Testimony of the
National Association of Insurance Commissioners

Before the
National Committee on Vital and Health Statistics
Subcommittee on Privacy and Confidentiality

Regarding:
Privacy Protections for Medical Records
of Non-Covered Entities

September 14, 2006

Robert Alan Wake, Ph.D., J.D.
Attorney, Maine Bureau of Insurance
National Association of Insurance Commissioners

Testimony of Robert Alan Wake, Ph.D., J.D.
Attorney, Maine Bureau of Insurance
National Association of Insurance Commissioners

Introduction

Chairman Rothstein and Members of the Subcommittee, thank you for inviting me to testify this afternoon on privacy protections for medical records of non-covered entities.

My name is Bob Wake, and I serve as an attorney with the Maine Bureau of Insurance. I am testifying today on behalf of the National Association of Insurance Commissioners (NAIC), which is the national organization of the chief insurance regulators of the 50 States, the District of Columbia and four U.S. territories.

My testimony today will focus on: (1) the federal legal framework of insurance information privacy protections; (2) state insurance information privacy protections; and (3) the role of health information in non-health insurance underwriting and claims practices.

The Federal Legal Framework of Insurance Information Privacy Protections

The first comprehensive federal privacy initiative protecting insurance consumers is Title V of the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA). GLBA establishes a comprehensive regulatory framework for an integrated financial services marketplace that permits affiliations and competition among banks, securities firms and insurance companies. As it applies to the insurance industry, GLBA builds upon and expressly reaffirms the McCarran-Ferguson Act of 1945, which recognizes and codifies the States' general authority to regulate all aspects of the business of insurance.

GLBA replaces the former system of entity-based regulation with a functional regulatory approach. Formerly, federal and state laws had required each financial institution—

a term used in GLBA to encompass the full spectrum of the financial services industry, including insurance companies and insurance agencies—to specialize in one sector of the industry, under the oversight of a single regulator. Now, under functional regulation, financial institutions are authorized to do business or establish affiliates in more than one sector, with activities in each sector subject to the oversight of that sector's regulator. Federal and state laws preventing such affiliations are repealed or preempted. Continuing the allocation of responsibilities under the McCarran-Ferguson Act, GLBA designates state insurance commissioners as the functional regulators for the insurance industry.

Title V of GLBA establishes threshold standards for consumer privacy protection with which all financial institutions must comply. It places strict limitations upon the disclosure of nonpublic personal information to non-affiliated third parties, unless the consumer has been given the opportunity to withhold permission ("opt out") and has declined to do so. Title V further requires all financial institutions to send their customers written notices at least annually, describing the kinds of nonpublic personal information they collect, their policies governing disclosure of such information to third parties, the customer's right to opt out where applicable, and the measures they take to protect the information's confidentiality and security.

Each functional regulator is given the authority to conduct rulemaking to implement Title V. Specifically, each functional regulator is required to establish standards both for consumer privacy and information security, with the privacy standards to include more detailed provisions on permitted information disclosures, opt-out procedures, and the form and contents of the initial and annual notices of information policies and practices. As the designated functional regulators of insurance under GLBA, state insurance departments are the only state agencies subject to the requirement to issue these standards and given the authority to enforce Title V. Sections 501 and 505 specifically provide that "the applicable State insurance authority of the State in which a person is domiciled" shall adopt and enforce the information security regulations required by GLBA, and every state has enacted regulations or statutes to implement GLBA's privacy requirements. In addition, GLBA expressly required the federal functional regulators to

establish their privacy standards through coordinated rulemaking within six months after GLBA's effective date, and to consult with representatives of the NAIC in developing those rules.

For health insurers, additional federal privacy requirements are imposed pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of the United States Department of Health and Human Services (HHS) to publicize standards for the electronic exchange, privacy and security of health information. HIPAA required the Secretary to submit detailed recommendations on health information privacy standards to Congress within a year after its enactment and then to issue privacy regulations governing individually identifiable health information, unless Congress enacted health information privacy legislation within three years after the passage of HIPAA. Congress did not address health information privacy in GLBA Title V, nor did Congress enact stand-alone health privacy legislation. Therefore, HHS developed a proposed rule and submitted it for public comment. The final regulation, the Privacy Rule, was published December 28, 2000 and the final modifications were published August 14, 2002. Before the HIPAA regulations, the right to privacy of health information varied significantly depending on the law of the state in which one lived; now, health care providers, health plans and other health care services that operate anywhere in the United States must abide by the minimum standards set by HIPAA.

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. The Privacy Rule sets a national standard for privacy of health information, but only applies to medical information maintained by health plans, health care clearinghouses, and to health care providers who transmit health information in electronic form. Thus, its scope as applied to the insurance industry is limited to those insurers that are "health plans" within the meaning of HIPAA, meaning health maintenance organizations, health service corporations, and insurers providing medical

insurance, Medicare or Medicaid benefits, Medicare supplement (Medigap) insurance, or long-term care insurance.

State Insurance Information Privacy Protections

State Health Information Privacy Laws Before HIPAA, GLBA

Before HIPAA and GLBA, health information privacy measures varied widely from state to state, and each state's specific laws represented a unique blend of statutes, regulations and court interpretations that had evolved over time. A 1999 survey of state privacy and confidentiality statutes by Georgetown University's Health Privacy Project observed certain common characteristics of state health privacy protections. First, state statutes tended to safeguard health information by entity. Rather than comprehensively protecting medical records, state privacy laws address specific users and uses of health information, such as the use of information for underwriting by insurers or for hiring practices by employers. As a result, the confidentiality of health information depends largely on the individual or the entity that possesses the information. Second, few state privacy laws were intended to be comprehensive. Except in a handful of states that had passed comprehensive health privacy laws, state statutes frequently regulated information for certain entities and not others. Third, many state statutes presumed an ethical duty to maintain confidentiality. State laws often did not explicitly require certain entities that have access to health information to meet privacy standards, although they sometimes prescribed penalties for confidentiality breaches. The obligation of certain entities to maintain ethical duties—according to professional standards—sometimes had to be worked out in common law through the courts, but that form of protection is more open to interpretation and subject to uneven application. Finally, state lawmakers face significant challenges to keep up with the evolving nature of health care delivery and information technology.

NAIC Privacy Protection Model Legislation

State insurance officials, working through the NAIC, have been discussing and addressing the privacy of personal information for more than 20 years. In 1980, the NAIC adopted the *Insurance Information and Privacy Protection Model Act*, and amended the Act in 1982. This model applies to all insurance information and specifically addresses health information. It generally requires insurers to receive affirmative authorization from individuals ("opt-in") in order to disclose personal information. Although an exception to the opt-in requirement allows some personal information to be shared for marketing purposes on an opt-out basis, which makes the practical impact more similar to GLBA than may appear at first glance, that exception does not apply to health information. Health information may not be shared without the consumer's affirmative consent except for a limited range of essential purposes narrowly spelled out in the Act. When Maine enacted its version of the *Privacy Act*, the Maine Legislature added the further requirement that any disclosure of personal information be limited to the minimum necessary to accomplish a lawful purpose, a standard similar to one subsequently incorporated into HIPAA.

In September 1998, the NAIC continued its efforts to strengthen protections for consumers' personal information by adopting a new model solely focused on the issues specific to health information, the *Health Information Privacy Model Act.* Its adoption followed an extensive, four-year dialogue with all stakeholders, including representatives of the insurance and managed care industries, and representatives from the provider and consumer communities, building on experience with the 1980 privacy model and confidentiality provisions in other more specialized model laws such as the ones protecting subjects of domestic abuse. This model applies to all insurers and, similar to the 1980 privacy model, generally requires an entity to obtain an authorization ("opt-in") from the individual to collect, use or disclose individually identifiable health information.

With development of the 1998 Model, the NAIC reaffirmed and refined the principle that health information deserved a higher level of protection than other types of information

due to its sensitive, deeply personal nature and the damage that can result when it is used improperly. Work on the legislation that eventually became HIPAA began shortly after the NAIC began work on the *Health Information Privacy Model Act.* Although HIPAA was enacted midway through the NAIC process, Congress was unable to reach a consensus on specific privacy standards and referred the matter to HHS, as discussed earlier. A primary motivating factor in the NAIC's decision to continue work on the model act through final adoption was to provide a resource that could give guidance to Congress and HHS. The Privacy Rule is consistent with many of the NAIC's recommendations.

The NAIC GLBA Privacy Regulations

As discussed in the previous section, the states are required to adopt laws or regulations implementing Title V of GLBA. Accordingly, in September 2000, the NAIC adopted a model privacy regulation—*Privacy of Consumer Financial and Health Information Model Regulation*—to give guidance to the state insurance regulators in implementing the privacy requirements for insurers as directed by the GLBA. One of the NAIC's goals was to develop a regulation that could fit harmoniously with the regulations adopted by the federal functional regulators for their sectors of the industry. At the same time, insurance regulators recognized that the insurance industry poses unique privacy issues not found in other financial services because insurers often must collect and use health information. Fortunately, Section 507 of GLBA authorizes the states to enact laws that give consumers greater privacy protections than the provisions of GLBA, which were developed with financial information in mind. Therefore, in keeping with the philosophy used in our previous models and as authorized under GLBA, the members of the NAIC decided to provide more stringent protections for health information than for financial information, to avoid the risk of consumers' sensitive health information being shared freely without distinction from financial information.

In addition to financial information provisions substantially similar to those in the federal implementing regulations, the NAIC's model privacy regulation requires consumer

consent before any disclosure of protected health information ("opt-in"). Although consideration was given to exempting health insurers from the scope of the model because they would soon be subject to stronger protections under HIPAA, the NAIC decided to make the health provisions in this model applicable to health insurers as well as to lines not covered by HIPAA. This established minimum protections on an interim basis until the HHS privacy regulation became effective. It also maintained concurrent oversight and enforcement jurisdiction so that NAIC members could continue to do their part in protecting consumer privacy.

In April 2002, the NAIC adopted the *Standards for Safeguarding Customer Information Model Regulation*. This model establishes standards that insurance entities must meet to be in compliance with GLBA's information security provisions. Based on the guidelines established by the federal functional regulators, the model requires each insurance licensee to establish an information security program, which must provide protection for the nonpublic personal information of the licensee's current personal lines customers, and may include such optional provisions as identifying reasonably foreseeable internal or external threats, assessing their likelihood and potential damage, training staff, and exercising appropriate due diligence in selecting service providers.

Functionally Uniform Health Information Privacy Protections for Non-Health Insurers

As discussed, GLBA establishes a federal floor for consumer privacy protections while permitting the states to enact more laws and regulations that are more protective of consumer privacy. To date, all 50 states plus the District of Columbia and Puerto Rico have privacy protections in place that meet or exceed GLBA's requirements:

- 40 states, plus D.C. and Puerto Rico, have promulgated regulations based on the NAIC's *Privacy of Consumer Financial and Health Information Model Regulation*, which was adopted by the NAIC in response to GLBA.
- 17 states (including some of the states that have adopted versions of the *Model Regulation*) have laws based on the NAIC's *Insurance Information and Privacy Protection Model Act*, which was adopted by the NAIC in the early

1980s – long before Congress started thinking about consumer financial privacy. The consumer protections embodied in the model act differ in some ways from those mandated by GLBA, but are in many respects more protective of consumer privacy than the federal law.

- 33 states have laws based on the NAIC's *Standards for Safeguarding Customer Information Model Regulation*.

The NAIC and all 50 states continue to work towards developing increased insurance consumer privacy protections beyond the minimum required by federal law.

Health Information in Non-Health Insurance Underwriting and Claims Handling

Underwriting is Critical to the Efficient Operation of Insurance Markets

"Underwriting" is sometimes used as a legal term of art to mean "acting as an insurer." Within the insurance industry in America, however, it generally refers to the process of risk assessment, classification and selection of insureds so that an insurer can take on an appropriate portfolio of risks and determine appropriate premiums. The ultimate objective is to match each risk with an appropriate premium and terms of coverage. To the extent that an insurer's rating plan does not fully accommodate all variations in risk, the insurer must decline risk for which its products are unsuitable. Some risks may not meet basic requirements for insurability; *i.e.*, the probability of loss is too high or uncertain to charge an economically feasible premium and provide insurance. All else being equal, insurers with lower prices must have more stringent underwriting standards, while insurers with higher prices can afford to have less stringent standards.

Several principles guide proper underwriting: 1) selection according to standards, 2) proper balance within classifications, and 3) equity among policyholders. Standards are necessary to ensure the application of underwriting decisions to different risks by underwriters and agents consistent with an insurer's business plan. Some standards are fairly objective and clear; *e.g.*, declining applicants who have been convicted of fraud or

arson. Others may be more subjective and discretionary; *e.g.*, the apparent care that an applicant has taken in maintaining his or her home. For life and health insurance lines, medical history and current health status are key indicators of risk; so the collection and use of sensitive health information traditionally has been at the heart of these insurers' underwriting and rating practices, which raises important public policy issues.

The appropriateness and fairness of some underwriting guidelines and risk classifications have been a matter of public debate, and some practices are prohibited by law, either generally or in their application to particular insurance transactions. In those cases the principle of equity among policyholders is maintained by applying the standards uniformly for all affected policyholders and all insurers in the marketplace. In order to promote access to health care and the pooling of risk, state and federal laws have required guaranteed issuance and guaranteed renewal of medical insurance in many situations, and many states have placed limitations on insurers' ability to vary medical insurance premiums according to health risk.

Although these laws increase access to coverage for those who most need it, this comes at a cost. Insurers' desire to use all valid underwriting information at their disposal is aimed at avoiding "adverse selection." Adverse selection is the phenomenon that high-risk individuals are more likely to purchase insurance than low-risk individuals. This can happen when applicants have better knowledge of their risk than insurers. Adverse selection causes an excessive concentration of high-risk insureds within an insurer's portfolio. This in turn can burden an insurer's efficiency and financial performance, and even threaten its solvency unless prices are increased to match. Thus, an insurer—or a whole market segment—that writes an increasing concentration of high-risk insureds may no longer be competitively priced for low-risk insureds. In the worst case, this may result in a "death spiral" in which the price increases result in a further concentration of high-risk insureds, which in turn requires further premium increases, with no stable equilibrium ever reached.

There is a trade-off between affordable coverage and adverse selection. For medical insurance, there is a public policy consensus that some degree of adverse selection is the acceptable cost in order to make health care more affordable; although this is by no means unanimous and there is considerable disagreement even among those who support some restrictions on medical underwriting—such as guaranteed renewability—to what additional restrictions, if any, are appropriate. However, for non-health lines, the issues are very different, because the public policy consensus is that these lines of coverage are optional purchases rather than basic necessities. Therefore, the law generally recognizes medical underwriting as a legitimate underwriting tool and focuses on requiring insurers to collect and use medical information in a fair and responsible manner and to maintain it with due regard for its sensitivity.

Life Insurance Underwriting

Life insurance products provide financial security against the risk of premature death. Life insurers also write annuity products, which protect against the risk of an individual outliving his or her source of income. An important distinction between life insurance and other types of insurance is that the covered event (death) is uncertain in any given year, but certain in the long term. Key factors such as the age and health of the insured play a greater role in assessing, selecting and classifying individual risk for both life insurance and annuities. Therefore, life insurers commonly review applicants' medical records, inquire into personal and family medical histories, and require routine medical examinations and tests, and share information on applicants to reduce the risk of fraud. It should be noted that the *Model Privacy Act* includes provisions regulating the activities of "insurance support organizations" such as the Medical Information Bureau.

Although health insurers also use health information as part of the underwriting process, a few characteristics specific to life insurance make the acquisition and use of this information especially important. First, whereas one in 10 non-elderly individuals receive health coverage through the individual market, a majority of life insurance and annuity contracts are purchased individually. This means that a majority of life insurance

contracts are underwritten based on individual health information rather than underwritten based on the loss characteristics of the group. Second, many life insurance policies are perpetual and cannot be canceled so long as premiums are paid, and even term life insurance is typically sold on an "annually renewable" basis with coverage guaranteed at specified rates for ten years or even longer. Whereas health insurance policies typically provide coverage for a year term, life insurers get one bite at the underwriting apple. Once an applicant is accepted, a policy remains in effect and the premiums are not adjusted based on changing risk factors. Finally, unlike other types of insurance, life insurance is not a contract of indemnity, which involve an attempt to put the individual back in the same financial position as before the loss. Life insurance promises to pay a large cash payment upon the death of the policyholder, and there is no possibility of a partial loss.

Disability Income and Long-Term Care Insurance

Disability income insurance and long-term care (LTC) insurance illustrate the difficulty of drawing a meaningful bright-line distinction between "health insurance" and "non-health insurance." Although both of these lines of business are usually classified as health insurance for most purposes, an insurer's underwriting and rating considerations and the applicable regulatory framework for these lines of business are significantly different than they are for medical insurance. Although long-term care insurance is classified as a "health plan" within the meaning of HIPAA, disability income insurance is not.

Disability income insurance provides periodic payments when the insured is unable to work because of illness, disease or injury. The coverage is intended to replace a significant portion, but not all, of the income lost from the incapacity to work. The partial replacement reflects the expectation that workers' income needs are reduced when they are not working. It also guards against moral hazard and gives an incentive to incapacitated workers to return to work.

Most disability policies are group-based, but a significant minority is underwritten in the individual marketplace. Individuals purchase disability insurance both to protect against short-term disabilities, which may last up to one to five years, and long-term disabilities, which can last up to the age of retirement. Policies may either be noncancellable, meaning that the premiums and benefits will remain the same throughout the life of the policy, or guaranteed renewable, for which coverage is automatically renewed but the price can increase if the experience changes for the entire class of insured. In neither case can the insurer unilaterally terminate coverage.

Disability insurance underwriting relies to a great extent on medical information, but other factors, such as occupation, may be of equal or greater importance. Moreover, disabilities that inhibit an individual's ability to work also can be caused by non-medical factors, such as workplace injuries or result from an active lifestyle. Different medical information than that used for life insurance can prove significant in disability underwriting. For instance, a health condition such as a history of a lower back injury may have limited statistical implications for life insurance but can increase an applicant's risk significantly for the purpose of disability insurance.

LTC insurance is another form of coverage that is becoming increasingly important as the population ages and more individuals require extended medical or custodial care at home or in a more formal setting. One study has found that 40 percent to 45 percent of persons reaching age 65 will stay in a nursing home at least once during their lifetime. Nursing home care is expensive, and Medicare and Medicaid will cover the cost of this care for only a fraction of the individuals that will need it.

The LTC insurance market is evolving and insurers offer a variety of plans at different rates. Although LTC insurance is considered a type of health plan for purposes of HIPAA, most states allow this line of business to be written by life insurers. LTC insurance policies typically cover skilled nursing care, immediate nursing care, assisted living care, adult day care and home health care. However, policies differ in terms of aggregate benefits, elimination periods, eligibility for benefits and inflation protection. Insurers' financial solidity is an important consideration given the length of time that can elapse between when premiums are paid and benefits are received, and the difficulty this

can create in pricing the product accurately, especially with the services available and the understanding of patients' needs evolving as rapidly as the coverage is evolving. LTC insurance also can be expensive, with rates sometimes increasing significantly with the age of the insured when the policy is purchased. Because of these issues and need for consumer protection, LTC insurance is a significant area of state regulatory attention.

Medical underwriting is much more prevalent in the LTC insurance market than it is in other lines, primarily because most LTC insurance is sold on an individual basis. Even group LTC insurance plans include an element of individual underwriting. Unlike other lines, LTC insurance policyholders tend to be older and potentially more sensitive to conditions that may limit their independence. Cost also is a factor in medical underwriting for LTC insurance, with insurers potentially more on guard against known risks that could increase claims and raise premiums for the entire pool of insureds. The key to predicting risk is determining how someone's likely future medical condition will affect his or her independence. Medical records and physician statements contribute to the assessment of the individual's general health condition. Where insurers once relied on acute medical conditions alone, applicants now typically are assessed using standardized tests of their functional and cognitive abilities, asked about their ability to perform activities of daily living, and interviewed for additional medical information or required to take a paramedical exam. Insurers consider age and also determine whether a spouse or children are available to provide care if the applicant becomes dependent.

The Use of Health Information in the Claims Process

Finally, another important area in which insurers must use sensitive health information is in processing insurance claims. Medical information, often of a particularly sensitive kind, is integral to the claims process in both disability insurance and long-term care insurance since the claimant must prove that he or she is either unable to work or in need of long-term care. Furthermore, insurance claims involving medical information are not limited to life and health insurance. Medical evidence is also at the heart of claims for benefits under workers' compensation insurance, and for personal injury claims under a wide variety of liability coverages including automobile, medical malpractice, homeowners' and commercial liability. These pose a unique set of concerns because they

are third-party claims; that is, they are claims against the insured rather than claims by the insured. The claimant—the subject of the health information in question—is not a customer, a former customer, or a prospective customer. Although it is important to require insurers to respect the sensitivity and confidentiality of this information, and the *Model Privacy Regulation* treats third-party claimants as consumers for this limited purpose, it must also be kept in mind that the insurer's relationship to a third-party claimant is not contractual, or even voluntary, and the insurer's primary duty is to its own insured.

Conclusion

The NAIC believes protecting the privacy of insurance consumers is an area that demonstrates the real strength of state regulation—effective consumer protection that responds to local demands. The NAIC and many states developed and implemented insurance consumer privacy protections long before Congress and federal agencies addressed this issue in GLBA. Furthermore, the NAIC's efforts have extended beyond current federal requirements as state governments continue to actively address consumer privacy.

The NAIC also believes health information must be treated differently than financial information and more stringent protections for health information should be provided, especially in light of the example of GLBA, which in the absence of action by state regulators would have allowed insurance consumers' sensitive health information to be shared freely without distinction from other sorts of financial information. The goal of state insurance officials is to achieve effective privacy and confidentiality protections for all insurance consumers in each of our member states.

Thank you for this opportunity to address the Subcommittee, and I look forward to your questions.