

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN 0991-AB54

HIPAA Administrative Simplification: Standards for Privacy of Individually Identifiable Health Information

AGENCY: Office for Civil Rights, HHS.

ACTION: Proposed rule.

SUMMARY: The Department of Health and Human Services (HHS) proposes to modify certain provisions of the "Standards for Privacy of Individually Identifiable Health Information" (Privacy Rule), issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of these proposed modifications is to implement section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 (GINA) regarding the privacy and confidentiality of genetic information, as well as to make certain other changes to the HIPAA Privacy Rule.

DATES: Comments on the proposed rule will be considered if we receive them at the appropriate address, as provided below, no later than December 7, 2009.

ADDRESSES: Written comments may be submitted through any of the methods specified below. Please do not submit duplicate comments.

- *Federal eRulemaking Portal:* You may submit electronic comments at <http://www.regulations.gov>. Follow the instructions for submitting electronic comments. Attachments should be in Microsoft Word, WordPerfect, or Excel; however, we prefer Microsoft Word.

- *Regular, Express, or Overnight Mail:* You may mail written comments (one original and two copies) to the following address only: U.S. Department of Health and Human Services, Office for Civil Rights, Attention: GINA NPRM (RIN 0991-AB54), Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. Mailed comments may be subject to delivery delays due to security procedures. Please allow sufficient time for mailed comments to be timely received in the event of delivery delays.

- *Hand Delivery or Courier:* If you prefer, you may deliver (by hand or courier) your written comments (one original and two copies) to the following address only: Office for Civil Rights, Attention: GINA NPRM (RIN 0991-AB54), Hubert H. Humphrey Building,

Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. (Because access to the interior of the Hubert H. Humphrey Building is not readily available to persons without federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. We will post all comments received before the close of the comment period at <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT:

Andra Wicks, 202-205-2292.

SUPPLEMENTARY INFORMATION:

I. Background

The "Standards for Privacy of Individually Identifiable Health Information," or "Privacy Rule" was issued on December 28, 2000 (and later amended in August 2002), pursuant to the Administrative Simplification Provisions of Title II, Subtitle F, of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191. Subtitle F of Title II of HIPAA added a new Part C to Title XI of the Social Security Act (sections 1171-1179 of the Act, 42 U.S.C. 1320d-1320d-8). The Privacy Rule is one of a suite of rules required by the Administrative Simplification provisions of HIPAA, and put in place the first national standards for the privacy protection of certain individually identifiable health information (called "protected health information" or "PHI"). The other HIPAA Administrative Simplification Rules provide national standards for electronic health care transactions and code sets, unique health identifiers for employers and health care providers, and the security of electronic PHI. The HIPAA Privacy and other Administrative Simplification Rules currently apply to three types of covered entities: health care providers who conduct covered health care transactions electronically, health plans, and health care clearinghouses.

The HIPAA Privacy Rule protects individuals' medical records and other individually identifiable health information held by HIPAA covered entities by, among other provisions, requiring appropriate safeguards to protect the privacy of such information, and setting limits and conditions on the uses and disclosures that may be made

of the information. The Privacy Rule also gives patients rights over their PHI, including rights to examine and obtain a copy of their health records, and to request corrections.

On May 21, 2008, President Bush signed into law the Genetic Information Nondiscrimination Act of 2008 ("GINA"), Public Law 110-233, 122 Stat. 881. Congress enacted GINA to "establish [] a national and uniform basic standard [that] is necessary to fully protect the public from discrimination and allay their concerns about the potential for discrimination, thereby allowing individuals to take advantage of genetic testing, technologies, research, and new therapies." GINA section 2(5). To that end, GINA generally prohibits discrimination based on an individual's genetic information with respect to both health coverage and employment.

In particular, with respect to health coverage, Title I of GINA generally prohibits discrimination in group premiums based on genetic information, proscribes the use of genetic information as a basis for determining eligibility or setting premiums in the individual and Medicare supplemental policy (Medigap) insurance markets, and limits the ability of group health plans, health insurance issuers, and Medigap issuers to collect genetic information or to request or require that individuals undergo genetic testing. Title II of GINA generally prohibits use of genetic information in the employment context, restricts acquisition of genetic information by employers and other entities covered by Title II, and strictly limits such entities from disclosing genetic information. The Departments of Labor (Employee Benefits Security Administration), Treasury (Internal Revenue Service), and HHS (Centers for Medicare & Medicaid Services) are responsible for administering and enforcing the GINA Title I nondiscrimination provisions, and the Equal Employment Opportunity Commission (EEOC) is responsible for administering and enforcing the GINA Title II nondiscrimination provisions.¹

¹ The Departments of Labor (Employee Benefits Security Administration), Treasury (Internal Revenue Service), and HHS (Centers for Medicare & Medicaid Services (CMS)) have issued regulations in a separate rulemaking to implement sections 101-103 of GINA, which amended: section 702(b) of the Employee Retirement Income Security Act of 1974 (29 U.S.C. 1182(b)); section 2702(b) of the Public Health Service Act (42 U.S.C. 300gg-1(b)); and subsection (b) of section 9802 of the Internal Revenue Code of 1986. Section 104 of GINA applies to Medigap issuers, which are subject to the provisions of section 1882 of the Social Security Act that are implemented by CMS, and which incorporate by reference certain provisions in a model regulation of the National Association of

In addition to these nondiscrimination provisions, Title I of GINA contains certain new privacy protections for genetic information. In particular, section 105 of GINA, entitled "Privacy and Confidentiality," amends Part C of Title XI of the Social Security Act by adding section 1180 to address the application of the HIPAA Privacy Rule to genetic information. Section 1180 requires the Secretary of HHS to revise the Privacy Rule to clarify that genetic information is health information and to prohibit group health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes.

In this proposed rule, HHS is proposing to implement the modifications required by GINA section 105, as well as to make certain other modifications to the HIPAA Privacy Rule, and seeks public comment on its proposal. In developing its proposal, HHS consulted with the Departments of Labor and Treasury, as required by section 105(b)(1) of GINA, to ensure, to the extent practicable, consistency across the regulations. In addition, HHS coordinated with the EEOC in the development of these regulations.

II. Description of Proposed Modifications

Overview and Scope

In accordance with section 105 of GINA² and the Department's general authority under sections 262 and 264 of HIPAA, the Department proposes to modify the HIPAA Privacy Rule to: (1) Explicitly provide that genetic information is health information for purposes of the Rule; (2) prohibit health plans from using or disclosing protected health information that is genetic information for underwriting purposes; (3) revise the provisions relating to the Notice of Privacy Practices for health plans that perform underwriting; (4) make a number of conforming modifications to definitions and other provisions of the Rule; and (5) make technical corrections to update the definition of "health plan."

Section 105 of GINA requires HHS to modify the Privacy Rule to prohibit "a

covered entity that is a group health plan, health insurance issuer that issues health insurance coverage, or issuer of a medicare [sic] supplemental policy" from using or disclosing genetic information for underwriting purposes. GINA section 105 provides that the terms "group health plan" and "health insurance coverage" have the meanings given such terms under section 2791 of the Public Health Service Act (42 U.S.C. 300gg–91), and that the term "medicare [sic] supplemental policy" has the meaning given such term in section 1882(g) of the Social Security Act. In addition, the term "health insurance issuer," as defined at 42 U.S.C. 300gg–91, includes a health maintenance organization (HMO). These four types of health plans (i.e., group health plans, health insurance issuers, and health maintenance organizations, as defined in the Public Health Service Act, as well as issuers of Medicare supplemental policies), correspond to the types of health plans listed at subparagraphs (i) through (iii) and (vi) of paragraph (1) of the definition of "health plan" at § 160.103 in the HIPAA Privacy Rule.

In addition to these four categories of health plans, the HIPAA Privacy Rule also applies to many other types of health plans, including: (1) Long-term care policies (excluding nursing home fixed-indemnity policies); (2) employee welfare benefit plans or other arrangements that are established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers (to the extent that they are not group health plans or health insurance issuers); (3) high risk pools that are mechanisms established under State law to provide health insurance coverage or comparable coverage to eligible individuals; (4) certain public benefit programs, such as Medicare Part A and B, Medicaid, the military and veterans health care programs, the Indian Health Service program, and others; as well as (5) any other individual or group plan, or combination of individual or group plans that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)). This last category includes, for example, certain "excepted benefits" plans described at 42 U.S.C. 300gg–91(c)(2), such as limited scope dental or vision benefits plans. See the definition of "health plan" at § 160.103.

The Department proposes to apply the prohibition in GINA on using and disclosing protected health information that is genetic information for underwriting to all health plans that are subject to the Privacy Rule, rather than solely to the plans GINA explicitly

requires be subject to the prohibition. We believe that this interpretation is consistent with both GINA and the Secretary's broad authority under HIPAA.

Section 264 of HIPAA (42 U.S.C. 1320d–2 note) provides the Secretary with authority to promulgate privacy standards that govern:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

Accordingly, the Secretary has wide latitude to promulgate privacy standards that limit the use or disclosure of individually identifiable health information, including genetic information. Furthermore, section 262 of HIPAA, codified at 42 U.S.C. 1320d–1, states that:

Any standard adopted under this part shall apply, in whole or in part, to the following persons:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1).

While other portions of HIPAA were limited to group health plans, *see, e.g.*, sections 101 and 102 of HIPAA, the Administrative Simplification subtitle governs a substantially broader definition of "health plan," 42 U.S.C. 1320d, and instructs that "any standard" will apply to all such health plans.

Based on this broad definition of "health plan," the wide latitude Congress provided to the Secretary to promulgate privacy standards, and the charge that "any standard" should apply to all health plans, we interpret that the HIPAA administrative simplification provisions provide the Secretary with broad authority to craft privacy standards that uniformly apply to all health plans, regardless of whether such health plans are governed by other portions of the HIPAA statute.

In GINA, Congress recognized a privacy interest on the part of individuals, distinct from the nondiscrimination provisions, with respect to the use or disclosure of individuals' genetic information in health coverage decisions. At a minimum, GINA requires the Secretary to apply this privacy interest to uses and disclosures of group health plans, health insurance issuers that issue health insurance coverage, and issuers of

Insurance Commissioners (NAIC). The NAIC amended its model regulation on September 24, 2008, to conform to section 104 of GINA, and the amended regulation was published by CMS in the *Federal Register* on April 24, 2009 at 74 FR 18808. With respect to Title II of GINA, the EEOC issued a notice of proposed rulemaking on March 2, 2009, at 74 FR 9056.

² Any reference in this section of the preamble to GINA is a reference to Title I of GINA, except as otherwise indicated.

Medicare supplemental policies. Apart from this required change to the HIPAA Privacy Rule, however, nothing in GINA explicitly or implicitly curtails the broad authority of the Secretary to promulgate privacy standards for any and all health plans that are governed by the HIPAA Administrative Simplification provisions.

Under the Privacy Rule, consistent with the HIPAA statutory text discussed above, an individual's privacy interests and rights with respect to the use and disclosure of PHI are protected uniformly without regard to the type of health plan that holds the information. Thus, under the Privacy Rule, individuals can expect and benefit from privacy protections that do not diminish based on the type of health plan from which they obtain health coverage.

Therefore, in keeping with a uniform privacy construct, and pursuant to its authority under HIPAA sections 262 and 264, the Department proposes to apply the prohibition on using or disclosing PHI that is genetic information for underwriting purposes to all health plans that are covered entities as defined by HIPAA section 262, and, correspondingly, by the Privacy Rule. The Department believes that individuals' interests in uniform protection under the Privacy Rule against the use or disclosure of their genetic information for underwriting purposes outweigh any adverse impact on health plans that are not covered by GINA. This is particularly true since we do not expect that all of the health plans subject to the Privacy Rule use or disclose PHI that is genetic information for underwriting today (or even conduct underwriting generally, in the case of some of the public benefit plans).

Consistent with § 160.104(c), the Department intends to require health plans to comply with these modifications to the privacy standards no later than 180 days from the effective date of such modifications. Note that the Department does not propose to extend the compliance date for small health plans as the Department believes 180 days is sufficient time for small health plans to come into compliance with the proposed requirements.

With this overview and description of the scope of the proposed rule as foundation, the following discussion describes the proposed modifications to the Privacy Rule section by section. Those interested in commenting on the proposed provisions can assist the Department by preceding discussion of any particular provision in the comment with a citation to the section of the proposed rule being discussed, or, if submitting a comment relevant to the

above discussion, with the term "Scope."

Section 160.103—Definitions

The Department is proposing to modify § 160.103 to: (1) Explicitly provide, as required by GINA, that the definition of "health information" encompasses "genetic information"; (2) add a number of terms used in GINA Title I for purposes of implementing GINA's provisions; and (3) make certain technical corrections to update the definition of "health plan." We note that with respect to the GINA terms, this proposed rule proposes to adopt definitions that are generally consistent with the definitions of such terms promulgated in the implementing regulations for sections 101–103 of GINA.

1. Health information. The Department has always maintained that genetic information is health information protected by the Privacy Rule to the extent such information is individually identifiable and held by a covered entity (subject to the general exclusions from the definition of "protected health information"). Frequently Asked Question number 354, available at <http://www.hhs.gov/ocr/privacy/hipaa/faq/about/354.html>, states:

Question: Does the HIPAA Privacy Rule protect genetic information?

Answer: Yes, genetic information is health information protected by the Privacy Rule. Like other health information, to be protected it must meet the definition of protected health information: it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse. See 45 CFR 160.103.

Nevertheless, section 105 of GINA requires the Secretary to revise the Privacy Rule to make clear that genetic information is health information under the Rule. Accordingly, the Department proposes to modify the definition of "health information" at § 160.103 to explicitly provide that such term includes genetic information. We note, however, that as before, genetic information, while health information, is only covered by the Privacy Rule to the extent that it meets the definition of "protected health information." That is, the genetic information must be individually identifiable and maintained by a HIPAA covered entity (or business associate of a covered entity) (and not otherwise fall within one of the exceptions to the definition). See the definition of "protected health information" at § 160.103.

2. Genetic information. The term "genetic information" is a defined term in GINA that establishes what information is protected by the statute.

GINA section 105 provides that the term "genetic information" in section 105 shall have the same meaning given the term in section 2791 of the Public Health Service Act (PHSA) (42 U.S.C. 300gg–91), as amended by GINA section 102. Section 102(a)(4) of GINA defines "genetic information" to mean, with respect to any individual, information about: (1) Such individual's genetic tests; (2) the genetic tests of family members of such individual; and (3) the manifestation of a disease or disorder in family members of such individual (i.e., family medical history). GINA also provides that the term "genetic information" includes, with respect to any individual, any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by such individual or family member of such individual; however, GINA excludes information about the sex or age of any individual. The basic definition of "genetic information" in section 102(a)(4) of GINA (and that is to apply for purposes of section 105) is also expanded by section 102(a)(3), which provides that any reference to genetic information concerning an individual or family member in the PHSA shall include: with respect to an individual or family member of an individual who is a pregnant woman, the genetic information of any fetus carried by such pregnant woman; and with respect to an individual or family member utilizing an assisted reproductive technology, the genetic information of any embryo legally held by the individual or family member. The Department proposes to include this statutory definition of "genetic information" in § 160.103 without substantive change.

3. Genetic test. As indicated above, GINA provides that the term "genetic information" includes information about an individual's genetic tests or the genetic tests of family members of such individual. As with the term "genetic information," GINA section 105 provides that the term "genetic test" shall have the same meaning as the term has in section 2791 of the PHSA (42 U.S.C. 300gg–91), as amended by section 102 of GINA. Section 102(a)(4) of GINA amends section 2791 of the PHSA to define "genetic test" to mean "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes." GINA further clarifies that the term "genetic test" does not include an analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes, or that is directly related to a

manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved.

Consistent with the statutory definition of "genetic test," the Department proposes to define "genetic test" at § 160.103 as an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations or chromosomal changes, and to provide in the definition that "genetic test" does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition. The statute does not define "manifestation" or "manifested." Consequently, as discussed below, the Department proposes to include a definition of "manifestation or manifested."

Under this proposed definition of "genetic test," a test to determine whether an individual has a gene variant associated with breast cancer (such as the BRCA1 or BRCA2 variant) is a genetic test. Similarly, a test to determine whether an individual has a genetic variant associated with hereditary nonpolyposis colorectal cancer is a genetic test. However, medical tests that analyze genetic material that is not of human origin, such as tests that detect the presence of viruses or bacteria in an individual, or tests that do not detect genotypes, mutations, or chromosomal changes, are not genetic tests. For example, an HIV test, complete blood count, cholesterol test, liver function test, or test for the presence of alcohol or drugs is not a genetic test.

4. *Genetic services.* GINA provides that the term "genetic information" includes, with respect to any individual, any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by such individual or any family member of such individual. As with the definitions above, section 105 of GINA provides that the term "genetic services" shall have the meaning given such term in section 2791 of the PHSA (42 U.S.C. 300gg-91), as amended by section 102 of GINA. Section 102(a)(4) of GINA defines "genetic services" to mean: (1) A genetic test; (2) genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) genetic education. Thus, the fact that an individual or a family member of the individual requested or received a genetic test, counseling, or education is information protected under GINA.

Genetic counseling is a means for individuals to obtain information and support about potential risks for genetic diseases and disorders. Genetic education is also a means for individuals to obtain information about potential risks for genetic diseases and disorders. The Department proposes to add the statutory definition of "genetic services" to § 160.103 without substantive change.

5. *Family Member.* The term "family member" is used in the definition of "genetic information" in GINA to indicate that an individual's genetic information also includes information about the genetic tests of the individual's family members, as well as family medical history. GINA section 105 states that the term "family member" shall have the meaning given such term in section 2791 of the PHSA (42 U.S.C. 300gg-91), as amended by GINA section 102(a)(4), which defines "family member" to mean, with respect to any individual: (1) A dependent (as such term is used for purposes of section 2701(f)(2) of the PHSA, 42 U.S.C. 300gg(f)(2)) of such individual; or (2) any other individual who is a first-degree, second-degree, third-degree, or fourth-degree relative of such individual or of a dependent of the individual. Section 2701(f)(2) of the PHSA uses the term "dependent" to mean an individual who is eligible for coverage under the terms of a group health plan because of a relationship to the participant.

The Department proposes to incorporate the statutory definition of "family member" into § 160.103 but also to clarify in the regulatory text that relatives by affinity (such as by marriage or adoption) are to be treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor) and that, in determining the degree of 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). This is consistent with the legislative history of GINA, which suggests that the term "family member" is to be broadly construed to provide the maximum protection against discrimination. See House Report 110-28, Part 2 at 27. In addition, the Department proposes to include in the regulatory definition, non-exhaustive lists of persons who are first-, second-, third-, or fourth-degree relatives. Finally, the Department proposes in the definition of "family member" to refer to the definition of "dependent" in the implementing regulations at 45 CFR 144.103 rather

than to the PHSA directly. The Department invites public comment on this definition.

We also note that the term "family member" is not currently defined in the Privacy Rule but is used in the Privacy Rule at § 164.510(b), which provides the standard for uses and disclosures of an individual's PHI to family members and other persons involved in the individual's care and for notification purposes. It is not expected that adding to the Privacy Rule the above broad definition of the term "family member" would impact the scope of these existing provisions, particularly given the use in the provisions of the additional terms "other relative," "close personal friend," "other person identified by the individual," "personal representative," and "other person responsible for the care of the individual," which would appear to capture any other person, as appropriate, who would not qualify as a "family member" by the new definition.

In addition to the use of the term "family member" in the Privacy Rule, the term "family" is used in three other instances in the Rule: (1) In reference to the Family Educational Rights and Privacy Act in the definition of "protected health information" at § 160.103; (2) in the definition and disclosure permission for psychotherapy notes (at §§ 164.501 and 164.508(a)(2)(B), respectively) where such notes may be created based upon, and used to train within, a family counseling session; and (3) in the disclosure permission at § 164.512(k)(4) for medical suitability determinations by the Department of State for circumstances where family accompany a Foreign Service member abroad. It is also not expected that including a definition of "family member" in the Privacy Rule would impact these provisions, as the scope of the term "family" in each occurrence is determined independently of the Privacy Rule.

6. *Manifestation or manifested.* Although not separately defined by GINA, the terms "manifestation" or "manifested" are used in GINA in three important contexts. First, GINA uses the term "manifestation" to incorporate "family medical history" into the definition of "genetic information" by stating that "genetic information" includes, with respect to an individual, the *manifestation* of a disease or disorder in family members of such individual. Second, GINA uses the term "manifested" to exclude from the definition of "genetic test" those tests that analyze a physical malady rather

