

Implementing the Obligations of the Gramm-Leach-Bliley Act – The NAIC Model for State Privacy Regulation

This memorandum provides an analysis of the provisions of the National Association of Insurance Commissioners (“NAIC”) Model Privacy Regulations. The first section provides a general overview of the privacy obligations imposed by the GLBA and embodied in the NAIC Model regulations. The second section provides a section-by-section analysis of the NAIC Model provisions.

I. OVERVIEW OF GLBA AND NAIC PRIVACY OBLIGATIONS

As you know, the GLBA eliminated the barriers that have long existed between the banking, securities and insurance industries and established a regulatory framework for each of these financial activities. Title V of the GLBA also created two new privacy-related requirements that the States, the federal banking regulators, the Federal Trade Commission (“FTC”) and the Securities and Exchange Commission (“SEC”) are required to implement and that all insurance agencies as well as many state affiliates will be required to satisfy.

These two new privacy obligations are the *notice requirement* and the *opt-out notification requirement*. These two requirements apply to “financial institutions” that have customers who are individuals.¹ A “financial institution” is defined as “any institution the business of which is engaging in financial activities” and “financial activities” are defined to include, among other things, insurance agency and brokerage activities. The NAIC Model is a set of proposed regulations designed to implement these requirements for insurance providers.

A. The Notice Requirement

The GLBA requires all financial institutions to provide an easily understandable notice of their privacy practices,² including their basic handling of “nonpublic personal information,” to their “customers.” This disclosure must be made when a “customer relationship” is established and on an at least annual basis thereafter. A “customer relationship” is defined to include any on-going relationship. The proposed federal regulations and the NAIC Model clarify that the sale of an insurance policy would establish such a relationship.

¹ The GLBA privacy requirements do not apply when the customer is a business.

² See GLBA Section 502(a); NAIC Model Sections 5 and 6; see also 16 C.F.R. § 313.5(a)(1) (2000).

It is important to note that the GLBA does not require a financial institution to have any *particular* privacy policy (except for the opt-out requirement discussed below). Instead, it requires “financial institutions” to disclose certain facts about their privacy policies – whatever those policies may be.

B. The Opt-Out Notification Requirement

In addition, before disclosing nonpublic personal information about any individual (or “consumer”) to a non-affiliated third party for a non-exempted purpose, the financial institution must notify the consumer that the information may be shared and that the consumer has a right to direct the financial institution to not disclose the information (known as a right to “opt-out” of the information sharing).

Under the “opt-out” requirement, a “financial institution” must inform its consumers that they have the right to prohibit it from sharing their nonpublic personal information with *unaffiliated* third parties. The right is qualified to the extent that it does not prohibit financial institutions from sharing the information for the purposes of completing the transaction for which the information was provided (or a related transaction), or for other specifically limited purposes, such as where permitted or required by law.²

There are two other major exceptions to this “opt-out” right. First, financial institutions are not required to let customers “opt-out” of information sharing between the financial institution and a third-party that is done under a joint marketing agreement. Second, the financial institutions are permitted to disclose customer information to unaffiliated third parties to market the institution's own products and services. The precise scope of these exceptions, the conditions under which they are available, and the form that the opt-out notification must take will be resolved by the pertinent state insurance and federal regulators.

The States have the primary authority to interpret and enforce the GLBA's new privacy requirements for all of those that are engaged in the business of insurance, while the federal banking agencies⁴ and the Securities and Exchange Commission have the authority to interpret and enforce these new requirements for any entities subject to their jurisdiction. The Federal Trade Commission (“FTC”) has the residual authority to interpret and enforce the requirements for any other entity subject to the GLBA privacy requirements. This means that if the States do not enact their own privacy regulations, insurance providers will be subject to the regulations imposed by the FTC.

³ The GLBA also permits disclosures which relate to the performance of any insurance function; protect certain delineated legal rights or obligations; provide information to insurance rating organizations, guaranty funds, or to the institution's attorneys, accountants or auditors; where necessary to comply with any legal obligation or to the extent explicitly permitted under other laws; or where necessary for completing a sale or merger of the institution.

⁴ These are the Office of the Comptroller of the Currency, the Federal Reserve, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision.

The FTC, the SEC, and the four federal banking regulators all finalized their GLBA privacy regulations this past summer. As a general matter, the obligations imposed by the various federal agencies' regulations are substantively identical to one another.

On September 12, 2000, the NAIC adopted a model set of state privacy regulations consistent with the requirements of the GLBA and federal regulations. Like the GLBA, the NAIC Model does not require a financial institution to have any particular policy but, instead, governs the disclosure of information regarding whatever privacy policy the institution has in place. Almost all of the NAIC Model provisions are substantively identical to the federal regulatory requirements.

The most important thing to understand about the NAIC Model is that it preserves an independent agent's flexibility to comply with the GLBA privacy requirements in one of three ways:

- (1) Adhere to the requirements of its own privacy policy;
- (2) Choose to be bound by and adhere to the requirements of a carrier's privacy policy; or
- (3) Adhere to a joint (carrier-agent) privacy policy.

There are only three significant differences between the NAIC Model regulations and the federal agencies' GLBA regulations:

- (1) The NAIC Model includes a special "opt-in" requirement for health information.⁵
- (2) The NAIC Model rules apply to insurance "licensees," while each federal agency's requirements apply to the financial institutions within its jurisdiction.⁶
- (3) The examples used to clarify which individuals are "customers" (and thus entitled to receive privacy *and* opt-out and opt-in notices) and which are "consumers" (and thus entitled to receive only opt-out and opt-in notices) are tailored to insurance under the NAIC Model.⁷

5 NAIC Model, Section 17. It is important to note that any personal health information that a financial institution maintains about its customers is treated as protected information under the federal regulations. The major change effected by the NAIC's special health information provisions is to require an "opt-in" rather than an "opt-out" before such information can be shared.

6 NAIC Model, Section 4Q.

7 NAIC Model, Sections 4F(2) and 4J(2).

II. THE NAIC MODEL – SECTION BY SECTION ANALYSIS

Article I: General Provisions. Article I of the NAIC Model consists of four standard introductory regulatory provisions: Section 1, Authority; Section 2, Purpose and Scope; Section 3, Rule of Construction; and Section 4, Definitions. Of these provisions, the two most important to highlight are the Model's Purpose and Scope, and certain Definitions.

Section 2: Purpose and Scope. The Purpose of the NAIC Model is to provide regulations governing the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees of a state's insurance department.⁸ What this means is that the NAIC Model provides a method for the states to implement the two new privacy obligations of the GLBA with respect to insurance providers conducting business within their borders. Consistent with the GLBA and federal regulations, the NAIC Model:

- (1) Requires a licensee to provide notice to individuals about its privacy policies and practices;
- (2) Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and
- (3) Provides methods for individuals to prevent a licensee from disclosing that information.

The NAIC Model covers in scope certain nonpublic personal financial information and all nonpublic personal health information. Specifically with respect to nonpublic personal financial information, the NAIC Model regulations govern the treatment of such information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. The regulations do not apply, however, to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes.

Section 4: Definitions. Section 4 contains the definitions of twenty-three key terms used in the NAIC Model regulations. Illustrative examples of many of the terms also are provided, which fosters a clearer, better understanding of the terms as they are applied. Several definitions of particular interest are discussed below.

"Clear and conspicuous." Subsection 4B defines a "clear and conspicuous" notice as

⁸ To give licensees some guidance for complying with Title V of the GLBA in those states that do not have laws or regulations that meet GLBA's privacy requirements, the NAIC Model provides that a licensee domiciled in the regulating state that is in compliance with the privacy provisions in a state that has not enacted laws or regulations that meet the requirements of Title V may nonetheless be deemed to be in compliance with Title V in such other state. See NAIC Model, Subsection 2C.

a notice that is reasonably understandable and designed to call attention to the nature and significance of the information in the notice. Examples of what it means for a notice to be “reasonably understandable” and “designed to call attention” are provided. By following these examples, a licensee is ensured that its notices will comply with the requirements of GLBA. Also included are examples of what constitutes a clear and conspicuous notice on a web page.

“Consumer.” Subsection 4F defines “consumer” as “an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has non-public personal information, or that individual’s representative.” The consumer definition triggers the opt-out and opt-in notification obligations of Articles II and V. All “consumers” must be provided with the requisite opt-out notification before their personal information can be shared with a third party for a non-exempted purpose.

“Customer.” Subsection 4I defines “customer” as a consumer who has a customer relationship with a licensee. The customer definition triggers who is entitled to receive initial and annual privacy notices. Customers are entitled to receive initial privacy notices at the point that a customer relationship is established and then on an annual basis thereafter.

It is important to understand that, while all customers are consumers, not all consumers are customers. A customer is a consumer who meets a higher threshold in that he or she has established an actual customer relationship with the insurance provider. Accordingly, a customer is entitled to something in addition to the opt-out notice that must be provided to all consumers before their information may be disclosed. That “something in addition” is the initial and annual privacy notice.

“Licensee.” Subsection 4Q defines “licensee” as “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 the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state’s Public Health Law].”

Significantly, the NAIC definition exempts agents, employees and representatives of other licensee’s from the privacy requirements only if “[t]he licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this regulation.”⁹ This preserves an agent’s ability to

⁹ NAIC Model, Sec. 4(Q)(2).

adhere to the requirements of its own privacy policy, the privacy policy of its principal or a joint privacy policy of the agent and principal.

“Nonaffiliated third party.” Consistent with the GLBA and federal privacy regulations, the NAIC Model specifically excludes from the definition of nonaffiliated third party a licensee’s affiliates and persons employed jointly by two financial organizations. Accordingly, a joint employee does not trigger the opt-out and other requirements when he or she receives personal information from a customer of either of the organizations for which he or she is acting.

“Nonpublic personal information.” The NAIC Model regulations separate nonpublic personal information into two categories, nonpublic personal financial information and nonpublic personal health information. Subsections 4T, 4U, and 4V provide examples of both.

Article II: Privacy and Opt-Out Notices for Financial Information. Article II contains six provisions implementing the GLBA’s two basic privacy obligations for nonpublic personal financial information. The NAIC Model regulations are substantively identical to the federal agencies’ privacy regulations governing the treatment of nonpublic personal financial information.

Section 5: Initial Privacy Notice to Consumers Required. The NAIC Model regulations governing the initial privacy notice requirement are fully consistent with the GLBA and federal regulations. Specifically, the NAIC Model requires that a licensee provide a clear and conspicuous notice disclosing its privacy policies and practices to “customers” upon establishing a customer relationship, and to “consumers,” but only before the licensee discloses any nonpublic personal financial information about the consumer to any nonaffiliated third party.¹⁰ This approach is consistent with the GLBA in that institutions are not required to give privacy notices anytime someone applies for insurance. Instead, notices are required when someone actually becomes a “customer” or, in the case of “consumers,” only prior to actual disclosure of information to a nonaffiliated third party.¹¹

Subsection 5C provides specific examples of when a customer relationship is established. Significantly, Subsection 5(C)(2)(a) provides that a licensee establishes a customer relationship when the consumer becomes a policyholder. Furthermore, the NAIC approach clarifies the meaning of “policyholder” by tying the initiation of the relationship directly to policy delivery.

¹⁰ NAIC Model, Sec. 5(A)(1), (2).

¹¹ See 16 C.F.R. § 313.3(n) (2000).

Section 6: Annual Privacy Notice to Customers Required. The NAIC Model regulations governing the annual privacy notice requirement also are fully consistent with the GLBA and federal regulations. In order to give insurance institutions and agents flexibility in complying with the annual disclosure requirement, Section 6 explicitly provides that “annually” means at least once in any period of twelve consecutive months during which the customer relationship exists. This is the definition that has been adopted under federal privacy regulations.

Subsection 6A sets forth the general rule and a clarifying example to ensure compliance. Subsection 6B also sets forth examples of when a customer relationship has been terminated (and thus annual notice is no longer required). This guidance is essential for life insurance and title insurance agents who do not have regular contact with customers.

Section 7: Information to be Included in Privacy Notices. Section 7A sets forth the General Rule for the information that must be included in a licensee’s initial, annual and revised privacy notices. The NAIC Model in this respect is identical to the federal regulations. The GLBA, the proposed federal regulations and the NAIC Model all require that these disclosures specifically include the following:

- (1) The categories of nonpublic personal financial information that the licensee collects;¹²
- (2) The categories of nonpublic personal information that the licensee discloses;¹³
- (3) The categories of affiliates and nonaffiliated third parties to whom the financial institution discloses nonpublic personal information;¹⁴
- (4) The categories of nonpublic personal information about former customers that the licensee discloses and a list of affiliates and nonaffiliated parties to which such nonpublic personal information is disclosed;¹⁵
- (5) With regard to disclosures to nonaffiliates, a statement of the categories of information that are disclosed to non-affiliated third parties and the cate-

¹² NAIC Model, Section 7A(1); GLBA Section 503(b)(1)(B)(2); see also 16 C.F.R. § 313.6(a)(1) (2000). As a general matter, all of the disclosure requirements are limited to requiring only the listing of categories and classes of information.

¹³ NAIC Model, Section 7A(2); see also 16 C.F.R. § 313.6(a)(2) (2000). A financial institution also can include a list of categories of nonpublic personal information that it reserves the right to disclose in the future, but does not currently disclose.

¹⁴ NAIC Model, Section 7A(3); GLBA Section 503(b)(1)(A); see also 16 C.F.R. § 313.6(a)(3) (2000).

¹⁵ NAIC Model, Section 7A(4); GLBA Section 503(b)(1)(B); see also 16 C.F.R. § 313.6(a)(4) (2000).

gories of third parties with which the financial institution has a contractual relationship;¹⁶

- (6) If the financial institution discloses nonpublic personal information to non-affiliated third parties for a non-exempt purpose, an explanation of the consumer's right to opt-out of such disclosures and the methods by which the consumer may exercise the right;¹⁷
- (7) Any disclosures the financial institution is required to make under the Fair Credit Reporting Act,¹⁸ and
- (8) The financial institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.¹⁹

Subsection 7B provides that, if a licensee discloses nonpublic personal financial information under an exception discussed in either Sections 15 or 16 (e.g., disclosures made for processing and servicing transactions), the licensee is not required to list the recipients of that information in its initial or annual privacy notices. Instead, when the licensee is describing the categories of parties to whom disclosure is made (as otherwise required by Subsection 7A), the licensee is required only to state that it makes disclosures to other affiliated or nonaffiliated third parties "as permitted by law."²⁰

Subsection 7C provides a straightforward but comprehensive list of examples of the information that would satisfy the information disclosure requirements listed in Subsection 7A of the NAIC Model (and Section I(A) of this Memorandum). The NAIC Model thus provides a significant benefit to licensees by describing in easily understood language exactly how to comply with the GLBA's privacy notice obligation. Subsection 7D provides an optional short form initial notice (with opt-out notice) for consumers who are not customers. Appendix A to the NAIC Model also provides a list of sample clauses illustrating some of the notice content required by Section 7.

Section 8: Form of Opt-Out Notice to Consumers and Opt-Out Methods. Section 8 provides that, if a licensee is required to provide an opt-out notice, it shall provide a clear and

16 NAIC Model, Section 7A(5); see also 16 C.F.R. § 313.6(a)(5) (2000). If disclosures are made to non-affiliated third parties for a purpose that exempts the disclosure from the opt-out obligations, that should be noted here.

17 NAIC Model, Section 7A(6); see also 16 C.F.R. § 313.6(a)(6) (2000). The opt-out notification obligation is discussed in more detail below.

18 NAIC Model, Section 7A(7); GLBA Section 503(b)(4); see also 16 C.F.R. § 313.6(a)(7) (2000).

19 This requirement is satisfied by describing in general terms who is authorized to have access to the information and stating whether security practices and procedures are in place to ensure the confidentiality of the information in accordance with the financial institution's policy. Technical information regarding the safeguards in place is not necessary. NAIC Model, Section 7A(8); see also 16 C.F.R. § 313.6(a)(8) (2000).

20 NAIC Model, Section 7B; see also 16 C.F.R. § 313.6(b) (2000).

conspicuous notice to each of its customers explaining the right to opt-out and providing a reasonable means by which the consumer can exercise the opt-out right. Again, the NAIC Model includes illustrative examples of adequate notices and reasonable and unreasonable opt-out means.

Section 9: Revised Privacy Notices. Section 9 governs the issuance of revised privacy and opt-out notices, which are required before a licensee discloses a new category of information or makes a disclosure to a new category of nonaffiliated third parties that was not adequately described in the initial privacy notice.

Section 10: Delivery. Section 10 explains how to provide notices and be reasonably assured that a consumer will receive them. Examples of reasonable methods are hand-delivering the notice, mailing a printed copy of the notice to the last known address of the consumer (which can be done separately or in a policy, billing or other written communication), and posting a notice on a website and requiring the consumer to acknowledge receipt. Section 10 also governs issuance of annual notices.

Subsections 10F and 10G specifically address joint notices and joint consumer relationships. These provisions preserve an agent's flexibility in providing privacy notices. The NAIC Model recognizes that agents are often responsible for delivering policies to insureds and thus expressly enables agents to give separate notices on behalf of insurers, if the insurer so directs. Thus, Subsection 10F permits a licensee to provide a joint notice with another financial institution or *on behalf of* another institution. Subsection 10G provides that if two or more consumers jointly obtain an insurance product or service, the licensee may satisfy the initial, annual and revised notice requirements by providing one notice to those consumers jointly.

Article III: Limits on Disclosures of Financial Information. Article III contains three sections on the limitation on the disclosure of nonpublic personal financial information to nonaffiliated third parties. These limitations also are substantively identical to the federal GLBA privacy regulations.

Section 11: Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties. Section 11 contains the general rule governing disclosure of nonpublic personal financial information. Except as authorized by a specific exemption, a licensee may not disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless: (1) the licensee has provided an initial privacy notice; (2) the licensee has provided the requisite opt-out notice; (3) the licensee has given the consumer a reasonable opportunity to respond; and (4) the consumer does not opt-out. Examples of "a reasonable opportunity to opt-out" are provided, and a "partial opt-out" (where the consumer selects certain information or certain nonaffiliated third parties with

respect to which he or she wants to exercise the opt-out right) also is addressed.

Section 12: Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information. Section 12 contains limitations on the redisclosure and reuse of nonpublic personal financial information, which essentially dictate that an entity that receives protected information cannot redisclose or reuse that information except as permitted under the Section. These limitations are separated into four categories, (1) information the licensee received under an express exception; (2) information a licensee receives outside of an express exception; (3) information a licensee discloses under an express exception; and (4) information a licensee discloses outside of an express exemption. With respect to the reuse or redisclosure of financial information, the general rule of thumb for all four categories is that non-affiliated third parties may redisclose information only to affiliates (their own or the affiliates of the institution that the disclosed the information to them), or to non-affiliates under an express exception and only to carry out the purpose for which the information was originally disclosed.

Section 13: Limits on Sharing Account Number Information for Marketing Purposes. This section imposes limitations on the sharing of account number information. Section 13 deviates from the federal regulations. Rather than focus on the disclosure of an “account number,” the NAIC Model focuses on the key piece of insurance information – policy information. Thus, Section 13 provides that a licensee shall not disclose a customer’s “policy number or similar form of access number or access code for a consumer’s policy or transaction account” to any nonaffiliated third party for marketing purposes. This preserves the ability of agents to perform many of the services in which they normally engage on behalf of carriers, without running afoul of the regulation.

Furthermore, Section 13 contains an exception permitting disclosures “[t]o a licensee who is a producer solely in order to perform marketing for the licensee’s own products or services.” This exception reflects the unique relationship between carriers and producers and their unique need for a heightened ability to share customer information to service their mutual customers.

Article IV: Exceptions to Limits on Disclosures of Financial Information. Article IV sets forth certain exceptions to Article III’s limitations on the disclosure of financial information.

Section 14: Exception to Opt-Out Requirements for Disclosure of Nonpublic Personal Financial Information for Service Providers and Joint Marketing. Section 14 sets forth a key exception to the opt-out requirement for service providers and joint marketing. Consistent with the GLBA and the federal regulations, the NAIC Model rule is that the opt-out requirements do not apply when a licensee provides nonpublic personal financial information to a

nonaffiliated third party who perform services for the licensee or who functions on behalf of the licensee. Section 14 contains a provision incorporating language directly from the GLBA, which states that such services may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and another financial institution.²¹

Section 15: Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions. Section 15 incorporates exceptions to the privacy opt-out requirements for processing and servicing transactions. Specifically, Section 8 and 11's opt-out requirements do not apply if a licensee discloses nonpublic personal financial information necessary to effect, administer or enforce a transaction that a consumer authorizes, or that takes place in connection with certain processing and servicing functions:

- (1) Servicing or processing an insurance product or service that a consumer requests or authorizes;
- (2) Maintaining or servicing the consumer's account with a licensee or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;
- (3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or
- (4) Reinsurance or stop loss or excess loss insurance.

"Necessary to effect, administer or enforce a transaction" is defined to include, among other things, disclosures necessary to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part,²² and necessary to underwrite insurance for any of the following purposes as they relate to a consumer's insurance:

account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law.²³

21 NAIC Model, Section 14B

22 NAIC Model, Section 15(B)(2)(b).

23 NAIC Model, Section 15(B)(2)(E).

These examples, like the other exceptions in Section 15, are consistent with the GLBA and federal regulations.

Section 16: Other Exceptions to Notice and Opt-Out Requirements. Section 16 incorporates other exceptions to the privacy notice and opt-out requirements set forth under the GLBA and the federal regulations. Significantly, Section 16 includes an express exception permitting the disclosure of nonpublic personal financial information “[f]or purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers’ compensation plan.”²⁴

Article V: Rules for Health Information. Sections 18, 19, 21 and 22 address the special opt-in rules that apply to the sharing of health information.

Section 17: When Authorization Required for Disclosure of Nonpublic Personal Health Information. Section 17A sets forth the basic opt-in requirement, that a licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

Subsection 17B contains the limits of this requirement by setting forth an extensive list of insurance functions (performed by or on behalf of the licensee) that do not trigger the opt-in requirement. The excepted insurance functions include: claims administration; claims adjustment and management; fraud investigation; underwriting; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; and activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit.

Also excepted are any activities permitting disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; and any activities otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process.

²⁴ NAIC Model, Section 16(A)(8).

Section 18: Authorizations. Section 18 identifies the requirements of a valid authorization (or exercise of the opt-in) to disclose nonpublic personal health information. Specifically, an authorization must be in written or electronic form and must contain:

- (1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;
- (2) A general description of the types of nonpublic personal health information to be disclosed;
- (3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;
- (4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and
- (5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

Section 19: Authorization Request Delivery. Section 19 addresses the appropriate delivery of an opt-in notice. The provision permits an authorization request and form to be delivered as part of an opt-out notice, provided that the authorization and form are clear and conspicuous. But Section 19 also makes clear that an authorization form is not required to be delivered or included in any other notices unless the licensee intends to disclose protected health information.

Sections 20 and 21: Relationship to Federal Rules and State Laws. Section 20 describes the relationship between Article V and Federal Rules. In essence, if a licensee complies with all of the requirements of the federal Health Insurance Portability and Accountability privacy rule (as promulgated by the U.S. Department of Health and Human Services), regardless of whether a licensee is actually subject to that rule, then the licensee is not subject to the health privacy requirements of Article V.

Finally, Section 21 makes clear that nothing in Article V shall preempt or supercede existing state law related to medical records, health or insurance information privacy.

Article VI: Additional Provisions. The final five sections of the NAIC Model regulations set forth standard provisions for nondiscrimination, violations, severability and effective date of the regulations. Consistent with the GLBA, Section 22 expressly provides that nothing in the regulations shall be construed to modify, limit or supercede the operation of the federal Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.²⁵

²⁵ NAIC Model, Sections 22-26.