Health Law
ADVISORY BULLETIN

CONTENTS

THE OTHER PRIVACY LAW: PREPARING FOR THE GRAMM-LEACH-BLILEY ACT

BY REECE HIRSCH

While the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has grabbed more headlines and industry attention, for many health plans and insurers, the most urgent privacy and security legal compliance issues in the coming months will involve the Gramm-Leach-Bliley Act ("Gramm-Leach"). This new law will require health plans and insurers to take a variety of actions with respect to the handling of member and subscriber data, in electronic and other formats, that parallel certain aspects of their HIPAA compliance efforts. The reason that Gramm-Leach is a front-burner issue for health plans and insurers is that compliance with Gramm-Leach will be required in most states by July 1, 2001.

The Gramm-Leach-Bliley Act was enacted on November 12, 1999 to remove certain restrictions on mergers, affiliations and other business activities of banks that date to the Depression era. Concerns about the sharing of personal financial information among merged banks nearly scuttled the legislation, and resulted in the addition of new privacy provisions that apply to a wide range of entities in the financial services industry, including essentially all insurers and health plans.

The privacy provisions of Title V of Gramm-Leach apply only to non-public personal information about individuals who obtain financial products or services for personal, family or household purposes, and not to companies or individuals obtaining products or services for business purposes. "Non-public personal information" generally includes any personally identifiable financial information provided by a customer or consumer to a financial institution to obtain a financial product or service.

Gramm-Leach generally provides that financial institutions may share virtually any information with "affiliated" companies, and can share information with "nonaffiliated" companies only following notice of a company's information sharing practices to the affected customers and providing an opportunity for those customers to "opt-out" of certain types of disclosures.

Gramm-Leach became effective November 13, 2000, but financial institutions have until July 1, 2001 to be in "full compliance." Seven different federal agencies have responsibility for enforcing Gramm-Leach: the Federal Trade Commission ("FTC"), the Department of the Treasury, the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration and the Securities and Exchange Commission. Each of these agencies has issued, either individually or jointly, final regulations implementing Gramm-Leach. The rules that govern insurers and health plans, will, however, be found in the new state laws and regulations that are being enacted to implement Gramm-Leach, as provided in 15 U.S.C. Section 6805. As the FTC's final rule states, Gramm-Leach "explicitly commits the enforcement jurisdiction of 'persons engaged in providing insurance' to state insurance authorities, thus excluding them from the Commission's authority."

Almost every state has enacted, or is in the process of enacting, Gramm-Leach implementation legislation or regulations. Many of these state measures are based upon the National Association of Insurance Commissioner's Model "Privacy of Consumer Financial and Health Information Regulation" (the "NAIC Model Regulation"). As of this writing, all state implementing laws or regulations have retained the July 1, 2001 compliance date of the federal rules. Penalties for noncompliance with Gramm-Leach by insurers and health plans will be established under the state implementing laws and regulations.

CONTINUED ON NEXT PAGE

Davis Wright Tremaine LLP

Davis Wright Tremaine is monitoring the progress of the Gramm-Leach implementation efforts in each of the states. Although no state currently requires compliance prior to July 1, 2001, several states have imposed certain notice requirements that apply to HMOs and insurers prior to July 1. For example, the Arkansas Insurance Department requires insurers and HMOs to inform their adjusters, appointed agents and members of the Gramm-Leach compliance date and provide them with a copy of Arkansas' proposed implementing regulation. In a circular letter dated February 20, 2000, the New York Insurance Department required insurers and HMOs to provide a written report to the Department by May 1, 2001, outlining policies, procedures and controls that are in place as of April 15, 2001 or planned, to comply with the New York Gramm-Leach implementing regulation regarding financial (not health) information.

Prepare a Privacy Notice

In order to comply with Gramm-Leach, a health plan will need to begin work immediately on preparation of a Privacy Notice to be provided to its "consumers" and "customers" (terms that will be defined below). The Privacy Notice must contain the following:

- The categories of nonpublic personal information that the plan collects;
- The categories of nonpublic personal information that the plan discloses;
- The categories of affiliates and nonaffiliated third parties to whom the plan discloses nonpublic personal information, unless an exception under Gramm-Leach applies;
- The categories of nonpublic personal information about the plan's former customers that the plan discloses and the categories of affiliates or non-affiliated third parties to whom such disclosures are made;
- If the plan discloses nonpublic personal information to a nonaffiliated third party, and no exception applies to such disclosures, a statement of the categories of information that the plan discloses and the categories of third parties with whom the plan has contracted;
- An explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) for exercising that right; and
- A description of the plan's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Conduct a Privacy Audit

In order to prepare the Privacy Notice, it will be necessary for a health plan to audit its current privacy policies and data management procedures. Such an initiative is consistent with audit efforts that the plan may be undertaking as part of its HIPAA compliance efforts. If the audit identifies deficiencies regarding the plan's protection of customer/consumer information and records, then it may be necessary to adopt or revise certain policies and procedures to comply with Gramm-Leach prior to issuing the Privacy Notice. A privacy audit should also seek to identify all components of a health plan's or insurer's operations providing "financial services" subject to Gramm-Leach. For example, a health plan offering members online access to claims payment data is probably providing a financial service.

Issuing the Privacy Notice

A health plan will need to issue a Privacy Notice annually to existing customers, but may issue the notice at the same time each calendar year to all required parties. The Privacy Notice must also be issued to all new customers at the time that the customer relationship is established. If a plan intends to disclose nonpublic personal information in a way other than as described in its current Privacy Notice, it will also be necessary to issue a revised Privacy Notice and permit the customer or consumer to opt out of the disclosure. Privacy Notices must be provided in writing or, if the consumer conducts transactions electronically and agrees, electronically.

While the deadline for Gramm-Leach compliance in most states is July 1, 2001, the Privacy Notices should be issued at least 30 days prior to that date, giving customers the required 30 days to opt out of disclosures. If Privacy Notices are not mailed out until July 1, 2001, then nonpublic personal information may not be shared with nonaffiliated third parties until the expiration of 30 days after mailing.

A Health Law Practice for the 21st Century

DWT's national health law practice serves all sectors of the health system through our 11 offices across the country. We offer practical, cost-effective solutions to issues faced by both traditional payers and providers and the variety of newly-emerging integrated organizations in the ongoing restructuring of the healthcare system. Our healthcare lawyers represent a full range of clients including licensed professionals and physician organizations, hospitals and multinational health systems, tax-exempt, publicly traded and mutual health insurance companies and HMOs, retirement facilities and healthcare trade associations.

For more information on DWT's Health Law Department, contact your DWT attorney at any of our offices below or call us on our toll-free client line at:

(877) 398 (DWT)-8415

Anchorage, AK
(907) 257-5300

Bellevue, WA
(425) 646-6100

Charlotte, NC
(704) 332-0800

Honolulu, HI
(808) 538-3360

Los Angeles, CA
(213) 633-6800

New York, NY
(212) 489-8230

Portland, OR
(503) 241-2300

San Francisco, CA
(415) 276-6500

Seattle, WA
(206) 622-3150

Washington, DC
(202) 508-6600

Shanghai, China
(011) 86-21-6279-8560

Reece Hirsch is a partner in the San Francisco office of Davis Wright Tremaine LLP. His practice focuses upon representation of health plans, healthcare providers and technology companies with respect to privacy, security and eHealth legal issues.

Reece can be reached at (415) 276-6514 or reecehirsch@dwt.com.

The meaning of Gramm-Leach's distinction between "consumers" and "customers" is critical to determining who should receive a plan's Privacy Notice. Consumers are essentially potential customers who have sought a financial product or service, but who do not develop an ongoing customer relationship. Customers are those consumers that enter into a "customer relationship" with the financial institution. A health plan's consumers may include visitors to the plan's website and individuals requesting information about plan products. The question of who a health plan's customers are is not so simple and will be discussed below.

Many health plans and insurers contract with employers to offer their plan products, rather than selling directly to individual members and subscribers. Under the Gramm-Leach implementing laws and regulations of many states, it is often unclear whether the employer or the individual member or subscriber is the "customer" entitled to receive the Privacy Notice under Gramm-Leach. This is obviously a critical compliance issue that is currently being considered by insurance and health plan regulators in many states.

Health plans and insurers should carefully review their website Privacy Policies for Gramm-Leach compliance. For consumers of a health plan who are not customers (i.e., visitors to the plan's website and individuals inquiring about plan products), a Privacy Notice must be provided if the plan discloses nonpublic personal information about the consumer to a nonaffiliated third party. A website Privacy Policy that discloses the sharing of personal information with non-affiliated third parties may inadvertently trigger the requirement to issue Privacy Notices under Gramm-Leach. When the HIPAA privacy regulations become effective (currently anticipated to be April 14, 2003), the Gramm-Leach Privacy Notice may be combined with the notice of privacy practices that health plans will be required to deliver to members pursuant to HIPAA.

System Modifications

After conducting the privacy audit, a health plan will need to implement any modifications to its existing IT systems necessary to

- track and administer elections by customers and consumers to opt out of disclosures; and
- protect against the unauthorized disclosure of nonpublic personal information.

Conduct Employee Training

To the extent that the Gramm-Leach audit and compliance efforts described above result in new plan privacy policies and procedures, employee training will be necessary to implement those policies and procedures.

Review and Amend Plan Contracts

Gramm-Leach requires that, if the plan shares nonpublic personal information with nonaffiliated third parties, those third party entities may not further disclose the information, unless the disclosure would be lawful if made directly by the plan. This requirement of Gramm-Leach may be addressed by amending existing contracts with such third parties to require their compliance with plan privacy policies. These contract amendments are consistent with the HIPAA requirements that will cause health plans to amend many contracts with "business associates" with which the plan shares protected health information.

HIPAA and Gramm-Leach

For health plans and insurers, HIPAA and Gramm-Leach address similar regulatory concerns and contain several common compliance elements, but HIPAA is a much more comprehensive and rigorous system of regulations. The drafters of HIPAA and Gramm-Leach have recognized the need to coordinate these two regulatory schemes. In the commentary to the FTC's final rule on Gramm-Leach, it is noted that "it appears likely there will be overlap between HIPAA and the financial privacy rules." The FTC also notes that the FTC and other agencies enforcing Gramm-Leach will consult with the Department of Health and Human Services ("DHHS") after final HIPAA rules are published to avoid duplicative or inconsistent requirements.

DHHS notes in the commentary to the final HIPAA privacy rule that, "GLB has caused concern and confusion among health plans that are subject to our privacy regulation." DHHS adds that health plans will need to evaluate state laws implementing Gramm-Leach

CONTINUED ON BACK PAGE

This *Health Law Advisory Bulletin* is a publication of the law firm of Davis Wright Tremaine LLP and is prepared by its Health Law Department, chaired by Susan G. Duffy, Peter N. Grant and Keith M. Korenchuk.

Our purpose in publishing this advisory bulletin is to inform our clients and friends of recent legal developments in the area of healthcare. It is not intended, nor should it be used, as a substitute for specific legal advice since legal counsel may be given only in response to inquiries regarding particular factual situations.

To change your address or to receive additional information, please contact Barrie Handy in our Seattle, Washington office at (206) 628-7404 or barriehandy@dwt.com.

Davis Wright Tremaine LLP
2600 Century Square
1501 Fourth Avenue
Seattle, Washington 98101-1688

**FIRST CLASS
PRE-SORT
U.S. POSTAGE PAID
SEATTLE, WA
PERMIT NO. 1538**

CONTINUED FROM PAGE 3

under the preemption analysis provided under HIPAA, which generally provides that the federal HIPAA regulations will preempt all "contrary" state laws unless a state law is more stringent. Thus, health plans operating in multiple states will be faced with a complex legal analysis in determining whether various state Gramm-Leach laws are subject to preemption under HIPAA. However, given the still-unsettled nature of the HIPAA regulations and the looming July 1, 2001 deadline for Gramm-Leach compliance, it is clear that health plans must comply with Gramm-Leach now and sort out preemption issues later.

As health plans and insurers await the final security rule and the outcome of the new 30-day comment period for the HIPAA privacy rule, Gramm-Leach compliance efforts will serve as an excellent starting point for future HIPAA compliance initiatives. A health plan's audit of privacy practices for purposes of preparing a Gramm-Leach Privacy Notice may be coordinated with the HIPAA readiness assessments that many plans are currently undertaking. In this complex and rapidly evolving regulatory environment, health plans and insurers should develop compliance strategies that do not focus solely on HIPAA, but which coordinate and attempt to reconcile the variety of new and existing state and federal laws relating to security and privacy, including Gramm-Leach.

Davis Wright Tremaine LLP