Prepared by the North Dakota Legislative Council
staff for the Family Law Committee
July 2001

MEDICAL AND FINANCIAL PRIVACY LAWS - BACKGROUND MEMORANDUM

INTRODUCTION

Senate Concurrent Resolution No. 4019 (2001), attached as Appendix A, provides for a study of the medical and financial privacy laws in the state; the effectiveness of medical and financial privacy laws in other states; the interaction of federal and state medical and financial privacy laws; and whether current medical and financial privacy protections meet the reasonable expectations of the citizens of this state.

LEGISLATION ENACTED IN 2001

House Bill No. 1082 provides that if the Commissioner of Financial Institutions furnishes confidential information to a third party authorized to receive that information, the information remains confidential in the possession of the third party, and likewise, if the commissioner receives confidential information, that information remains confidential in the possession of the commissioner. The bill also expands the persons to whom the commissioner may furnish information and may enter sharing agreements to include the Insurance Commissioner and the Securities Commissioner.

House Bill No. 1234 provides that a medical release is valid for three years or the time specified in the release, whichever is less. The bill also allows for termination of the release at any time and allows a provider to share medical information with another provider during the time necessary to complete a course of treatment.

House Bill No. 1329 provides a financial institution may disclose customer information for the purposes of reporting suspected exploitation of a disabled adult or vulnerable elderly adult.

Senate Bill No. 2065 requires a North Dakota federally chartered corporate credit union to allow the Commissioner of Financial Institutions to access records and sets a rate of reimbursement for the credit unions for searching and processing records.

Senate Bill No. 2117 provides a definition of customer as it pertains to the sharing of commercial or financial customer information by the Bank of North Dakota.

Senate Bill No. 2127 provides that insurance companies, nonprofit health service corporations, and health maintenance organizations are required to comply with the privacy provisions of Title V of the Gramm-Leach-Bliley Act. Additionally, the bill allows the Insurance Commissioner to adopt rules to implement the Gramm-Leach-Bliley Act if the rules are consistent with and not more restrictive than the model regulation adopted by the National Association of Insurance Commissioners.

Senate Bill No. 2191 provides that the state's statutory provisions relating to the disclosure by financial institutions of customer information are not applicable if the disclosure is subject to federal law and the financial institution complies with the federal law. The bill also provides temporary disclosure requirements applicable to agricultural and commercial customers of financial institutions, effective through July 31, 2003.

NORTH DAKOTA PRIVACY LAWS

Privacy law and disclosure of information can be evaluated and considered at least two different ways. One approach is to focus on the entity that is being regulated, for example, a financial institution. Another approach is to focus on the nature of the information, for example, medical information or customer information.

Financial Institutions

North Dakota state law does not specifically address the regulation of insurance business privacy and securities business privacy. North Dakota Century Code (NDCC) Chapter 6-08.1, which was enacted in 1985, addresses disclosure of customer information by financial institutions.

As used in NDCC Chapter 6-08.1, a financial institution appears to be limited to more traditional banking institutions and is not as broad as the definition used for purposes of federal legislation. Prior to the 57th legislative session, Chapter 6-08.1 provided a financial institution was prohibited from disclosing customer information unless the disclosure was made pursuant to customer consent or met some other provisions enumerated in the chapter. However, Senate Bill No. 2191 (2001), which became effective July 1, 2001, provides that the state disclosure law under Chapter 6-08.1 does not apply to a financial institution that discloses customer information to a nonaffiliated third party if the disclosure is subject to federal law. The effect of Senate Bill No. 2191 is to defer to federal privacy law if it applies and to rely on state privacy law only to the extent the disclosure is not addressed in federal law.

Medical Information

North Dakota law specifically addresses limitations on the disclosure of medical information under NDCC Section 23-12-14, which, as amended by House Bill

No. 1234 (2001), provides the circumstances under which a medical provider is required to disclose patient medical records. This law is specific to medical providers and patient medical records and does not directly limit disclosure but instead requires disclosure in certain circumstances. Additionally, disclosure of medical information may be limited by professional ethics. For example, Section 43-17-31(13) provides disciplinary action may be taken against a physician for willful or negligent violation of confidentiality between physician and patient.

FEDERAL LAWS

Although there are privacy provisions in a broad range of federal laws, the three Acts that are in the forefront of the privacy issue are the 1996 Health Insurance Portability and Accountability Act; the Financial Services Modernization Act of 1999, which is also known as the Gramm-Leach-Bliley Act; and the Fair Credit Reporting Act.

1996 Health Insurance Portability and Accountability Act

The 1996 federal Health Insurance Portability and Accountability Act was drafted in part to address the lack of a comprehensive federal law protecting the privacy of people's medical records. The Act provides that if Congress failed to pass a comprehensive health privacy law by August 21, 1999, the Secretary of Health and Human Services would be required to issue health privacy regulations. Congress failed to pass health privacy legislation, and the regulatory deadline was triggered. The final regulations were released by the Department of Health and Human Services on December 20, 2000, and the regulations went into effect on April 14, 2001. There is a two-year implementation period before most entities will have to comply with the regulations; however, small health plans will have three years to come into compliance. The Department of Health and Human Services Office for Civil Rights is responsible for implementing and enforcing the privacy regulations. Violations of the regulations can result in civil and criminal penalties of up to $250,000 and 10 years in prison. The regulations do not authorize the Department of Health and Human Services to regulate other entities that handle sensitive medical information, such as life insurers and workers' compensation programs, and do not authorize the regulation of entities that are business associates of health care providers.

The regulations apply to health plans, health care clearinghouses, and health care providers, such as hospitals, clinics, and health departments that conduct financial transactions electronically. The regulations apply to personally identifiable information in any form, whether communicated electronically, on paper, or orally. The regulations do not preempt state laws that afford more stringent privacy protection. The regulations afford:

- Patients' rights to education regarding privacy safeguards;
- Access to medical records;
- A process for correction of medical records; and
- Protection of records by requiring patient permission for disclosure of personal information.

The regulations make special provisions for disclosure of health information for research, public health, law enforcement, and commercial marketing.

There appears to be an ongoing debate among interested persons regarding what the regulations require and allow. On July 6, 2001, the Department of Health and Human Services issued its first guidelines to address questions and concerns regarding implementation of the regulations. Additionally, on July 18, 2001, two state medical societies filed lawsuits challenging the constitutionality of the privacy regulations. The South Carolina Medical Association and the Louisiana State Medical Society argue the regulations are unconstitutional on the following three grounds:

- In enacting the regulations, Congress violated the separation of powers clause of the United States Constitution by delegating its lawmaking powers to the Department of Health and Human Services without adequate guiding principles;
- The regulations are so vague on the issue of state preemption that they violate the due process clause of the United States Constitution; and
- Even if Congress did appropriately delegate its lawmaking powers to the Department of Health and Human Services, the agency exceeded its authority by including all communications, not just electronic transactions mandated by the Act in the final privacy rule.

Financial Services Modernization Act of 1999 - Gramm-Leach-Bliley Act

The federal Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, which was enacted on November 12, 1999, became effective on November 13, 2000. Financial institutions must be in full compliance with the Act by July 1, 2001. The Act removes certain Depression-era restrictions on mergers, affiliations, and other business activities of financial institutions. As used in the Act, a financial institution means any institution that is significantly engaged in financial activities. This extends to:

- Any kind of traditional, regulated financial company, including banks, bank-holding companies, financial-holding companies, securities firms, insurance companies, insurance

agencies, investment companies, thrifts, and credit unions;
- Any other type of business that is significantly engaged in financial activities, regardless of whether the business is regulated or otherwise considered a financial company, such as mortgage brokers, finance companies, and check cashers; and
- Any other type of business that engages primarily in commercial activities but also engages significantly in financial activities, such as a retailer that issues its own credit card with respect to its credit card customers.

Title V of the Act contains privacy provisions applicable to nonpublic personal information about individuals who obtain financial products or services for personal, household, or family purposes. Nonpublic personal information generally includes personally identifiable financial information provided by a customer or consumer to a financial institution in obtaining a financial product or service. Title V of the Act sets a floor for financial information privacy, explicitly permitting states to enact higher standards of protection.

Title V of the Act also provides that financial institutions may share virtually any information with affiliated companies. However, the Act provides for a comprehensive study by the Department of the Treasury; federal functional financial regulatory agencies; and the Federal Trade Commission of current information-sharing practices among financial institutions and their affiliates and unaffiliated third parties. In conducting this study, the Department of the Treasury is directed to consult with representatives of the state insurance authorities. In order to share information with nonaffiliated third-party companies, a financial institution is required to give notice to the customer regarding the institution's information-sharing practices and is required to provide the affected customers an opportunity to opt-out of certain types of disclosures.

As used in the Act, the term “opt-out” refers to the provision of the Act that requires that consumers be notified of their right to prevent their information from being shared with third parties. Under the opt-out provision, unless a customer takes an affirmative action to inform the financial institution that the customer does not want that customer's information shared, the financial institutions may share the information. The term “opt-in” refers to a more protective state law a state may enact, which provides unless a consumer takes an affirmative action to inform the financial institution that the customer wants that customer's information shared, the financial institutions may not share the information.

The nine specific categories of information that must be included in the initial and annual privacy notices under the Act are:

- Categories of nonpublic personal information collected;
- Categories of nonpublic personal information disclosed to others;
- Categories of entities to whom nonpublic personal information is disclosed;
- Policies regarding the disclosures of nonpublic personal information of former customers;
- Nonpublic personal information disclosed under the joint marketing and agency exception;
- Explanation of the Act opt-out right;
- Explanation of the Fair Credit Reporting Act opt-out right;
- Explanation of security and confidentiality practices and procedures; and
- Explanation of the types of disclosures that will be made which are covered by the Act’s general exceptions.

Title V of the Act provides specific exceptions and general exceptions to the restrictions on sharing nonpublic personal information to third parties. The specific exceptions address the provision of information to third parties to perform services or functions on behalf of the financial institution which are intended to cover transfers necessary for joint marketing arrangements or to facilitate a third-party servicing of consumer goods. Under these specific exceptions, the transfers of information must be fully disclosed to the consumers, and the financial institutions are required to enter contractual agreements with third parties, which require the third parties to maintain the confidentiality of such information. The following general exceptions do not require the financial institution to provide any notice to the consumer before transferring the nonpublic personal information to certain third parties:

- Transfers as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer in connection with servicing or processing a financial product or service, maintaining or servicing the consumer's account, or a proposed or actual securitization, secondary market sale, or similar transaction;
- Transfers made with the consent of or at the direction of the consumer;
- Transfers made to protect the confidentiality or security of a consumer's records, to protect against fraud, unauthorized transactions, for required institutional risk control or other liability, or for resolving customer disputes or inquiries;
- Transfers to persons holding beneficial interests relating to the consumer, or to persons acting in a fiduciary or representative capacity on behalf of the consumer;
- Transfers to provide information to an insurance rate advisory organization, a guaranty fund or agency, a credit rating agency, and to permit

the assessment of the financial institution's compliance with industry standards;
- Transfers to the financial institution's attorneys, accountants, and auditors;
- Transfers permitted or required under other laws and in accordance with the federal Right to Financial Privacy Act of 1978, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety;
- Transfers to a consumer reporting agency and transfers from a consumer report produced by a consumer reporting agency in compliance with the federal Fair Credit Reporting Act, in accordance with interpretations of such Act by the Board of Governors of the Federal Reserve System or the Federal Trade Commission;
- Transfers in connection with a sale, merger, transfer, or exchange of all or a portion of the business or operating unit of the financial institution if the disclosure concerns only customers of that business or unit; and
- To comply with federal, state, or local laws and rules; comply with civil, criminal, or regulatory investigations; comply with federal, state, or local summons or subpoenas; and respond to judicial process of government authorities with jurisdiction over the financial institutions.

The state insurance authorities and the following seven federal agencies are responsible for enforcing the Act:

- Federal Trade Commission;
- Department of the Treasury;
- Comptroller of the Currency;
- Federal Reserve System;
- Federal Deposit Insurance Corporation;
- National Credit Union Administration; and
- Securities Exchange Commission.

Each of these seven federal agencies has issued, either individually or jointly, final regulations implementing the Act. The rules adopted by these federal agencies implement the privacy rules for banking institutions and securities institutions. The Act provides that states are responsible for implementing a uniform privacy rule based on the Act for the business of insurance. The National Association of Insurance Commissioners (NAIC) has developed a model privacy regulation for the *states--Privacy of Consumer Financial and Health Information Regulation*, a copy of which is attached as Appendix B.

The National Conference of State Legislatures reports that the NAIC model regulations generally follow the Act, with two notable exceptions:

- The NAIC model regulations set higher standards for health information. The regulations place an opt-in requirement for the disclosure of nonpublic personal health information to affiliates and nonaffiliated third parties, whereas the Act requires only an opt-out standard for all financial information, including health information.
- The NAIC model regulations broadly interpret the federal mandate to include claimants and beneficiaries among those who must receive initial disclosure notices before nonpublic personal information may be shared. The model regulations extend protections to individuals who are not policyholders, such as employees filing workers' compensation claims.

Fair Credit Reporting Act

The federal Fair Credit Reporting Act is enforced by the Federal Trade Commission. The purpose of the Act is to promote accuracy and ensure privacy of information used in consumer reports. The current, amended version of the Act provides consumers added protection over the privacy of their credit bureau files and the sensitive information they contain. In addition to the requirement that employers must obtain an applicant's written permission before obtaining a credit report, employers that deny employment because of something in an applicant's report, now must provide the applicant with a copy of the credit report used before making the adverse decision, rather than just a postdenial notice that their report played a role in the denial. Consumers also now must consent to the release of any consumer report that contains medical information about them. Additionally, consumers also gain protections against unsolicited credit and insurance offers, including the multiple credit card offers that many consumers receive on a daily basis. Under the old law, creditors and insurers were able to use the credit reporting agencies' file information as a basis for developing lists of consumers to whom they send offers. Under the new law, consumers can follow a simple procedure to opt-out of inclusion on future lists. They can call a toll-free number that each bureau must establish, and have their name removed from these lists for two years; if they request, they will be sent a form that will allow them to take their names off these credit bureau lists permanently.

OTHER STATES' PRIVACY LAWS

The organization Privacy Headquarters.com has identified state legislation and regulations from the 2001 legislative session which limit the dissemination of nonpublic personal information. The table is current as of July 10, 2001, and provides information identifying bills by number, indicating whether the legislature is in session or has adjourned, and summarizing the bill or regulation. A copy of the table is attached as Appendix C and can be found at *http://www.privacyheadquarters.com/legwatch/state.html*.

PUBLIC PERCEPTION OF PRIVACY

The Health Privacy Project of the Institute for Health Care Research and Policy at Georgetown University collected the following health privacy polling data:

- Two out of three adults in the United States report they do not trust health plans and government programs such as Medicare to maintain confidentiality all or most of the time;
- 27 percent of those polled believed that their medical information had been improperly disclosed;
- Almost one-third of health care leaders could describe confidentiality violations in their organizations in detail;
- 70 percent of the respondents said the privacy of their personal health information is very important;
- 61 percent of respondents said they are very concerned that their personal health information might be made available to others without their consent;
- 55 percent of respondents said they would not trust an insurance company or a managed care company to keep their personal health information private and secure;
- 85 percent of those polled indicated they were very concerned or somewhat concerned that insurers or employers might have access to and use their genetic information; and
- 11 percent of consumers said they or a family member paid out of pocket for health care rather than submit a claim in order to protect their privacy.

Polling results from the Howard W. Odum Institute for Research in Social Science at the University of North Carolina at Chapel Hill indicate:

- 44.4 percent of those adults polled report they think privacy protection in the year 2000 will get worse (July 1996);
- 52.2 percent of those adults polled report they are very concerned about threats to their personal privacy (June 1998);
- 67.7 percent of adults polled report they strongly agree or somewhat agree that if companies and industry associations adopt good voluntary privacy policies, that would be better than enacting government regulations in this country (June 1998);
- 59.5 percent of adults polled report they have not been a victim of what they thought was an improper invasion of privacy by a business; and
- 78.3 percent of adults polled report they agree that if we rewrote the Declaration of Independence today, we would probably add privacy to the list of life, liberty, and the pursuit of happiness as a fundamental right (January 1990).

STUDY APPROACH

A possible approach to the study of medical and financial privacy laws in this state; the effectiveness of medical and financial privacy laws in other states; the interaction of federal and state medical and financial privacy laws; and whether current medical and financial privacy protections meet the reasonable expectations of the citizens of North Dakota would be to:

- Receive testimony from public and private interested persons regarding the effectiveness of the state's privacy laws, including:
  - The Secretary of State;
  - The Insurance Commissioner;
  - The Commissioner of Financial Institutions;
  - Representatives of financial institutions;
  - Interested citizens;
  - The State Health Officer;
  - The North Dakota Medical Association;
  - The North Dakota Health Care Association;
  - The Attorney General; and
  - The American Civil Liberties Union.
- Review medical and financial privacy laws of other states.
- Follow the implementation of the federal Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.
- Arrange to have a poll of North Dakota adults regarding their medical and financial privacy protection expectations and whether these expectations are being met.

ATTACH:3