Testimony
Before the Subcommittee on Health
Committee on Energy and Commerce
United States House of Representatives

Statement of

Susan D. McAndrew, J.D.

Deputy Director for Health Information Privacy
Office for Civil Rights
U.S. Department of Health and Human Services

For Release on Delivery
Expected at 1:00 p.m.
Thursday, March 8, 2007

Introduction

Mr. Chairman and members of Committee, I am Susan McAndrew, Deputy Director for Health Information Privacy, in the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS). OCR is responsible for the administration and enforcement of the Privacy Rule, issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). On behalf of Winston Wilkinson, the Director of OCR, I thank you for the invitation to testify today on the role of the Privacy Rule in the protection of genetic information held by those health plans and health care providers that are covered by the Rule.

Background

The *Standards for Privacy of Individually Identifiable Health Information* – better known as the HIPAA Privacy Rule – establishes, for the first time, a set of national standards for the protection of certain health information. In December 2000, HHS issued the Privacy Rule to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Those regulations were modified in a number of significant ways by further rulemaking in August 2002 to ensure the final Privacy Rule was workable and to avoid unintended consequences of certain provisions that would have impeded an individual's access to health care or prompt payment for those health care services. These federal privacy standards have been in operation for almost four years, and we are pleased to note that significant progress is being made to embed these privacy principles into the daily practices of health plans and health care providers across the nation.

The Privacy Rule standards address the use and disclosure of certain health information that is individually identifiable – called protected health information – by persons or entities that are subject to the HIPAA requirements – called covered entities. It is important to remember that the HIPAA Privacy Rule only directly applies to persons or entities that are defined as "covered entities," including health plans, health care clearinghouses, and any health care provider that electronically transmits health information in connection with a transaction – such as billing a health plan for reimbursement for services – for which there is a HIPAA standard transaction and code set. The Privacy Rule standards also give individuals certain rights with respect to their health information, including the right to receive notice from a covered entity about that entity's privacy responsibilities and practices and about the individual's other rights under the HIPAA Privacy Rule; the right to access and get a copy of their medical record; the right to have that record amended if it is incomplete or incorrect; and the right to request an accounting from the covered entity of certain disclosures of protected health information. The HIPAA Privacy Rule creates a uniform federal floor of privacy protections for health information; however, it does not prevent states or entities from adopting laws or practices that provide additional privacy protections.

The Privacy Rule is carefully balanced to ensure strong privacy protections without impeding the flow of information necessary to provide access to quality health care, and to that end, the Rule permits covered entities to share protected health information for core purposes – to treat the individual and to obtain payment for the health care service provided – without obtaining the individual's prior consent or authorization. The Privacy Rule also permits other uses and

disclosures of protected health information without an individual's authorization, including uses and disclosures necessary for the normal business operations of health plans and providers, as well as a limited number of public interest disclosures where identifiable health information is needed for these purposes. For example, and subject to specific conditions or limitations, a covered entity may, without individual authorization, disclose protected health information as required by other federal or state law, for public health purposes, or to permit health oversight agencies to carry out their functions. And, of course, the individual may authorize in writing any other use or disclosure of protected health information. The Rule establishes standards to make sure that individuals' authorizations for particular uses or disclosures of protected health information are both informed and voluntary.

Key Privacy Rule Provisions for Genetic Information

With this general background, I would like to turn to the specific provisions of the HIPAA Privacy Rule that will have the most direct impact on how genetic information is protected and the circumstances that permit a covered entity to share such information with others.

Genetic Information as Protected Health Information

The HIPAA Privacy Rule protects certain individually identifiable health information that is held by a covered entity or its business associate. Individually identifiable genetic information that is obtained by a covered health care provider or health plan is therefore subject to the protection of

the HIPAA Privacy Rule. As indicated above, the Privacy Rule provides a federal baseline of protection for all protected health information, including genetic information.

With very limited exceptions that are not relevant to the protection of genetic information, the Rule does not differentiate among the identifiable health information protected – that is, it does not classify some protected health information as "sensitive" or provide heightened protections for these types of information. The Privacy Rule does, however, preserve state or other law that may provide more stringent privacy protections for particular types of health information. Therefore, state laws that provide additional privacy protections for genetic information remain in effect.

Permitted Uses and Disclosures of Protected Health Information by Health Plans

The Privacy Rule standards control how health plans – as covered entities under HIPAA – may use or disclose protected health information, including genetic information. The Privacy Rule recognizes payment for health care services as a core function, and permits the use and disclosure of protected health information without individual authorization for payment purposes, along with the health care operation activities necessary to support this function. These core functions allow a health plan to use or disclose protected health information as necessary to determine or fulfill its responsibilities for coverage and provision of benefits under the health plan, and to provide payment or reimbursement for health care services provided to individuals. Among the activities included in the payment function are determinations of eligibility or coverage, risk adjusting, billing and claims management, collection of premiums,

and utilization review activities. In addition, health plans may, with some additional limitations on the recipient of such information, use or disclose protected health information for underwriting, premium rating, or other activities related to the creation, renewal or replacement of a contract of health insurance. When using or disclosing protected health information for these payment or health care operations purposes, or when requesting protected health information from another covered entity, the health plan must make reasonable efforts to use, disclose or request only such information as is minimally necessary to accomplish the intended purpose.

In general, under the Privacy Rule, a health plan is not permitted to require the individual to sign an authorization for the release of protected health information as a condition payment, enrollment in or eligibility for benefits under a health plan. However, the Rule does allow health plans to condition enrollment in or eligibility for benefits under the plan on obtaining an individual's authorization, if it is requested by the plan prior to the individual's enrollment. The authorization must limit the health information sought to that needed for an enrollment or eligibility determination for that individual or for its underwriting or risk rating determinations. Thus, under the HIPAA Privacy Rule, protected health information, including genetic information, could be requested by the plan for enrollment, eligibility or underwriting purposes and used by the plan in making these determinations today.

While beyond the scope of my testimony here today, I should note that other laws exist to protect the use of genetic information for health insurance purposes. For example, HIPAA Title I prohibits discrimination in enrollment and eligibility for benefits in group health plans based on

health status, including genetic information. HIPAA Title I also prohibits increasing premiums or contribution rates of an individual in a group health plan based on health status, including his or her genetic information. Further, HIPAA Title I prohibits group health plans and group health insurance issuers from using genetic information – in the absence of a diagnosis of a condition related to that genetic information – as the basis for a "preexisting condition exclusion."

It is important to remember that the Privacy Rule is concerned with maintaining the confidentiality of individually identifiable health information provided to health care providers and health plans without impeding the ability of providers and plans to efficiently and effectively deliver high quality health care and pay for that care. The Privacy Rule does not seek to regulate the health insurance industry or the conditions or terms for the provision of coverage for health insurance. Thus, the Privacy Rule does not specifically limit how a health plan may use or disclose genetic information in its enrollment or underwriting activities, but would treat such information as any other protected health information needed for these core functions.

Disclosures of Protected Health Information to Employers

Just as the HIPAA Privacy Rule does not seek to regulate the provision of health insurance, the HIPAA statute does not permit the regulation of employers in general, or the employment functions of covered entities. A business is not a covered entity under the HIPAA Privacy Rule simply by virtue of being an employer. The Department understands that covered health insurance issuers and health care providers are also employers, and, thus, may have obtained individually identifiable health information about their employees both in their health care

capacities and in their employment capacities. To avoid potential confusion, the HIPAA Privacy Rule was amended in 2002 to expressly exclude from the definition of "protected health information" an employee's individually identifiable health information in the employment records held by a covered entity in its role as an employer.

To illustrate this distinction, the medical record of a hospital employee who is receiving treatment at the hospital is protected health information and is covered by the Privacy Rule. The hospital may use that information, including genetic information, only as permitted by the Privacy Rule, and in most cases will need the employee's authorization to access or use the information in the medical record for employment purposes. When employees give their medical information to the covered entity as the employer, such as when submitting a doctor's statement to document sick leave, or when the covered entity as employer obtains the employee's written authorization to obtain protected health information (which may include protected health information held by the employer in its capacity as a covered health care provider under HIPAA), such as an authorization to disclose the results of a fitness for duty examination, that health information becomes part of the employment record, and as such, is no longer protected health information under the HIPAA Privacy Rule. The employers' obligations with respect to employee health information contained in employment records of the employer are governed by other law on employment practices, such as the Americans with Disabilities Act, not the HIPAA Privacy Rule.

The Privacy Rule does address another employer role – that is, as the sponsor of a group health plan. Again, the Rule does not generally regulate the employer's duties or functions as a plan

sponsor, but rather determines when the group health plan – as the HIPAA covered entity – may disclose protected health information to the employer. The Privacy Rule permits the disclosure of summary health information to the plan sponsor for obtaining premium bids or for modifying, amending or terminating the group health plan, and allows the sharing of individual information on enrollment or disenrollment in the group health plan. Otherwise, the Privacy Rule restricts disclosures of protected health information, including genetic information, by the group health plan to the plan sponsor to those purposes set forth in the plan documents. Importantly, the Rule requires that the plan documents specify that the plan sponsor may not use such information for any employment related decisions. The Privacy Rule, however, does not, and cannot, restrict employment actions with respect to genetic information received by an employer directly from the employee or by virtue of a written authorization from the employee.

Closing

I trust this information will be helpful to the Committee in furthering its consideration of legislation to protect genetic information from discriminatory uses in the health insurance and employment arenas. The Department favors enactment of legislation to prohibit the improper use of genetic information in health insurance and employment, and, as you can see from my testimony, the HIPAA Privacy Rule provides an important federal baseline of protection for all protected health information, including genetic information. For additional information on Privacy Rule, the Office for Civil Rights HIPAA Privacy web site at http://www.hhs.gov/ocr/hipaa, contains the full regulatory text, as well as useful summaries of the Rule and answers to over 200 frequently asked questions.

Again, we welcome the opportunity to explain how the HIPAA Privacy Rule operates to protect an individual's health information, without impeding or delaying the delivery of health care. Mr. Chairman, this completes my prepared remarks and I will gladly answer any questions you or other members of the Committee may have at this time.