes aligning the definition of "state" in the HIPAA rules with the same definition used in the HITECH Act. The change is added to §160.103 and removes it from §164.406. The change includes reference to the American Samoa and the Northern Mariana Islands.

For breaches of more than 500 residents of a state or jurisdiction and in addition to the required individual notice, covered entities must provide a breach notice to prominent media outlets servicing the state/jurisdiction following the discovery of a breach of unsecured PHI. This must be completed without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. The notification to the media must include the same information required to be included in the individual notifications.

"Prominent media outlet" will vary based on state/jurisdiction but might include a major, general interest newspaper with a daily circulation throughout the area.

When the breach involves multiple states, notice is only required if the breach affected more than 500 individuals for a given state/jurisdiction. For example, if a covered entity discovers a breach impacting 600 individual occurs, but 200 individuals reside in state A, 200 individuals reside in state B, and 200 individuals reside in state C, then the breach did not impact more than 500 individuals in any one state so

notification is not required in the media. Individual notification must still be completed and a notification requirement to the Secretary for a breach involving 500 or more individuals applies.

The final rule clarifies that covered entities are not required to incur any cost to print or run media notice about a breach of unsecured PHI if there is insufficient or out-of-date contact information for 10 or more individuals affected. It also does not obligate prominent media outlets who receive notification of a breach from a covered entity to print or run information about the breach. It is also emphasized that posting a press release about a breach of unsecured PHI on the home page does not fulfill the requirement of providing notice to the media.

4. Section 164.408---Notification to the Secretary [78Fr5653]

The final adopts the interim final rule with one change. The modification now requires that all breaches of unsecured PHI affecting fewer than 500 individuals be reported to the Secretary no later than 60 days after the end of the calendar year in which the breach was "discovered," not in which it "occurred." Covered entities may maintain a log of these breaches occurring during the year and annually submit the log to the Secretary.

Covered entities must report breaches affecting 500 or more individuals to the Secretary immediately. "Immediately" is interpreted to require that notification be sent to the Secretary concurrently with the notification sent to the individual. HHS will continue to maintain on its website a list of covered entities that have reported breaches of unsecured PHI involving more than 500 individuals.

Covered entities must notify the Secretary of all discovered breaches involving more than 500 individuals without regard to whether the breach involved more than 500 individuals in one State or jurisdiction.

5. Section 164.410---Notification by a Business Associate [78FR5655]

The final rule adopts the interim final rule. Business associates are required to notify the covered entity of a breach upon discovery. Business associates must provide notification to covered entities without unreasonable delay and in no case later than 60 days from discovery of the breach. Breaches shall be treated as discovered by a business associate on the first day the breach is known to the business associate or by exercising reasonable diligence would have been known to the business associate.

Business associates must provide covered entities with the identity of each individual whose unsecured PHI has or is believed to have been affected. Business associates can notify the business associate immediately of a breach, then follow up with other required information (e.g. identities, nature of the breach, cause of the breach - §164.404(c)) as it becomes available. The information must be provided within the 60 day time limit; however, the rule requires that business associates provide any information even if it becomes available after the time limit or after notifications have been sent. Business associates that maintain PHI for multiple covered entities need only notify the covered entity(s) whose PHI was involved in the breach.

If a business associate is acting as an agent (§164.404(a)(2)), the business associate's discovery of the breach will be imputed to the covered entity. Therefore, the covered entity must provide notifications based on the time the business associate discovers the breach, not from the time the business associate notifies the covered entity. If the business associate is not an agent, then the covered entity must provide notification based on the time the business associate notifies the covered entity of the breach.

The covered entity is ultimately responsible for providing notification to individuals of breaches. The clock starts ticking upon knowledge of the incident even if it's not clear whether the incident in fact is a breach.

Business associates and covered entities will continue to have the flexibility to set forth the obligation for each party, including who will provide notice to the individuals and when notification from the business associate to the covered entity is required, following a breach. It is encouraged that covered entities discuss and define in all business associate agreements the requirement regarding how, when, and to whom a business associate should report to the covered entity a potential breach.

HHS has published sample business associate agreement provisions on its website to help provide guidance.

6. Law Enforcement Delay [78FR5657]

The final rule adopts this provision without modification. If a law enforcement official determines that required breach notification, notice, or posting would impede a criminal investigation or cause damage to national security, the notification, notice, or posting will be delayed in the same manner as provided under the Privacy Rule.

The covered entity or business associate must temporarily delay notification to the individual, the media (if applicable), to a covered entity by a business associate, and to the Secretary if instructed by a law enforcement official.

A law enforcement official may provide a statement in writing that states the delay in notification is necessary because it would impede a criminal investigation or cause damage to national security and specify the time which the delay is required. The covered entity or business associate must delay the notification for the time period specified.

If the request is made orally, the covered entity or business associate must document the statement and identity of the official. The oral request is only valid for 30 days unless a written statement (meeting all requirement stated above) is provided.

7. Section 164.414 –Administrative Requirements and Burden of Proof [78FR5657]

The final rule adopts the interim final rule without modification. This provision emphasizes the importance of workforce training and education about breaches, its meaning, its requirements, and organizational policies and procedures. Organizational policies and procedures must be updated to reflect the final rule.

Burden of proof lies with the covered entity or business associate to demonstrate that all notifications were made as required. All necessary documentation must be kept and maintained to meet this burden of proof. This includes documentation that no breach occurred and notification was not necessary.

8. Technical Corrections [78FR5658]

The final rule adopts all the technical changes made in the interim final rule to align the HIPAA rules with the breach notification requirements.

9. Preemption [78FR5658]

The final rule adopts the preemption standards as discussed in the interim final rule. Contrary state law will be preempted by the breach notification regulations.

10. Response to Other Public Comments [78FR5658

In response to a public comment, OCR clarifies that it will enforce the breach requirements under those listed both in the breach as well as the enforcement sections.

VI. MODIFICATION TO THE HIPAA PRIVACY RULE UNDER GINA [78FR5658]

A. Background [78FR5658]

Similar to previous sections, OCR provides background on the Genetic Information Nondiscrimination Act of 2008 and how it relates to HIPAA.

B. Overview of the Proposed Rule [78FR5659]

Again OCR reviews the proposed rule.

C. Section-by-Section Description of Final Rule and Response to Public Comment [78FR5659]

1. Scope: Extension of Required Protections to all Health Plans Subject to the HIPAA Privacy Rule [78FR5659]

OCR notes: "The final rule adopts the approach of the proposed rule to apply the prohibition on using or disclosing protected health information that is genetic information for underwriting purposes to all health plans that are covered entities under the HIPAA Privacy Rule, including those to which GINA does not expressly apply, except with regard to issuers of long term care policies."

HIPAA expands the prohibition on underwriting with genetic information from the four types of entities expressly listed in GINA (group health plans, health insurance issuers, health maintenance organizations, and issuers of Medicare supplemental policies) to include employee welfare benefit plans, high risk pools, certain public benefit programs and any other individual or group plan, or combination of individual or group plans. At this time issuers of long-term care policies are exempted. Though long-term care plans are exempted from prohibition of using genetic information for underwriting, they are still subject to the Privacy Rule, to use, disclose and protect genetic information in accordance to the rule.

2. Section 160.101 – Statutory Basis and Purpose (starting page [78FR5661]

OCR states: "We have revised § 160.101, which describes the statutory basis of the HIPAA Rules, to include a reference to section 1180 of the Social Security Act, as added by section 105 of GINA (Public Law 110-233)."

3. Section 160.103 – Definitions [78FR5661]

a. Definition of Health information [78FR5661]

The definition for health information was modified to add "including genetic information." Any health plan that also performs underwriting will need to revise its policies and procedures to comply if it used the health information definition.

b. Definition of Genetic information [78FR5661

"Genetic information" is defined in GINA and is added to the Privacy Rule definitions as follows:
"(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:
(i) The individual's genetic tests;
(ii) The genetic tests of family members of the individual;
(iii) The manifestation of a disease or disorder in family members of such individual; or
(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.
(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:
(i) A fetus carried by the individual or family member who is a pregnant woman; and
(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.
(3) Genetic information excludes information about the sex or age of any individual."

c. Definition of Genetic test [78FR5662]

"Genetic test" is also defined in GINA and this term is added to the Privacy Rule and defined as "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes."

d. Definition of Genetic services [78FR566]

GINA defines "genetic services" and this term is added to the Privacy Rule and defined as:
"(1) A genetic test;
(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or
(3) Genetic education."

e. Definition of Family member [78FR5663]

The term "family member" is used in GINA to indicate that an individual's genetic information also includes information about the genetic tests and family history of that individual's family. The term is adopted and means "with respect to an individual:
(1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-

siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.
(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins."

f. Definition of Manifestation or manifested [78FR5663]

"Manifestation" or "manifested" is not separately defined in GINA; however, given the importance of this term, HHS defined this to mean: "with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information."

The following examples are not included in the final regulation, but are used to illustrate the definition:

- "An individual may have a family member that has been diagnosed with Huntington's disease and also have a genetic test result that indicates the presence of the Huntington's disease gene variant in the individual. However, when the individual is examined by a neurologist (a physician with appropriate training and expertise for diagnosing Huntington's disease) because the individual has begun to suffer from occasional moodiness and disorientation (symptoms which are associated with Huntington's disease), and the results of the examination do not support a diagnosis of Huntington's disease, then Huntington's disease is not manifested with respect to the individual. In contrast, if the individual exhibits additional neurological and behavioral symptoms, and the results of the examination support a diagnosis of Huntington's disease by the neurologist, then Huntington's disease is manifested with respect to the individual.

- An individual has had several family members with colon cancer, one of whom underwent genetic testing which detected a mutation in the MSH2 gene associated with hereditary nonpolyposis colorectal cancer (HNPCC). On the recommendation of his physician (a health care professional with appropriate training and expertise in the field of medicine involved), the individual undergoes a targeted genetic test to look for the specific mutation found in the family member of the individual to determine if the individual himself is at increased risk for cancer. The genetic test shows that the individual also carries the mutation but the individual's colonoscopy indicates no signs of disease and the individual has no symptoms. Because the individual has no signs or symptoms of colorectal cancer that could be used by the individual's physician to diagnose the cancer, HNPCC is not a manifested disease with respect to the individual. In contrast, if the individual undergoes a colonoscopy or other medical tests that indicate the presence of HNPCC, and the individual's physician makes a diagnosis of HNPCC, HNPCC is a manifested disease with respect to the individual.

- If a health care professional with appropriate expertise makes a diagnosis based on the symptoms of the patient, and uses genetic tests to confirm the diagnosis, the disease will be considered manifested,

despite the use of genetic information. For example, if a neurologist sees a patient with uncontrolled movements, a loss of intellectual faculties, and emotional disturbances, and the neurologist suspects the presence of Huntington's disease, the neurologist may confirm the diagnosis with a genetic test. While genetic information is used as part of the diagnosis, the genetic information is not the sole or principal basis for the diagnosis, and, therefore, the Huntington's disease would be considered a manifested disease of the patient."

g. Definition of Health Plan [78FR5664]

There is a slight change in the definition of "health plan to include voluntary prescription drug benefit programs."

4. Section 164.501 – Definitions [78FR5665]

a. Definition of Underwriting purposes [78FR5665]

"Underwriting purposes is defined as with respect to a health plan means, or with respect to a group health plan, health insurance coverage, or Medicare supplemental policy: (A) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy; (B) the computation of premium or contribution amounts under the plan, coverage, or policy; (C) the application of any pre-existing condition exclusion under the plan, coverage, or policy; and (D) other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits."

The Department proposed to adopt:

b. Definition of Health Care Operations [78FR5666]

OCR notes that the definition of healthcare operations has been changed and adds underwriting and similar terms.

c. Definition of Payment [78FR5666]

OCR notes that the definition of payment includes such items as determination of benefits and underwriting.

5. Section 164.502(a) – Uses and Disclosures of Protected Health Information
General Rules [78FR5666]

a. Prohibition

OCR has added this section to clearly outline the prohibited uses and disclosures of genetic information for underwriting purposes except for issuers of long-term care policies. OCR further clarifies that underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under a plan.

6. Section 164.504(f)(1)(ii) – Requirements for Group Health Plans [78FR5667]

This section clarifies that health plans may release summary health information to the plan sponsor with genetic information, as long as the request is not for underwriting purposes. OCR also ensures that any agents who receive the PHI agrees to the same restrictions that apply to the plan sponsor.

7. Section 164.506 – Uses and Disclosures to Carry out Treatment, Payment, or Health Care Operations [78FR5667]

This section was modified to add the cross reference of §164.502(a)(5)(i) that prohibits the use of genetic information for underwriting even though this use and disclosure is typically considered a payment or healthcare operation.

8. Section 164.514(g) – Uses and Disclosures for Activities relating to the creation, Renewal, or Replacement of a Contract of Health Insurance or Health Benefits [78FR5667]

The final rule clarifies that a health plan may continue to use or disclose genetic information as required by law, except when doing so would be contrary with §164.502(a)(5)(i), which prohibit the use of genetic information for underwriting.

9. Section 164.520 – Notice of Privacy Practices for Protected Health Information [78FR5667]

If a health plan plans to perform underwriting activities, it must include a statement in the Notice of Privacy Practices that it is prohibited from using or disclosing genetic information for such purposes.

10. Other Comments [78FR5668]

It is important to note that healthcare providers may continue to disclose genetic information, as this meets the minimum necessary standard, to health plans for payment purposes. It is the health plan that is required not to use this information for underwriting purposes.

VII. Regulatory Analysis [78FR5669]

Under a variety of laws, a rule notice must contain analysis responses to a series of requirements. As OCR indicates in its Executive Summary (78FR5567), it expects the costs associated with the rules above to be somewhere between $114 million and $225.4 million, while it cannot accurately break down the benefits to the stakeholders involved especially the individual. As Congress did not specify a cap on costs, the rule proceeds to implementation and compliance.

Readers interested in specifics in the OCR analysis can find the breakdown as follows:

A. Introduction [78FR5669]

B. Why is the Rule Needed [78FR5670]

C. Costs [78FR5670]

1. Breach Notice Costs [78FR5670]

Cross the board annual compliance costs for Breach Notification in 2011: $14,475,600.00 which includes:

- E-mail and 1st Class Mail: $ 3,467,122
- Substitute Notices and Media Notices: 571,200
- Substitute Notices and Toll Free Number: 1,816,379
- Imputed costs to affected individual who called the toll-free line: 2,052,665
- Notice to Media of Breach Over 500: 15,420
- Report to the Secretary: 500 or More: 15,420
- Investigation Costs: Under 500: 5,277,456
- Investigation Costs: 500 or More: 837,500
- Annual Report to the Secretary: Under 500: 422,438

2. Notifying Individual of Their New Privacy Rights [78FR5675]

OCR provides an estimate of the cost of providing a new notice as explained above. OCR estimates the total costs at $55.9 million.

3. Business Associate and Covered Entity and Their Contractual Relationships [78FR5677]

OCR provides an estimate of the costs involved, based on hours and related to Security Rule compliance documentation and business associate agreements between business associates and subcontractors as:

- Security Rule: $ 22.6 million - $113 million
- business associates and Subcontractors: $ 21 million - $42 million

4. Qualitative Analysis of Unquantified Costs [78FR5679]

This section includes discussion on:

- Authorizations for Uses and Disclosure of Protected Health Information for Marketing and Sales of PHI
- Individual Right to Opt Out of Fundraising Communications
- Individuals' Access to PHI
- Right to Restrict Certain Disclosures to Health Plans
- Impact of Genetic Information Underwriting Probation on Health Plans
- Enforcement Provisions

D. Qualitative Analysis of Unqualified Benefits [78FR5682]

1. Greater Privacy Protections for Individuals [78FR5682]
2. Breach Notification [78FR5682]
3. Compound Authorizations for Research Uses and Disclosures [78FR5683]
4. Authorizations for Future Research Uses and Disclosures [78FR5683]
5. Period of Protection for Decedent Information [78FR5683]
6. Disclosure About a Decedent [78FR5683]
7. Public Health Disclosures [78FR5683]

E. Additional Regulatory Analysis [78FR5684]

This section covers analysis under a separate law. Subjects include:

1. Regulatory Flexibility Act
2. Unfunded Mandate Reform Act

3. Federalism

F. Accounting Statement [78FR5686]

VIII. Collection of Information Requirements [78FR5687]

List of Subparts [78FR5687 – 5702]

45CFR Part 160 – 164: Language of the final rule.

Representing more than 67,000 specially educated Health Information Management professionals in the United States and around the world, the American Health Information Management Association is committed to promoting and advocating for high quality research, best practices and effective standards in health information and to actively contributing to the development and advancement of health information professionals worldwide. AHIMA's enduring goal is quality healthcare through quality information.

www.ahima.org