INSURANCE
DEPARTMENT OF BANKING AND INSURANCE
DIVISION OF INSURANCE

Standards for Safeguarding Customer Information

Adopted New Rules: N.J.A.C. 11:1-44

Proposed: November 17, 2003 at 35 N.J.R. 5210(a)

Adopted: March 18, 2004 by Holly C. Bakke, Commissioner, Department of Banking and Insurance

Filed: March 18, 2004 as R. 2004 d. 148, with technical changes not requiring additional public notice and comment. (See N.J.A.C. 1:30-6.3.)

Authority: N.J.S.A. 17:1-8.1, 17:1-15e and 15 USC §§ 6801, 6805(b) and 6807

Effective Date: April 19, 2004

Expiration Date: January 31, 2006

Summary of Public Comments and Agency Responses:

The Department of Banking and Insurance (Department) timely received written comments from the following:

1. MIIX Advantage Insurance Company in New Jersey;
2. The Professional Insurance Agents of New Jersey;
3. State Farm Insurance Companies;
4. The Independent Insurance Agents of New Jersey;
5. Horizon Blue Cross and Blue Shield of New Jersey and its subsidiaries;
6. A joint comment from the Insurance Council of New Jersey and the American Insurance Association; and
7. Allstate New Jersey Insurance Company.

COMMENT: One commenter requested confirmation that the rules do not apply to insurers writing only commercial insurance. The commenter stated that N.J.A.C. 11:1-44.2 defines "licensee" to mean "all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to Title 17 and 17B in the New Jersey Statutes, …and any other person or entity subject to the statute governing information practices at N.J.S.A. 17:23A-1 et seq." The commenter stated that this statute generally applies to "insurance transactions," which is defined to mean insurance primarily for personal, family or household needs, rather than for business or professional needs. The commenter thus believed that the rules apply only to insurers writing personal lines and not commercial insurance.

RESPONSE: The rules by their terms apply to all insurers authorized or admitted pursuant to Titles 17 or 17B of the New Jersey Statutes regardless of the type of insurance written. However, the rules set forth minimum baseline standards for the implementation of a security program to provide for administrative, technical and physical safeguards for the protection of "customer information." "Customer information" is "nonpublic personal information" that is required not to be disclosed or which only may be disclosed under certain circumstances in accordance with the statute governing insurance information practices at N.J.S.A. 17:23A-1 et seq. As the commenter noted, this statute generally applies to insurance transactions that relate to personal lines rather than commercial lines insurance. Accordingly, to the extent that information is not "personal information" or "privileged information," the disclosure of which is limited by N.J.S.A. 17:23A-1 et seq., or otherwise not required to be kept confidential pursuant to law, these rules would not apply. The Department, however, believes that it would be prudent

for an insurer that writes solely commercial lines insurance nevertheless to develop a security program in the event that the insurer should seek to transact insurance or ascertain information subject to N.J.S.A. 17:23A-1 et seq. or otherwise required to be kept confidential pursuant to law.

COMMENT: Several commenters supported the reproposed rules and conforming the reproposed rules to the model rules adopted by the National Association of Insurance Commissioners (NAIC) that have been adopted in many other states.

RESPONSE: The Department appreciates the support of its proposal.

COMMENT: Several commenters expressed concern with N.J.A.C. 11:1-44.10, which provides that failure to comply with the provisions of the subchapter shall be deemed to constitute a violation of the statutes governing trade practices at N.J.S.A. 17:29B-1 et seq. and 17B:30-1 et seq., as applicable, and shall result in the imposition of penalties as provided in those statutes, N.J.S.A. 17:22A-1 et seq., 17:23A-1 et seq., 17:33-2, and any other provision or law. The commenters generally believed that the rules relate to customer information practices, which are the subject of N.J.S.A. 17:23A-1 et seq., and its violation and penalty provisions. Accordingly, the commenters believed that the only proper citations for violations would be N.J.S.A. 17:23A-17 and 18. The commenters believed that the other statutes have only a tangential relation to the protection of the privacy of customer information. One commenter stated that, while producers will have customer information in their files, the producer licensing law does not deal with the issue, and producers otherwise are covered under N.J.S.A. 17:23A-1 et seq. In addition, the

commenter stated that the general penalty provision is not needed because there are penalties in N.J.S.A. 17:23A-1 et seq. that otherwise apply. Another commenter stated that the general penalty provision governs filing fees by insurance companies and the imposition of penalties related thereto.

In addition, the commenters generally stated the Unfair Trade Practices Act deals with actual sales transactions, underwriting transactions and claims transactions between insurers and customers, does not deal with the details of insurer filing systems, and insurers are covered under the penalty provisions of N.J.S.A. 17:23A-1 et seq.

Accordingly, one commenter specifically suggested that N.J.A.C. 11:1-44.10 be amended to read as follows (additions in boldface; deletions in brackets): "Failure to comply with the provisions of this subchapter shall be deemed to constitute a violation of **N.J.S.A. 17:23A-1 et seq.** [The statutes governing trade practices at N.J.S.A. 17:29B-1 et seq. and 17B:30-1 et seq., as applicable], and shall result in the imposition of penalties provided in [those statutes, N.J.S.A. 17:22A-1 et seq.,] N.J.S.A. 17:23A-1 et seq. [,17:33-2, and any other provision of law]."

RESPONSE: Upon review, the Department has determined not to change this provision. This comment was raised when the rules were originally proposed and the Department reiterates its response thereto in this adoption. As noted in the reproposal, the reference to the statutes governing trade practices in the penalties provision is consistent with the national standard as reflected in the NAIC model, and has been adopted in several states, including New York and California. The Department also believes that the references to the various penalty provisions is appropriate insofar as a violation of New Jersey's requirements may result in the imposition of penalties. The references set forth in the rules are intended to provide guidance to licensed

entities as to the potential penalties for violations of the subchapter. The Department would use its discretion in imposing any penalties, but excluding a reference to a particular statute in these rules would not limit the Department from utilizing same if the Department believed actions by a licensed entity constituted a violation of an applicable statute. The Department also notes that the general penalties provision at N.J.S.A. 17:33-2 applies to any violations of subtitle 3 of Title 17, and does not only relate to filing fees.

The Department is making one technical change upon adoption. N.J.S.A. 17:22A-1 et seq. has been repealed and replaced with N.J.S.A. 17:22A-26 et seq. Accordingly, the cite to N.J.S.A. 17:22A-1 et seq. is changed upon adoption to N.J.S.A. 17:22A-26 et seq. as a matter of form.

COMMENT: One commenter expressed concern with N.J.A.C. 11:1-44.3, which provides that each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information, and that these safeguards shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities. The commenter stated that many of its members are small businesses with an average of 10 employees and use standard rating and customer database systems offered by vendors. The commenter stated that the number of available systems is limited and they do not have the ability to customize or enhance these programs. The commenter stated that its members do not have the ability to "ensure" that these systems are of such nature to ensure against internal and external threats or hazards to the security or integrity of customer information. The commenter requested that the Department

consider the standards available to agencies when implementing or monitoring compliance with the rules.

RESPONSE: Initially, the Department notes that N.J.A.C. 11:1-44.3 reflects the NAIC model and rules adopted in other states, including New York and California. The Department believes that the rule addresses the commenter's concern in that it provides that the safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities. The Department expresses no opinion as to whether the existing programs utilized by certain producers would be sufficient. Programs established should be appropriate to the size and complexity of the producer. However, the size of a particular licensee does not exempt that licensee from establishing an appropriate program to ensure the security and confidentiality of customer information, reflecting the national standard adopted by the NAIC to implement the requirements of the Gramm-Leach-Bliley Act (GLBA), Section 501(b). This statute requires each agency or authority to establish appropriate standards for the financial institution subject to their jurisdiction relating to administrative, technical and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. Accordingly, the Department believes that it would be appropriate for licensees to review existing contracts with vendors, and make modifications where necessary, in order to comply with these rules and GLBA.

COMMENT: One commenter expressed concern with the definition of "service provider" in N.J.A.C. 11:1-44.2. The commenter believed that the definition will create inconsistencies in interpretation among licensees, which may lead to disparate application of the rules; disparate enforcement; significant administrative and other problems for licensees in implementing and maintaining compliance with the rules; and significant additional burdens for licensees beyond what is required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) and GLBA.

The commenter stated that, related to a comment and response in the reproposal at 35 N.J.R. 5212, the Department is seeking to identify in its creation of the concept of "service provider" individuals or entities who are, under HIPAA, in a "business associate" relationship with a licensee. For example, the commenter stated that the Department, in its response to the comment, contemplated that a service provider is a person in a third party relationship with the licensee. Thus, it should not be possible for an employee of the licensee to be characterized as a "service provider." However, the commenter believed that the definition could be interpreted to include an employee as a service provider in that it might be argued that an employee provides a service to his or her employer. The commenter thus suggested that the definition in the reproposal expressly exclude employees of the licensee.

In addition, the commenter stated that the Department's emphasis on the language of providing services "directly to the licensee," as opposed to "healthcare providers who provide services to the members of a health plan" as noted in the Department's response to the comment in this reproposal, appears to draw the same type of distinction that the Federal rules draw between mere network providers and, for example, a provider who performs an independent medical examination or utilization review directly on behalf of a health plan. Under the HIPAA

privacy rules, the commenter stated that the former is not a business associate whereas the latter is a business associate. The commenter further stated that HIPAA defines a person as a "business associate" due to his or her performance of "functions" on behalf of a licensee. Accordingly, the commenter stated that, due to the ambiguous nature of the word "service" in this context, and to clarify and align the compliance for licensees between Federal and State rules, the Department should replace the phrase "service provider" with "business associate" and that it cross-reference the HIPAA definition or incorporate the HIPAA language as a replacement for the definition.

RESPONSE: Upon a review, the Department has determined that no change is required. Much of the comment appears misplaced. The commenter appears to be relying solely on HIPAA. These rules relate to compliance with GLBA, and constitute a separate and distinct compliance requirement from HIPAA. The term "service provider" and its definition are taken verbatim from the NAIC model, which has also been adopted in several states, including California and New York. The Department did not, as the commenter apparently suggested, determine whether a contract with an employee would or would not constitute a service provider agreement. The Department believes utilization of the definition is appropriate and will minimize confusion and disparate application since it reflects the NAIC model language and thus reflects the national standard adopted by several states.

COMMENT: Several commenters expressed concern with N.J.A.C. 11:1-44.8, which provides that a licensee exercise appropriate due diligence in selecting its service providers; and requires its service providers to implement appropriate measures designed to meet the objectives of this

subchapter, and, where indicated by the licensee's risk assessment, take appropriate steps to confirm that its service providers have satisfied these obligations. One commenter stated that insurers appear to have a requirement for a much more extensive information security program than an independent insurance agency. The commenter stated that the rules could be construed to require an insurance agency to implement the same systems as a major insurance company. The commenter requested that the Department clarify the rule to recognize that it would be impossible, and it was not the Department's intent to require agencies to sign contract addendums agreeing, or otherwise being required to implement the same level program as an insurer.

This commenter also expressed concern with the provision that provides a licensee shall "where indicated by the licensee's risk assessment, take appropriate steps to confirm that its service providers have satisfied these obligations." The commenter stated that its members represent several insurers, and that information maintained within systems in offices includes agency-owned data that would not be applicable to a specific company. The commenter requested that the Department clarify that, should an insurer consider an agency to be a "service provider," and seek confirmation of compliance from the agency, that confirmation of compliance can be provided by the agency submitting a notice of same to the insurer. The commenter did not believe that the intent of this rule is to permit a company to inspect the actual operational data of an agency, which would include information to which they should not be entitled under GLBA and other contractual arrangements.

Another commenter expressed concern in that the HIPAA rules outline the steps a covered entity must take if its business associate reports to a covered entity a violation of the rules. The commenter stated that the requirement that a covered entity monitor compliance with

its service provider was removed from the HIPAA rules. The commenter stated that these rules go beyond the HIPAA requirement and create an affirmative duty to review the privacy and security practices of any "service provider" identified. The commenter believed that this would be difficult and expensive to create and maintain. In addition, the commenter stated that since it was not part of the HIPAA privacy requirement, it has not yet been contracted for, and that licensees would now be forced to amend their already existing business associate contracts to contemplate this activity. The commenter thus requested that the requirement that licensees ensure compliance of their "service providers" be deleted from the rule.

This commenter stated that, alternatively, if this requirement is not deleted, the Department should provide an implementation period of at least one year rather than six months. The commenter stated that it would take significant time and effort to develop and forward contract addenda to, and then negotiate with, potentially thousands of service providers. In addition, the commenter stated that, beyond the contracting process, the requirement to ensure service provider compliance would take significant time, including time to perform the risk assessment contemplated by the current rule.

RESPONSE: Upon review of the commenters' concerns, the Department has determined not to change this provision. As noted in N.J.A.C. 11:1-44.5, the provisions in N.J.A.C. 11:1-44.8 provide an example of a method of implementation of the requirements recited in N.J.A.C. 11:1-44.3 and 44.4. The rules do not mandate that every licensee execute a contract requiring monitoring of service providers, nor do they specify the level of any monitoring should a licensee deem it appropriate to exercise such oversight. The rule merely recognizes that a licensee may deem it appropriate to oversee its service providers in this area insofar as the

licensee would be responsible for any violation of the subchapter. The determination of whether, and to what extent, any monitoring is to be undertaken by a licensee of its service provider, including an insurance producer if a licensee deems it appropriate, would be the subject of negotiation between the parties.

The Department also believes that reliance on references to HIPAA is misplaced in this context. As noted in a response to a previous comment, these rules implement Section 501(b) of GLBA, which is independent of HIPAA, and is based on the NAIC model, which has been adopted by numerous states, including California and New York.

In addition, the Department does not believe that any additional time for implementation of the subchapter beyond the six months already provided is necessary. As noted above, the rule does not mandate monitoring of service providers, or prescribe the degree of any such oversight. Rather, consistent with the NAIC model, the rule provides one example of a means of compliance with the subchapter. In addition, as noted previously, this subchapter is based on a model adopted by the NAIC in 2002. Various states have already adopted these requirements in 2002 and 2003. The Department originally proposed similar requirements in March of 2003. Accordingly, licensees have had ample notice of these provisions.

Federal Standards Statement

Federal standards or requirements are not specifically applicable to entities subject to GLBA that are regulated by the Department. As noted in the Summary of the reproposal at 35 N.J.R. 5210(a), various Federal agencies have promulgated rules governing the entities they regulate. The requirements in these adopted new rules are generally comparable to the requirements imposed under those Federal rules.

Full text of the adoption follows (additions to proposal indicated in boldface with asterisks ***thus**; deletions from proposal indicated in brackets with asterisks *[thus]*):

11:1-44.10 Violations

Failure to comply with the provisions of this subchapter shall be deemed to constitute a violation of the statutes governing trade practices at N.J.S.A. 17:29B-1 et seq. and 17B:30-1 et seq., as applicable, and shall result in the imposition of penalties as provided in those statutes, N.J.S.A. ***[**17:22A-1 et seq.**]* ***17:22A-26 et seq.***, 17:23A-1 et seq., 17:33-2, and any other provision of law.

11:1-44.11 Effective date

A licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this subchapter, by *[(six months from the effective date of this subchapter)]* ***October 19, 2004***:

jc04-01/inoregs