



L. Chris Petersen  
202-408-5153  
lcp@mmmlaw.com  
www.mmmlaw.com

**Testimony Before the Subcommittee on Financial  
Institutions and Consumer Credit  
June 17, 2003**

Mr. Chairman, Members of the Subcommittee my name is Chris Petersen. I am a partner in the law firm of Morris, Manning & Martin, LLP and co-chair of the firm's Privacy and Security Practice Group. Over the past three years the firm has provided privacy advice to over 50 different insurance-related entities including insurance companies, agencies, trade associations and business associates or service providers.

I am testifying today on behalf of one of those clients, the Health Insurance Association of America ("HIAA"). HIAA is the nation's most prominent trade association representing the private health care system. Its nearly 300 members provide the full array of health insurance products, including medical expense, long-term care, dental, disability, and supplemental coverage to more than 100 million Americans.

My testimony today will focus on the continuum of federal and state privacy laws and the interplay among these various laws. The testimony will only focus on the major privacy laws regulating the insurance industry. These laws include the federal Fair Credit Reporting Act; HIPAA Privacy Rule, the Gramm-Leach-Bliley Act; NAIC/State Privacy Information Acts; and State-Based Information or Event Specific Privacy Laws.

The ordering of these laws generally represents the impact that these laws have on the insurance industry. However, subjective ranking of the law's impact is influenced by several factors. For instance, a single state health plan with very little state regulation might find the HIPAA Privacy Rule to have the greatest impact on its operation. On the other hand, large insurers implementing national, uniform privacy policies and procedures could find that individual state specific laws probably create the greatest challenges.

June 16, 2003

Page 2

When analyzing privacy laws insurance entities must begin by answering some initial questions. First, what types of entities does the law regulate: financial institution, insurance institution, health plan, licensee of a state insurance department, etc. Second, insurance entities must determine what kind of information is the law protecting: financial, medical, personal, protected health information, specific health information, etc. Each law, and quite often-individual states, takes unique approaches to regulating the uses and/or disclosures of the information that insurance entities gather and possess. The following is a summary of the major laws that regulate insurance entities uses and disclosure of information.

### **Federal Fair Credit Reporting Act ("FCRA")**

FCRA regulates "consumer reporting agencies" and the uses of "consumer reports." Under the FCRA, a consumer reporting agency is an entity "which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purposes of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." For insurance purposes, the key component of the definition is whether one "furnishes consumer reports to third parties."

A consumer report is any communication of any information that bears "on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for purposes of servicing as a factor in establishing the consumer's eligibility for...insurance to be used primarily for personal, family or household purposes." The statute, however, contains two key exceptions to the definition of a consumer report.

First, the term consumer report does not include a report containing information solely as to transactions or experiences between the consumer and the person making the report so long as the information is only shared among companies related by common ownership or affiliated by corporate control. Second, a consumer report does not include the communication of "other information" among affiliates if the sharing of the "other information" is disclosed to the consumer and the consumer is given the opportunity, before the information is shared, to direct that such information not be shared, i.e., they must be granted the right to "opt out" of the information sharing. Note that these exceptions only apply to the sharing of information with affiliates. The exceptions are not available if the entity shares the information with non-affiliated third parties.

The FCRA allows limited sharing of consumer reports, i.e., the sharing of information that is not related to the entity's own transactions or experiences or the sharing of information for which the entity has not provided the right to opt out of the sharing. For insurance purposes, consumer reports may only be furnished to "a person who intends to use the information in connection with the

June 16, 2003

Page 3

underwriting of insurance involving the consumer” or to “a person who otherwise has a legitimate business need for the information in connection with a business transaction that is initiated by the consumer or to review an account to determine whether the consumer continues to meet the terms of the account.” However, insurers and other entities that qualify as a consumer reporting agency may not share, without authorizations, consumer reports that contain medical information.

As the Committee is aware, important provisions of the FCRA are up for reauthorization. The HIAA supports the reauthorization of the FCRA.

### **Standards for Privacy of Individually Identifiable Health Information (“HIPAA Privacy Rule”)**

As a general rule, those insurers that meet the definition of a health plan may not use or disclose protected health information, except as permitted or required by the HIPAA Privacy Rule. The HIPAA Privacy Rule only mandates two types of disclosures: 1) disclosures to individuals who have requested access to their protected health information under the Privacy Rule’s access requirements; and 2) when required by the Secretary of Health and Human Services to investigate or determine the health plan’s compliance with the Privacy Rule. The HIPAA Privacy Rule does not mandate any uses of protected health information.

Although not mandated by the HIPAA Privacy Rule, the Privacy Rule permits health plans to make disclosures that are required by other applicable law. These disclosures are not “mandatory disclosures” under the Rule, but obviously health plans must comply with the provisions of these other laws regarding required disclosures.

In addition, the HIPAA Privacy Rule provides for six instances under which a health plan is permitted to use or disclose protected health information. The permitted uses and disclosures are: 1) to the individual; 2) for treatment, payment or health care operations; 3) incidental uses and disclosures that occur as a byproduct of a permitted use or disclosure; 4) pursuant to an authorization; 5) disclosures related to health care facility directories and disclosures to persons involved in an individual’s care; and 6) other enumerated uses and disclosures for certain public policy purposes. Each of these permitted disclosures is discussed in more detail below. It does not appear that any of these permitted uses or disclosures would allow a health plan to disclose protected health information to another financial institution for use in that institution’s credit granting process.

If an individual specifically seeks access to their information under the HIPAA Privacy Rule’s access and accounting provisions, health plans are generally required to disclose the information to the individual. All other disclosures to individuals are permissive; it is the health plan’s decision as to whether to disclose the information.

June 16, 2003

Page 4

Health plans may use and disclose protected health information for “treatment”, “payment” and “health care operations”. Health care operations encompass a fairly broad category of uses and disclosures necessary to administer a health plan’s business and provide benefits to covered individuals. Many of a health plan’s routine uses and disclosures fall under the health care operations umbrella. Examples include underwriting, reinsuring, medical review, legal services, fraud detection, customer service, resolution of internal grievances, creating, renewing and replacing coverage, selling or transferring business, etc

Payment also encompasses a fairly broad category of uses and disclosures. It includes activities undertaken to obtain premiums, determining responsibility for coverage and provision of benefits, coordination of benefits, subrogation of health claims, billing, claims management, medical necessity determinations and utilization review. Health plans generally will not be involved in treatment activities.

The HIPAA Privacy Rule permits certain incidental uses and disclosures of protected health information that occur as a result of a use or disclosure otherwise permitted by the Rule. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. However, an incidental use or disclosure is permissible only to the extent that the health plan has applied reasonable safeguards and has implemented, if applicable, the minimum necessary standards. An example of an incidental disclosure is when someone walks into an office and overhears a telephone conversation.

Health plans may use or disclose protected health information pursuant to a valid authorization. If a health plan uses or discloses information pursuant to an authorization, the plan’s uses and disclosures of the protected health information must be consistent with the authorization.

Under some circumstances, health plans may use or disclose protected health information to a family member, other relative or a close personal friend of the individual or other person identified by the individual who is involved in the individual’s if the information is directly relevant to the person’s involvement with the individual’s care or payment related to the care. An example might be when a spouse calls regarding payment under the other spouse’s insurance coverage and the other spouse does not object to the disclosure. Health plans may also use or disclose information to notify a family member, personal representative or any other person responsible for the care of the individual of the individual’s location, general condition or death.

In order to make these uses or disclosures, the health plan must, if the individual is present or was available prior to the use or disclosure, either 1) obtain the individual’s agreement, 2) provide the individual with an opportunity to object (health plans may not make the disclosure if the individual objects) or 3) reasonably infer from the circumstances that the individual does not object to the disclosures. If the individual is not present or the opportunity to agree or object cannot practicably be provided, health plans may still make the disclosure if they determine it is in the individual’s best interest to make the disclosure.

June 16, 2003

Page 5

The HIPAA Privacy Rule specifically states that the following additional types of uses and /or disclosures are permitted without an authorization: 1) uses and disclosures required by law; 2) uses and disclosures for public health activities; 3) disclosures about victims of abuse, neglect or domestic violence; 4) uses and disclosures for health oversight activities; 5) disclosures for judicial and administrative proceedings; 6) disclosures for law enforcement purposes; 7) uses and disclosures regarding decedents such coroners and funeral directors; 8) uses and disclosures for organ and tissue donations; 9) uses and disclosures for research purposes; 10) uses and disclosures to avert a serious threat to health or safety; 11) uses and disclosures for specialized government functions such as the military or secret service; and 12) disclosures for workers' compensation coverage purposes.

I do not believe that the HIPAA Privacy Rule's permitted disclosures would allow a health plan to disclose health information to another financial institution in order for that financial institution to make credit decisions regarding the individual that is the subject of the information without the individual's signed authorization.

The HIPAA Privacy Rule's provisions regarding the application of the minimum necessary standards do not apply to uses and disclosures of protected health information made to the individual, made pursuant to an authorization, uses and disclosures that are required by law or uses and disclosures that are required for compliance with the HIPAA Privacy Rule. All other permissive uses and disclosures are subject to the Privacy Rule's minimum necessary requirements.

The HIPAA Privacy Rule provides that any privacy standard or requirement under the Privacy Rule that is "contrary to a provision of state law preempts the provision of state law. The HIPAA Privacy rule defines "contrary" as 1) a state law that would make it impossible for a health plan to comply with both state and federal requirements or 2) a state requirement that makes creates an obstacle for health plans to meet the objectives of the HIPAA Privacy Rule.

There are several important exceptions to the HIPAA Privacy Rule state preemption requirement that health plans must consider when trying to determine whether to apply federal vs. state law. The most important of these exceptions is that the HIPAA Privacy Rule will not preempt any state law that relates to the privacy of health information that is "more stringent" than the Privacy Rule.

The HIPAA Privacy Rule provides some guidance as to when a state law is more stringent than the Privacy Rule. Two important areas where a state law regarding a use or disclosure will be more stringent when the state law meets one of the following criteria:

1. The state law prohibits or restricts a use or disclosure which would otherwise be permitted under the federal rules; or
2. The state law provides greater rights of access and amendments.

June 16, 2003

Page 6

The Privacy Rule also includes a catchall category that state law is more stringent when it provides greater privacy protection for the individual.

**Privacy of Consumer Financial and Health Information Regulation  
("Model GLBA Regulation")**

In 1999 Congress, by enacting GLBA, established a statutory framework under which all financial institutions are required to protect the privacy of their customers' nonpublic personal information. Under GLBA state insurance authorities are charged, under state insurance law, with enforcing GLBA's privacy requirements with respect to "any person engaged in providing insurance..." In order to assist state insurance officials in enforcing GLBA's privacy requirements, the NAIC drafted the Model GLBA Regulation as a model for states to adopt. A significant majority of states adopted privacy rule based on the Model GLBA Regulation.

The model provides that before an insurance entity discloses any nonpublic personal financial information about an individual to a nonaffiliated third party, the insurance entity must first give the individual the opportunity to say he/she does not want his/her financial information to be disclosed. This is known as the individual's "opt out" right. In general terms, the regulation states that before an insurance entity can share a person's information the insurance entity must do the following:

- Give the individual a privacy notice;
- Give the individual an opt out form; and
- Give the individual a reasonable period of time (in most cases 30 days) to decide whether he/she wants to opt out.

Insurance entities are only permitted to disclose the information if the individual does not opt out.

There are important exceptions to the Model GLBA Regulation's general requirement. The first exception allows insurance entities to share information related to insurance functions and the public good. Examples include:

- Disclosing information to protect against or prevent fraud;
- Providing information to rating agencies;
- Replacing group coverage;
- Disclosing information as part of a sale or merger;
- Complying with federal, state or local law;
- Responding to a subpoena or summons; and
- Responding to judicial or regulatory authorities with jurisdiction over your business.

June 16, 2003

Page 7

The second exception allows insurance entities to disclose information for processing and servicing transactions that have been requested by the insurance entity's consumers and/or customers. Examples include:

- Disclosing information to underwrite products;
- Sharing information in order to administer benefits or help process claims;
- Disclosing information to process premium payments;
- Providing confirmation statements; and
- Sharing information to recognize incentives or bonuses associated with insurance transactions.

The final exception allows insurance entities to disclose financial information to outside service providers and to do joint marketing with other financial institutions without providing an opt out notice. Examples include:

- Using an outside mail fulfillment business to send marketing letters to customers;
- Using an outside call center to conduct telemarketing; and
- Giving your customer list to another insurance company or bank in order to conduct joint marketing efforts.

The Model GLBA Regulation includes special rules regulating disclosures of nonpublic personal health information. Insurance entities may not rely on the opt out rule to disclose nonpublic personal health information. Insurance entities must either have the individual's authorization to disclose the information or the disclosure must be allowed under the regulation's permitted exceptions. Generally, the regulation allows an insurance entity to disclose information in order to service a transaction that a consumer requests, to conduct insurance functions or to make disclosures that are in the "public good." The permitted disclosures are similar to the disclosures described above for financial information, but the joint marketing exception is not available for disclosures of health information. The Model GLBA Regulation also expressly permits disclosure of health information without authorization for any activity that the HIPAA Privacy Rule permits without authorization.

Although the Model GLBA Regulation permits certain disclosures of health information, insurance entities are not permitted to disclose health information to another financial institution in order for that financial institution to make credit decisions regarding the individual that is the subject of the information without the individual's signed authorization.

### **NAIC Insurance Information and Privacy Protection Model Act ("1982 Model Act")**

In 1982 the NAIC adopted its first comprehensive privacy model. This model, the 1982 Model Act, provides that insurance entities shall not disclose any personal information (including medical record information) and privileged information about an individual collected or received

June 16, 2003

Page 8

in connection with an insurance transaction unless the disclosure is authorized or specifically allowed under the Act.

The 1982 Model Act specifically allows disclosures of information for insurance functions such as conducting audits, peer review, the sale or transfer of a block of business. The Act also permits insurance entities to disclose information for public good functions such as disclosures to insurance officials, in response to judicial orders, for fraud detection, etc.

The Act also limits certain disclosures that are made for marketing purposes. An insurance entity may disclose information to an affiliate for marketing purposes so long as the marketing is for an insurance product or service and the affiliate agrees not to disclose the information for any other purpose or to an unaffiliated purposes. Insurance entities may also disclose personal information, excluding medical record information and privileged information, to any person for marketing purposes but only if the individual has been given the opportunity to indicate that he or she does not want personal information disclosed for marketing purposes and the individual has given no indication that he or she does not want the information disclosed.

The 1982 Model Act does not permit insurance entities to disclose health information to another financial institution in order for that financial institution to make credit decisions regarding the individual that is the subject of the information without the individual's signed authorization.

### **State-Based Information or Event Specific Privacy Laws**

In addition to the comprehensive privacy laws discussed above, most states have enacted statutes that protect specific types of health information. Generally, these statutes regulate the uses and/or disclosures of "sensitive" information. The following are examples of the types of information where there is significant state regulation: domestic abuse; genetic information; mental health information; reproductive health; sexually transmitted diseases; and substance abuse treatment.

Condition specific laws further restrict the use and/or disclosures of protected health information. These laws limit insurance entities abilities to use the protected information. They also usually require an authorization or informed consent before the information may be disclosed.

I am not aware of any state-specific privacy law that allows an insurance entity to disclose health information to a third party for the other party to make credit decisions. Even if such a law existed it would likely be preempted as contrary to the HIPAA Privacy Rule.

As you can see from my comments, the health insurance industry has a long history of protecting the health and financial information in it possession. This history has its basis in law, industry practices and, most importantly, the needs of the customer.

June 16, 2003

Page 9

Thank you for the opportunity to appear before the Subcommittee. The Health Insurance Association of America looks forward to working with the Subcommittee on this important issue.