BCLP. Client Intelligent

Insights

KEY CONCEPTS IN PRIVACY LAW FOR INSURANCE COMPANIES: PART 1 – GLBA

PRIVACY SPEAKS SERIES

Oct 28, 2024

This article is the first in a series that will address privacy concerns for insurance companies, agents and brokers. The insurance industry is uniquely situated at the confluence of multiple data privacy regimes.

The Gramm-Leach-Bliley Act of 1999 ("GLBA")[1] was enacted to remove established restrictions on affiliations among financial institutions, including banks, securities firms, and insurance companies.[2]This liberalization sought to make financial firms, and markets, more efficient, but it also meant that data would be shared between entities and affiliates in ways that had not been previously contemplated. This data included "non-public personal information" or NPI, which GLBA defined as "personally identifiable financial information— (i)provided by a consumer to a financial institution; (ii)resulting from any transaction with the consumer or any service performed for the consumer; or (iii)otherwise obtained by the financial institution."[3]GLBA imposes numerous general restrictions on the use and disclosure of NPI by financial institutions.

INSURANCE COMPANIES AS FINANCIAL INSTITUTIONS

GLBA is broadly applicable to "financial institutions," which are defined not directly but by reference to a set of activities listed in a separate banking statute. Specifically, GLBA applies to "financial institutions" that are "significantly engaged" in any of the activities listed in section 4(k) of the Bank Holding Company Act.[4]And section 4(k) includes the following concerning insurance activities: "insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State."[5] Thus, GLBA is facially applicable to carriers, producers, and captive/managing agents.

Financial institutions are required to protect the privacy and confidentiality of their customers.[6]The statute sets forth notice requirements,[7]and restrictions on certain types of data use, including most

notably the transmission of NPI to nonaffiliated third parties unless the consumer has been provided with an opportunity to opt-out of the transfer.[8]Finally, GLBA confers rulemaking authority on a number of agencies depending on their jurisdictions,[9]but there is an important reservation of rights with respect to State insurance regulators.[10]The net result is that while GLBA has a federal statutory basis for its application to insurance companies, rulemaking authority is vested in state insurance regulators.[11]

SCOPE, CUSTOMERS AND CONSUMERS

GLBA applies to the NPI of customers and consumers. A consumer is 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* . . . ."[12]Consumers can include individuals like life insurance beneficiaries, claimants, annuitants, or mortgagors.[13]Consumers also include applicants.[14]

Customers are those individuals meeting the definition above, **and** that have an active and ongoing relationship with the insurance company in question.[15] Thus, all customers are consumers, but not all consumers are customers.

STATE INSURANCE REGULATIONS

The delegation to the States of rulemaking authority for application of GLBA to insurance companies has resulted in inconsistent and uneven application of the core principles of GLBA by the States. GLBA is over twenty years old, and has been the subject of multiple statutory updates over the years. These updates have been consolidated and accounted for by regulation at the federal level,[16]but the States have been less assiduous in updating their regulations. The result is that the current landscape of GLBA regulations applicable to insurance companies is uneven at best.[17]

As such, the following overall summary of requirements is based on the NAIC model regulations. The practitioner should note that there is considerable variability among the states, and certain key compliance features may be omitted entirely depending on the age of the state regulations (for example, the Safe Harbor for the federal "gray box" notice form in the most recent model law). The state law chart provided in footnote 17 also contains citations to the applicable laws.

NOTICE

The core requirements of notice to consumers (and customers) have not changed for some time. The contents of the notice must generally include the following:

- Categories of NPI collected;

- Categories of NPI disclosed;
- Categories of affiliates and third parties who receive NPI from the insurance institution (including that of former customers);
- Descriptions of any disclosures made under Section 15 (discussed below) not accounted for by another exception;
- An explanation of the consumer's rights, including the right to opt-out from non-affiliate marketing disclosures;
- Any disclosures made under the FCRA, including the right to opt-out from affiliate sharing in some instances;
- A description of the company's policies regarding confidentiality and security of NPI; and
- A catchall statement that the company makes other disclosures as permitted by law.[18]

Depending on how the company interacts with the consumer, the notice may take multiple forms, including printed and electronic.[19]But in every case, the initial notice must be *delivered* to the consumer. It is usually not enough, for the initial notice, to simply post it on a webpage or elsewhere.[20]

At the federal level, customers typically receive this notice in the form of a "gray box" notice. Perhaps recognizing the considerable consumer familiarity with this form, the 2017 NAIC model rule adopts the federal form as a permissible notice template and provides instructions for completing the form.[21]

Notices provided must be retained by the insurance company so that the consumer can obtain them or request them in writing at a later date. This requirement can be met by making the notice available on the company's website.[22]If a company wishes to undertake a use or disclosure that is not accounted for in its current initial (or annual notice), the company must "re-notice" the consumer in question. The consumer must be given a reasonable opportunity to opt-out.[23] A reasonable opportunity to opt-out, for this issue and for marketing opt-outs addressed below, is generally 30 days from the date of the mailing/transmission of the notice, except in one-time transactions.[24]

CONSUMER OPT-OUTS APPLICABLE TO INSURANCE COMPANIES

A customer or consumer's opt-out right applies broadly to any disclosure of that consumer's NPI to a non-affiliate, other than as permitted by Sections 15, 16, and 17 of the Model Law.[25]The prototypical example of such a disclosure is, of course, a disclosure to a non-affiliate for marketing

purposes. Because the right is structured as an opt-out, rather than an opt-in, the company's ability to disclose data to non-affiliates is dependent on notice to the consumer and a reasonable opportunity to opt-out (as noted above, "reasonable opportunity" generally means 30 days).

This is **not**, however, the only opt-out that is typically addressed in the "gray box" privacy notice. The company also must make a disclosure concerning affiliate sharing and there is at least one scenario in which an opt-out must be offered for the sharing of NPI among affiliates.[26]Specifically, as is made clear by the instructions provided in the Model Rule, the sharing of creditworthiness data subject to the FCRA among affiliates for marketing purposes may also be limited by the consumer—this rule is commonly referred to as the Affiliate Marketing Rule.[27]This opt-out right applies only to "information that would be a consumer report, but for clauses (i), Iii), and (iii) of section 1681a(d)(2)(A) of [the FCRA]."[28]

OTHER EXCEPTIONS TO THE OPT-OUT RIGHT

Consumers and customers are **not** entitled to opt-out from all disclosures to third parties. The experienced data privacy practitioner will note that many of these exceptions are consonant with customary exceptions in generally applicable data privacy laws, to wit:

- Section 15 (performance of services for company, direct marketing, and joint marketing): This exception allows the company to transmit data to third parties for *its own* marketing purposes, to perform the services requested by the consumer, or to engage in certain joint marketing relationships.[29]Reliance on this exception is dependent on having provided an initial notice describing the disclosures in question.[30] In addition, the insurance company must have entered into an agreement with the recipient that restricts usage of the NPI to that necessary to carry out the services.

- Section 16 (processing and servicing transactions): This exception allows transmission of data "to effect, administer, or enforce a transaction that a consumer requests or authorizes" related to (a) servicing an insurance product, (b) maintaining an account with another insurance company, or another entity offering credit, (c) securitization or secondary market sales, or (d) reinsurance.[31]The Rule goes on to list specific examples of transactions or transaction types. These disclosures can be made even if an initial notice has not been provided.

- Section 17 (catchall): This final exception is a sort of catchall for other disclosures, which includes, disclosures made with the consent of the consumer,[32]to protect the security of records,[33]to combat fraud,[34]for institutional risk control or resolving customer disputes,[35]to legal or beneficial interest holders,[36]or to fiduciaries.[37]There are also additional typical

exemptions for compliance with law, mergers and acquisitions, etc. These disclosures also may be made even absent an initial notice.

SPECIAL DATA CONSIDERATIONS

Certain special data types bear brief mention. While the GLBA does not have a concept of sensitive data, the transmission of health data is subject to heightened restrictions. Health data cannot be disclosed without an authorization from the consumer, subject to certain exceptions.[38]The authorization must contain specific content and be signed by the consumer.[39] And in fact the requirement looks very similar to the authorization requirement under HIPAA.

Finally, there is a general prohibition on the disclosure of account numbers and policy numbers, except to service providers, brokers/producers, or certain affinity programs that are previously disclosed to the consumer.[40]

REFERENCES

[1] 15 U.S.C. §§ 6801-6809, 6821-27.

[2] *American Bankers Assoc. v. Gould*, 412 F.3d 1081 (9thCir. 2005).

[3] 15 U.S.C. 6809(4)(A).

[4] 15 U.S.C. 6809 (citing 12 U.S.C. 1843(k)).

[5] 12 U.S.C. 1843(k)(4)(B).

[6] 15 U.S.C. 6801(a).

[7] *See generally* 15 U.S.C. 6803.

[8] 15 U.S.C. 6802(b).

[9] 15 U.S.C. 6804(a)

[10] 15 U.S.C. 6804(a)(1)(d) (“Nothing in this paragraph shall be construed to alter, affect, or otherwise limit the authority of a State insurance authority to adopt regulations to carry out this subchapter.”); *see also id.* at (2) (requiring consultation and coordination with “representatives of State insurance authorities designated by the National Association of Insurance Commissioners, for the purpose of assuring, to the extent possible, that the regulations prescribed by each such agency are consistent and comparable with the regulations prescribed by the other such agencies”).

[11] *See, e.g.,* FDIC Compliance Manual (available at: VIII. Privacy —GLBA (fdic.gov)), fn. 9.

[12] Model Rule at Section 4(F)(1) (emphasis added).

[13] *Id.* at 2(d).

[14] *Id.* at (b).

[15] Model Rule at Section 4(I-J).

[16] FDIC Compliance Manual at 1-3 (setting out a history of amendments and regulatory consolidation).

[17] The NAIC periodically publishes a chart of the current status of state regulations in this area.

[18] NAIC, Model Rule, Section 7A-B.

[19] *Id.* at section 11.

[20] *Id.* at 11.B(1)-(2). It may be possible to post annual notices in some cases, however, where the company has a reasonable expectation that the consumer will use the company's website. *Id.* at 11.B(3).

[21] *Id.* at appendix B.

[22] *Id.* at 11.E.

[23] *Id.* at section 9.

[24] *Id.* at section 12(3).

[25] *Id.* at section 12(A)(2).

[26] Certain state laws further restrict sharing in affiliate and non-affiliate contexts, and will be the subject of a later article.

[27] 15 U.S.C. 1681s-3(a) (use restriction); 15 U.S.C. 1681a(d)(2)(A)(iii) (sharing restriction); *see also* 16 C.F.R. 680. In fact, while the Model Rule refences section 624 of the FCRA (i.e., 15 U.S.C. 1681s-3), the actual sharing restriction is found in section 603 (i.e., 15 U.S.C. 1681a). As a practical matter, both opt-out rights can be consolidated and presented in the affiliate sharing box of the "gray box" notice, but the net effect of an opt-out is to restrict both use and sharing for marketing purposes. That is, the opt-out *also means that the entity receiving the opt-out cannot use FCRA data for marketing purposes under most circumstances, at least when that data has been received from another affiliate.*

[28] 15 U.S.C. 1681s-3(a).

[29] Model Rule at Section 15. “Joint marketing” means offering the company’s own services together with another financial institution pursuant to a “joint agreement,” which is “a written contract pursuant to which one or more financial institutions jointly offer, endorse, or sponsor a financial product or service.” *Id.* at 15(C).

[30] *Id.* at 15(A)(1).

[31] Model Rule at Section 16.

[32] *Id.* at 17(A)(1).

[33] *Id.* at 17(A)(2)(a).

[34] *Id.* at (b).

[35] *Id.* at (c).

[36] *Id.* at (d).

[37] *Id.* at (e).

[38] Model Rule at Section 18.

[39] Model Rule at Section 19.

[40] *See generally* Model Rule at Section 14.

RELATED CAPABILITIES

- Data Privacy & Security
- Insurance & Reinsurance
- Insurance Regulatory

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144
