Iowa Privacy Task Force
Final Report

Introduction

Like other Americans around the country and like the citizens of other highly developed countries, most Iowans live in an electronic age. We buy our groceries and our gasoline with the swipe of a credit or debit card. Most of us have access to the world wide web at work or at home which we use to search for information, entertain ourselves and purchase goods and services. E-mail has become nearly as common as a post card and the phrase "you've got mail" is as identifiable and as understood as any marketing jingle. Wireless phones and pagers have replaced the dinner bell for some children as the call to supper. Now, the telephone, the television, the radio and the Internet are beginning to merge, overlap and directly compete.

Partly fueled by changes in technology, our world has gotten more global and less local. We can search the world for information and electronically chat with unseen neighbors across the new "backyard fence" of the Internet. We are also more likely to do business with large, national or international corporations for many of the goods and services we buy. Electronic communication tools facilitate these new communication and trade pathways and they also create the capabilities to capture and track more information about each other.

These dramatic changes in the way we interact with each other have been a liberating experience for many individuals and a boon for many businesses. At the same time, these changes have raised concerns for many average citizens. Many Iowans, like other Americans, are concerned about a loss of privacy associated with the new Electronic Age. The ability of computers to track our incomes, our financial assets and liabilities, what we buy, what we see on the Internet, our health status, the health treatments we receive and even the flaws in our individual genetic makeup can be a scary reality to some Iowans..

In response to these tremendous changes in our world and the concerns that Iowans have about privacy in this new world, Governor Thomas Vilsack commissioned the Iowa Privacy Task Force in October 2000. The Governor asked the Task Force to focus on two areas of particular concern, the privacy of health and financial information. This is the final report of the Iowa Privacy Task Force.

The Iowa Privacy Task Force

In appointing the Iowa Privacy Task Force, Governor Vilsack sought to obtain the opinions of both average Iowa citizens and businesses and professionals that work with health and financial information. The Governor recognized that the free flow of information is essential to the vitality of the Iowa economy. At the same time, he also recognized the legitimate fears and concerns of Iowa citizens with the potential loss of privacy inherent in the vast new information flows in this new economy. In order to obtain broad and balanced input, the Governor appointed half the members of the Task Force to represent average Iowa citizens. The other half of the Task Force was appointed with representatives of the financial services industry, providers of health care and the health insurance industry. The Task Force was further balanced to

represent the different geographic regions of the state and gender. A total of 32 members were appointed to the Task Force.

The Task Force was co-chaired by Stephen Gleason, D.O., Director of the Iowa Department of Public Health and Holmes Foster, Director of the Iowa Department of Commerce. Meetings of the Task Force were facilitated by Paul von Ebers, President of von Ebers & Associates. This report on the deliberations of the Task Force was written by von Ebers & Associates. A list of Task Force members is included in Appendix A.

The Governor asked the Task Force to complete the following tasks:

1. To develop an understanding of the concerns of Iowans with regard to the privacy of health and financial information.
2. To develop an understanding of the needs and concerns of health and financial services businesses and institutions for the legitimate uses of information.
3. To evaluate current federal and Iowa law and the practices of state government regarding privacy of health and financial information.
4. To evaluate laws or proposed laws or regulations in other states that may offer valuable lessons for Iowa.
5. To make recommendations to the State of Iowa regarding any changes in law, regulation or policy that would enhance protection of the privacy rights of citizens and allow legitimate information use by the health and financial services industries.

The Task Force went about these tasks through health and finance work groups made up of Task Force members. Each work group was composed of eight consumer members and eight health or finance industry representatives. The Task Force met as a whole on three occasions. In between these meetings, the Health Work Group met 6 times and the Finance Work Group met 5 times. In addition, the Finance Work Group commissioned a sub-group of two consumer representatives and two industry representatives to resolve certain issues. This sub-group met 4 additional times.

In conducting its work, the Task Force heard testimony from national experts on financial and health privacy issues. The Task Force heard speakers describe to them the details of two federal laws dealing with health and financial information privacy, the Health Insurance Portability and Accountability Act (HIPAA) and Title V of the Financial Modernization Act of 1999 (also known as Gramm-Leach-Bliley or GLB). The Task Force reviewed information about the privacy activities of other states and the current privacy laws and regulations in Iowa. The Health Work Group conducted a public hearing to hear from interested Iowans about their privacy concerns and the Finance Work Group conducted a survey of Iowans to determine their primary privacy concerns.

This report of the Iowa Privacy Task Force is structured around a set of privacy principles developed by the Task Force. These principles were voted on by the Task Force and passed with unanimous or nearly unanimous votes by the members present at the meetings. In some cases, these principles represent compromises on the level of action that the group could agree on. In some cases, consumer representatives would have liked the principle to go farther in restricting use of personal information. In other

cases, industry representatives would have liked to see less restrictions on use of personal information. These differences are reflected in the discussion that follows each principle.

These principles, when taken together, provide a roadmap for Governor Vilsack and other Iowa policy makers to follow in finding a balanced approach for personal privacy and a vibrant economy. The Task Force did not go beyond principles to recommend specific changes to Iowa law and regulation for several reasons. First, and perhaps most importantly, new federal laws have just recently been imposed in the areas of financial and health information privacy. While financial privacy regulations under Gramm-Leach-Bliley (GLB) are final, the health information privacy rules under HIPAA, while officially final, are still being debated in Congress and may be changed. The Task Force noted areas where its principles differ from GLB or HIPAA. In particular, the Task Force defined the entities that handle financial and health information more broadly than does either GLB or HIPAA. In addition, the Task Force does not necessarily endorse all of the detailed regulatory requirements of HIPAA.

The Task Force believes that Iowa policy makers must carefully consider the early implementation stage of federal regulations in deciding whether these Iowa principles should be translated into Iowa law. Many of the principles can be implemented under current law or regulation or through voluntary and cooperative public-private efforts. However, this report should not be interpreted as endorsing current federal privacy law or as recommending that Iowa policymakers not consider additional state legislation if they believe it would be beneficial. This area of privacy law is complex and difficult. The Task Force did not believe that it had the time or the resources to adequately address all of the issues required to make final legislative recommendations. The Task Force urges the Governor and the Legislature to continue the effort to evaluate Iowa law and regulation on the basis of the principles in this report.

Background

The transformation of our world onto an electronic platform began several decades ago as businesses, and then government, began to use information technology tools to automate internal processes. Dictation gave way to word processing. Calculators and paper spreadsheets gave way to spreadsheet software. Accounting, inventory and billing systems became software based, instead of paper based. Gradually, internal networks were created to allow employees of businesses to communicate with each other.

With the birth of the Internet, a new wave of electronic communication and commerce emerged, allowing businesses and individuals to communicate and transact business across a variety of computer platforms, quickly, easily and inexpensively. Although the promise of the Internet briefly outran its reality in the dot.com bubble of the late 1990's, electronic communication and commerce have already radically transformed both our business and personal lives. This report, for example, will be published on the Internet, instead of a more traditional publishing format.

One side effect of this explosion in the use of electronic tools is the explosion of information captured in electronic transactions and records. As the cost of computer hardware and software plummeted, it became possible to capture, store and analyze

masses of data that did not exist before. Analytical software advanced in step with this data capability. Huge databases and the software to manage and understand them have allowed businesses to become more efficient in serving their customers, reducing business risk and marketing new products or services. Today, as this report goes to print, a commercial is running on major television stations that describes software used to track, analyze and anticipate the purchases of some unknown consumer. The fact that enough television viewers understand this commercial to make its broadcast worthwhile is a testimony to how much our world has changed.

One area where electronic commerce has grown with leaps and bounds is the financial services industry. Many financial services institutions now have websites that allow customers to transfer funds, pay bills and check balances on line. On-line investing has grown and a few financial institutions are completely Internet based, without any "retail" or commercial physical locations for customer interactions. Consumers are demanding and using more electronic tools to track and model their finances and calculate and pay their taxes. Financial services institutions, and many other businesses, are using electronic information tools to improve customer service, track inventories, assess and manage risk.

While the healthcare sector of our economy has lagged behind some other industries in the use of electronic tools, this world is changing as well. A majority of all claims for health insurance benefits are now filed electronically. Aside from e-mail, a top consumer use of the Internet is to search for health related information. Most health insurance companies have websites that allow customers to send inquiries or find a participating health care provider. Many employers are encouraging employees to select and manage their health benefits through company networks or the Internet.

Electronic tools have emerged in clinical settings as well. Physician orders and nursing notes are increasingly captured on electronic systems in hospitals. Hospital databases are helping clinicians locate and view medical images, lab results and surgical notes from workstations without tracking down paper medical records. Physicians and other professionals are beginning to use handheld devices to write prescriptions and research medical topics. A small, but growing number of practitioners are capturing all of their patient notes and test results in electronic medical records.

Iowans, like most Americans, have largely embraced these dramatic changes in the way we communicate, do business and obtain health care services. Our expectations of both financial and health care institutions have increased based on our understanding of the information tools available to health and financial professionals. At the same time, our concerns about privacy are perhaps highest in the areas of our financial and health information.

In many ways, we have no less privacy today than when most Iowans lived in small towns. In the small town of our histories, the grocer and the hardware store owner had a pretty good idea of what we bought as individuals. The librarian would recommend a good book based on what she knew of our reading preferences. Everyone had a pretty good idea of everyone else's income and, if we needed health services, our hospital admission was reported in the local newspaper and the church bulletin.

Our concerns about privacy are not so much how much is known about us, but how many people know and how much control we have over the information. We may be more concerned about an Internet bookseller knowing our reading preferences than the local librarian. We may be less comfortable with the privacy of our personal financial information in a national financial institution with 100,000 employees than we were at the local bank. We may be less concerned that our neighbors know our health condition than that a pharmaceutical company has access to our health records or a health insurance company has a copy of our personal genetic map.

A survey of Iowans conducted by the Task Force reflects these conflicting reactions to the new world we live in[1]. (A copy of the questionnaire and the survey results is included in Appendix B.) On the one hand, the large majority (97%) of surveyed Iowans have not experienced any problems with the privacy of their personal information in their dealings with a financial institution, a health care provider, an attorney, an accountant, other professionals or other businesses. Many Iowans are using electronic tools with few problems or concerns. The survey found that three out of four Iowans have a credit card or have had one. Twenty-five percent (25%) of those with credit cards have given their card number to a merchant over the phone at least occasionally. Fifty-seven percent (57%) of Iowans surveyed have used the Internet and forty percent (40%) of Internet users have used a credit card to purchase something online. Only thirty-eight percent (38%) of those who have purchased something on the Internet with a credit card were worried about the security of that transaction. Only thirty-five percent (35%) of those surveyed have their Social Security numbers on their personal checks, but nearly three quarters of those surveyed have provided a Social Security number if asked.

At the same time, Iowans seem much more conservative about some common business information practices. For example, a large majority of Iowa Internet users (69%) believe that Internet sites should not be allowed to use website registration information to market their own products or services. Nearly all Internet users surveyed believe that businesses or Internet Service Providers should be required to ask consumer permission before they can share or sell website registration information to other businesses. A majority (55%) of Iowans surveyed was somewhat or very concerned that personal financial information that they provide to businesses might be shared with other businesses without their permission.

Sixty-four percent (64%) of those surveyed were somewhat or very concerned that businesses might share or sell information about their purchases to other businesses without their permission. Ninety percent (90%) of survey respondents believe that businesses should be required to notify customers if they use names and addresses from customer checks to update mailing lists. Ninety-seven percent (97%) of Iowans surveyed agree that businesses should be required to ask permission from the customer before sharing or selling the names, addresses or phone numbers of customers to other businesses.

[1] The survey was conducted by the Iowa State University Statistical Laboratory under the direction of the Iowa Privacy Task Force. A statistically valid sample of 207 Iowans were interviewed. The survey has a Margin of error of ± 7% at the 95% confidence level.

While all surveys have limitations, the results of this survey do present a snapshot of the current attitudes of Iowans and the Task Force believes it is a valuable source of information when seen in that light.

The Task Force attempted to consider both the desire of Iowans to use electronic tools and the high levels of concern for privacy expressed by Iowans. The Task Force also sought to balance the needs of business to use information to meet customer needs and improve efficiency against the privacy concerns of Iowans. These sometimes conflicting concerns are reflected in the principles adopted by the Task Force.

Proposed Iowa Privacy Principles and Discussion

The following privacy principles are organized into three sets of principles: general principles that apply to health and financial information and then principles that apply specifically to health or financial information. Under each principle there is a discussion of the specific health or financial information privacy issues that were addressed by the Task Force[2].

General Privacy Principles

1) The State of Iowa should adopt a policy regarding the privacy of citizens' personally identifiable health or financial information.

   Many Iowans, like many other Americans, are concerned about their personal privacy especially the privacy of sensitive financial and health information. There are a number of federal and state laws and regulations that address a variety of privacy issues. However, these laws and regulations do not address, in a comprehensive way, all of the areas of concern of Iowans related to the privacy of personal financial and health information (see Appendix C for a summary of Iowa and Federal law addressing personal privacy). The State of Iowa should develop a comprehensive policy on the privacy of health and financial information of individual citizens. The policy should address the concerns of Iowans who believe that overly restrictive privacy policies will be harmful to consumers, businesses and the Iowa economy as well as the concerns of Iowans who believe that additional privacy restrictions are needed. As noted below in general principle number two, this policy may be implemented in a number of ways, including the administrative policies governing the activities of state agencies, enforcement of existing laws and regulation, educational and assistance efforts and possibly the enactment of a new law or laws.

2) Implementation of Iowa's health and financial privacy policies should include a full range of options, such as legislation, market-based and educational solutions,

[2] Please note that in developing these principles, the Financial Information Task Force intended that the words "citizen", "person" and "individual" refer to natural persons, rather than corporations, not for profit entities or other organizations. The word affiliate is intended to refer to situations where one entity controls, is controlled by or is under common control with another entity. The definition of control has not been addressed. Since not for profit organizations and government entities are included in the definition of covered entities, the definition of control may be different from some current privacy regulations.

enforcement and other appropriate means.

Law and regulation can be important tools for the protection of individual rights and for the creation of a competitive and efficient marketplace. However, law and regulation can also sometimes impose unnecessary costs and burdens on both individuals and businesses and can be difficult to change in response to new developments. Iowa policy makers should consider what protections for citizen privacy could be achieved through a rigorously competitive marketplace, through educational efforts and through additional law or regulation.

Health Discussion:As an example of current public and private efforts on health information privacy, the Task Force noted that privacy policies currently used by Iowa physicians and hospitals have been developed by private professional associations and accrediting agencies through their codes of conduct or ethics, but these private rules can be enforced under the Iowa Board of Medical Examiners and the licensing process for Iowa hospitals.

The Task Force suggests that Iowa policy makers consider the following factors in seeking the appropriate balance in these implementation tools. The recently promulgated HIPAA privacy regulations will impose many new requirements on both providers and payers. Industry representatives indicated that they believe the cost of compliance with all HIPAA requirements (including both privacy and other requirements of the law) will significantly exceed Y2K preparation expenses. Yet not all entities covered by these Iowa principles are covered directly by HIPAA. In some cases, Iowa principles call for tighter controls on the use of personally identifiable health information than HIPAA regulations. Policymakers will need to consider whether current federal regulation, competition and/or private/public educational efforts are likely to provide sufficient protection to Iowa citizens and create an appropriate business climate.

Finance Discussion: As an example of private efforts to protect privacy, industry representatives noted that some Iowa financial institutions are providing consumers with more privacy choices than required by federal law because they believe their customers are demanding such choices. The State of Iowa also is providing some educational resources to Iowans on how to avoid identity theft and how to increase their financial privacy in other ways. The tools that best balance the needs of citizens and businesses should be employed.

The Task Force suggests that Iowa policy makers consider the following factors in seeking the appropriate balance in these implementation tools. The Gramm-Leach-Bliley Act allows for states to enact legislation that has stronger protections for individual citizens than provided for in GLB. However, federal courts have sometimes ruled against state regulation of financial institutions that is stronger than federal regulations (e.g. In 2000, the United States Court of Appeals for the Eight Circuit found portions of Iowa Code 527, as it relates to ATMs, to be unenforceable against national banks). At the same time, GLB does not cover all of the entities listed by the Task Force as entities that should be covered by Iowa policy. Some Iowa statues (e.g. the Consumer Fraud Act) provide protection against "unfair practices" in connection with the sale or advertisement of merchandise. This

law was used in a recent case against a financial institution that involved both privacy issues and potential fraud. However, many of the principles covered in this report are not explicitly addressed for all proposed covered entities by either Iowa or federal law. Policymakers will need to consider whether current competition or private/public educational efforts are likely to provide sufficient protection to Iowa citizens.

Throughout the discussions of the financial privacy subcommittee of the privacy task force, industry representatives asserted that Iowa should not enact requirements that exceed those of federal law while consumer members asserted that Iowa should not foreclose the possibility of enacting legislation exceeding federal requirements, if deemed necessary to protect Iowans. Industry representatives argued that the GLB privacy provisions were the result of careful consideration and balancing of the beneficial and adverse effects of privacy protections, so changes to the federal standards are not necessarily desirable. In addition, other federal statutes, such as the Fair Credit Reporting Act, do not allow inconsistent state requirements covering certain subjects. Industry representatives asserted that the enactment of Iowa-specific privacy legislation would impose additional costs, not only on businesses that operate only in Iowa, but also on those that operate in Iowa and elsewhere. Industry representatives asserted that compliance with varying state laws would be difficult and that a uniform, federal law would be preferable. They also asserted concerns that Iowa businesses not be disadvantaged by having to comply with a state law with requirements which might go beyond those which might be interpreted by courts to set the limits on national businesses which also operate in Iowa. Industry representatives expressed concern that Iowa not be placed at a competitive disadvantage in business development vis-à-vis other states by having more stringent privacy laws than those of other states. Finally, industry representatives pointed out that consumers could benefit from the free flow of information as well as businesses, so that more privacy "protection" isn't necessarily better for consumers[3].

Task force members representing consumer interests pointed out that the federal Gramm-Leach-Bliley Act, as it relates to financial privacy, specifically provides that states may give greater protection to consumers than provided by the federal Act. They expressed concern that this report not unnecessarily tie Iowa to federal law as a "ceiling," when, in fact, Congress specifically intended it to be a "floor" and expected that states would wish to consider giving greater protection to consumers. Consumer task force members agreed with industry representatives that the application of an Iowa privacy law should not result in more stringent standards for Iowa businesses competing in Iowa with those that are not Iowa-based. However, they did not agree with the notion that the industry's desire for uniformity and concern about costs or difficulty of compliance with state-specific laws should

[3] A June 4, 2001 letter to the Task Force from Patricia Parachini of the American Council of Life Insurers identified the following benefits to consumers of information sharing:

- Reducing costs and making insurance, credit and other financial services more available and convenient.
- Speeding up insurance policy approvals and other decisions.
- Creating one-stop shopping for financial services.
- Identifying financial products and services that better meet consumers' needs.
- Facilitating online financial services.
- Preventing fraud.

override benefits to consumers under all circumstances.

Consumer members were adamant that this report not simply defer to the uniformity argument and that Iowa policymakers should, under all circumstances, consider the benefits for consumers of additional financial privacy protection which might be provided by Iowa-specific law and weigh that against the costs and other burdens of compliance. Finally, they also asserted that better privacy protection in Iowa might benefit economic development by making Iowa a more desirable place to live and work.

Both industry and consumer members agreed that the privacy policy of this state should extend consumer rights to transactions involving businesses and other entities not currently covered by the federal privacy law, including retailers, colleges and universities and others. The Task Force recognized that many entities that would be required to give privacy notices to consumers under the policies proposed in this report have not been part of the dialogue with the Task Force. The Task Force recommends that policymakers seek the input of those businesses and other entities in determining Iowa's policy regarding financial privacy.

3) Iowa privacy policy should cover all persons or entities that hold, handle, store or transfer personally identifiable health or financial information.

Health Discussion: This principle is designed to include all licensed or certified health care treatment providers and facilities and the employees of such providers or facilities, including some treatment providers not routinely covered under health insurance plans such as massage therapists and any other licensed service provider who routinely collects health information. This would include pharmacies and durable medical equipment retailers. It is also intended to include health insurance companies, health maintenance organizations, organized delivery systems, employer sponsors of health plans, disease and case management companies, wellness and preventive health service providers, health care advice organizations, third party administrators, claims clearinghouses, billing services, data warehouses, research organizations, pharmacy benefit management companies, provider network organizations and any other person or entity that routinely holds, handles, stores or transfers personally identifiable health information. It would theoretically include Internet website organizations, but state regulation of such sites may be difficult.

This definition of covered entities is substantially broader than those entities covered directly by the federal HIPAA legislation. HIPAA directly covers only those entities that are involved in the creation and transmission of certain electronic transactions. HIPAA regulations broaden the coverage by requiring covered entities to include HIPAA privacy protections in contracts they have with "business associate" organizations. This Iowa principle attempts to directly cover all entities that hold, handle, store or transfer personally identifiable health information.

Finance Discussion: The Finance Task Force identified a number of entities that should be covered by Iowa's financial information privacy policy. These entities should include but not be limited to those entities listed in Appendix D. It is important to note that this proposed list of covered entities is broader and more

comprehensive than those covered under the Financial Services Modernization Act (or Gramm-Leach-Bliley). This list reflects the understanding by the Task Force that many organizations other than financial institutions hold, handle, store or transfer personally identifiable financial information about Iowa citizens. Federal financial information privacy law does not cover, for example, retail establishments or hospitals except to the extent they are involved in financial activities, such as offering to finance purchases by their customers. Yet both retail stores and hospitals often collect and store credit card information of individual consumers. The proposed broad scope of Iowa privacy policies may require the implementation of new laws or regulations.

The Task Force agreed that the intent of this principle was to address entities that hold, handle, store or transfer financial and health information as part of their regular activities. However, it is also intended to cover any misuse of the personally identifiable information of another person, whether by a covered entity or any individual.

The Task Force discussed how this covered entity policy would apply to news organizations. The Task Force was clear that it did not want Iowa policy to restrict freedom of the press in any way. The Task Force felt that the privacy policy of the state should not apply to the news functions of news organizations. However, the business operations of a news organization could be covered by this policy. For example, if a news organization, as an employer, holds personal financial information of employees, this information would be covered by the privacy policies.

The Task Force also recognized that some entities and professions are already covered by law, regulation or professional standards of ethics. The Task Force recognizes that states are limited by the Fair Credit Reporting Act on changes that can be made in the regulation of credit reporting agencies. The extent to which Iowa or federal law and regulation for particular entities matches with the principles identified here will need to be carefully investigated by policy makers. The extent to which professional ethical standards of professions (e.g. certified public accountants and attorneys at law) effectively protect individual privacy should also be considered.

4) <u>Release or disclosure of health or financial information that is not personally identifiable or that is legally obtained from public sources is acceptable.</u>

Health Discussion: In this principle, an emphasis is placed on the word “identifiable”. Health information may be identifiable in many ways including name, address or phone number, identifying numbers such as a health plan ID number or Social Security number, demographic information, or a small population sample. Health information is considered “non-identifiable” only if the information cannot be identified with an individual by any means by the user of the information.

This principle suggests that it would be acceptable for a health care provider to release non-identifiable data for medical research or other purposes without disclosing this use to patients or obtaining their consent. As noted above, there is a need to develop reasonable rules on the use of individual case information in order to allow legitimate research while protecting individual privacy.

Hospital representatives have raised concerns about how the term "personally identifiable" will be interpreted. These representatives noted that the data collected by the Iowa Hospital Association (IHA) is currently available to hospitals and other entities for purposes of community health planning and improving health care quality and access to care. Patient names, addresses and Social Security numbers have been removed, however, the information does include dates of service, zip codes, and other information that could potentially be used to identify individuals. The likelihood of identifying individuals from this database is remote, but theoretically possible. Certain health plans and others use similar databases for similar research purposes. Under HIPAA the ability of IHA to collect this data may be in jeopardy. The Task Force discussed the data collection activity of the IHA and other similar data organizations and believes these are legitimate and appropriate uses of health care information and should be allowed to continue.

Finance Discussion: A majority of the members of the Task Force agreed with this principle, as it is stated. Financial information may be identifiable in many ways including name, address or phone number, e-mail address, identifying numbers, account numbers, PIN's, screen name, passwords or Social Security number, demographic information, or a small population sample. Financial information would be considered "non-identifiable" only if the information cannot be identified with an individual by any means by the user of the information.

There was one area of concern related to this principle that has not been resolved. First, some business members of the Task Force would have preferred the principle to say "legally <u>obtainable</u> from public sources." These members believe that if certain information is publicly available (such as names and addresses in a phone book), its use should not be restricted even if the information is not obtained from a public source. An example might be the name and address of an individual that is provided by that individual in the course of doing business with a covered entity. If this information is available in the phone book or another public source, businesses want to be able to use this information without restriction. Some consumer members want a choice on whether this information may be disclosed to an unrelated third party, even if the information is obtainable from a public source.

Task Force members who favored greater privacy restrictions contend that in this information age, a great deal of personally identifiable financial information about an individual could be collected – albeit at great expense – by aggregating seldom used public sources. They argue that the mere fact that a certain critical piece of information is theoretically public in some limited or unforeseeable way should not create a regulatory loophole that denies protection for personal information that was actually supplied and entrusted to a covered entity by a consumer. Examples used by Task Force members included Social Security numbers, financial account numbers, mortgage balances or other information that may be supplied to a government agency as part of a required filing or a request for assistance.

Some Task Force members proposed that such a loophole could be closed by limiting the public records exemption to information that was actually <u>obtained</u> from public sources. In justification of this view, proponents argue that it more closely comports

with what consumers expect when they personally supply information to covered entities. In addition, proponents believed that this limitation would reduce arguments over the source of information and the responsibilities of the parties.

Other Task Force members argued that the concerns noted above could be best addressed by examining what information is available from public sources. In addition, some members pointed out that information like mortgage balances ages quickly and most financial institutions would be likely to request such information directly from the consumer, rather than using public source information.

5) Individuals should have a reasonable right to access their personally identifiable health or financial information held by covered entities and the right to request corrections of inaccurate health or financial information.

Health Discussion: Codes of ethics for physicians and hospitals require that patients be allowed access to medical records. However, Iowa law does not require access, and these codes of ethics do not extend to all handlers of health information. This principle says that patients should be able to see and obtain a copy of medical records and health plan claim records. In addition, it would allow patients to request a correction of inaccurate information and to supplement information on the record. In general, the Task Force was supportive of access to and supplementing of personal health information records.

Corrections are more problematic. While the Task Force agreed that incorrect factual information should be corrected (e.g. the cause of death for a family member is incorrectly recorded in a family medical history), it was not agreed that providers would be required to honor the request for a correction from a patient. Providers are concerned that patients may wish to challenge information that reflects their medical judgment, not simply objective facts. Providers do not want to be compelled to change a record when there is a dispute between the professional judgment of the provider and that of the patient.

Since it is hard to draw a line between factual versus interpretive information, the Task Force agreed that providers should not be required to make any changes. Providers should accept supplemental information from patients, even if that supplemental information contradicts their professional judgment. Providers believe that factual errors will be corrected if called to their attention. Consumer members remain concerned that all errors may not be corrected.

Providers also pointed out that medical record standards do not allow the elimination of any information originally entered into the patient record. Any changes (even those correcting a factual error) must be made as an addendum or inserted in a way that allows the original notation to be read. The date and person making the changes must also be recorded.

Another area of concern is patient access to disclosure records. For example, assume a provider or a health plan wishes to disclose information to a third party and the patient has agreed. Should the consumer have access to a record of such disclosures? Provider members indicated that a disclosure track record is kept in most hospitals

and larger physician office settings, but may not be in smaller provider settings. It is unclear whether payers would have such disclosure tracking records.

Consumers raised concerns about whether consumer supplements to a medical record would follow the record when it is transferred from one entity to another. The Task Force agreed that consumer supplements should follow patient records as they are transferred from one provider to another.

Provider concerns were raised with unlimited patient access to medical records, especially, but not limited to, mental health patients. After hearing from mental health professionals, the Task Force agreed that providers should be able to restrict patient access to records if, in the opinion of the provider, such access would cause harm to the patient or others. Consumer members were concerned that a procedure should be in place to challenge restricted access to mental health records.

Finance Discussion: Consumers can be harmed by the use of incorrect information by organizations involved in financial transactions. Even information provided by the consumer may be incorrectly recorded by the organization holding the data. Consumers should have a reasonable right to see and request corrections of any personal financial information held by covered entities. In some cases, organizations may hold consumer information that is proprietary in nature (e.g. the reports of credit bureaus paid for by the organization). The Task Force concluded that organizations should not be required to provide such information to the consumer.. If the organization chooses to disclose such proprietary information, the Task Force acknowledged that organizations might charge a fee for this information. In some property transactions, appraisals must be disclosed to consumers, but the financial institution may charge for the appraisal report.

In addition, the Task Force concluded that covered entities should not be required to provide access to internal work products. Internal work products would include internal analyses of credit or insurance risk done by a financial institution before approving a loan or an insurance policy, customer service reports or market research analysis and other similar analyses or work notes. The term “reasonable right to access” allows for the use of reasonable copy charges for consumer information requests.

6) <u>There should be strong and effective remedies and enforcement procedures for privacy violations including meaningful penalties where appropriate.</u>

Health Discussion: While the Task Force generally agreed with this principle, industry representatives were concerned about penalty overkill. In addition, some members of the Task Force were concerned that penalties should not be applied to unintentional mistakes in handling health information. At the same time, some members believe that sufficient incentives should exist for organizations handling health information to reduce the risk of unintentional errors, since the harm caused by unintentional privacy violations can be as great as that caused by intentional violations.

Finance Discussion: While the Task Force is not directly recommending new legislation or regulation, it recognizes that if legislation or regulation is necessary, there must be reasonable mechanisms to enforce such a law or regulation that are carefully tailored, practical and effective.

7) Government should assist covered entities in maintaining high levels of security to ensure privacy of non-public personally identifiable health or financial information in their possession.

Due to the importance of personal privacy to Iowa citizens, Iowa government should support covered entities, especially small business, in maintaining security of non-public personal health and financial information. This assistance should take the form of educational materials to businesses, adult consumers and children in schools, direct assistance from Iowa state agencies (e.g. the Attorney General's office), adequate funding for law enforcement through the Attorney General and county attorneys and tax credits for costs associated with securing privacy within a vibrant and growing economy and other means.

8) Covered entities handling personally identifiable health or financial information should adopt privacy and security policies and procedures for the collection, storage, access, use and disclosure of such information.

Health Discussion: Providers noted that the Joint Commission for the Accreditation of Healthcare Organizations (JCAHO) has requirements covering these issues. However, JCAHO covers primarily hospitals and other health facilities. Professional providers and payer organizations are not covered. The primary concern of health care organizations on this principle has to do with the implementation requirements. The Task Force did not attempt to identify the appropriate level of privacy and security policies and procedures for each type of covered entity, but believed strongly that all covered entities should implement such policies and procedures that are reasonable and appropriate.

Finance Discussion: While this principle does not direct covered entities to implement specific levels of privacy and security procedures, the Task Force recognizes that appropriate activities will vary by the type and size of a covered entity. The Task Force, in particular, does not want to see undue burdens placed on small Iowa businesses. At the same time, the Task Force believes that all entities that hold, handle or store non-public, personal financial information should take steps to protect such information in accordance with these principles. In order to assist small business in holding down the costs of good privacy practices, the State of Iowa should prepare and distribute sample security policies and procedures for small businesses.

Health Information Principles

1) Personally identifiable health information should be defined broadly to include all individual patient demographic information, individual and family health history, individual diagnosis, treatment, diagnostic tests or images, professional treatment notes and individual health insurance coverage information.

This definition is intended to include nearly all personally identifiable information collected and used by health care providers and payers. Personally identifiable financial information collected by health care providers or payers is covered by the principles identified for both health information and financial information. Health information would be considered "non-identifiable" only if the information cannot be identified with an individual by any means by the user of the information.

Hospital representatives have raised concerns about how the term personally identifiable will be interpreted. These representatives noted that information collected by the Iowa Hospital Association (IHA) is available to qualified researchers on an individual case basis. Patient names, addresses and Social Security numbers have been removed from the IHA database, but the information does include dates of service, zip codes and other information that could be used to identify individuals. The Task Force does not intend to inhibit legitimate research. However, the Task Force is concerned about the release of potentially identifiable health information and recommends that reasonable guidelines be developed for the use of public databases to prevent the unintentional release of identifiable data.

2) Individuals should be given notice of the core and non-core uses of personally identifiable health information. Core use is that use required in order to obtain health services, for payment for health services, for the routine operations of a health service provider or payer, or as required by law. Non-core uses include all other uses of personally identifiable health information.

Patients expect that personally identifiable health information will be used to provide them with appropriate health services. Patients generally expect that personal health information will be shared within a health care organization or between health care providers (e.g. in the case of referrals) on a need to know basis in order to facilitate good treatment or other health services. They also generally expect that providers of care will use this information to apply for payment from health payers (health insurance plans and government programs). Personal health information may also be needed for certain operational activities, such as accreditation or credentialing. However, when personal health information is to be released outside the organization for purposes other than these "core" functions, individuals should be notified of this intended use.

There was some disagreement within the Task Force regarding the definition of the "core" functions of treatment, payment and operations. For example, some members of the Task Force are concerned about release of personal health information by health plans to disease management companies. Health plans offer disease management programs to members, usually on a voluntary basis. Such disease management programs often include patient educational materials and contact with case managers who advise patients about treatment alternatives and check with patients on treatment compliance. Potential participants in disease management programs may be identified by diagnosis and treatment information included in health insurance claims.

Health plans frequently outsource disease management programs to outside firms

that specialize in managing specific diseases. Even though health plans usually include a short description of disease management programs in benefit summary documents, some consumer members of the task force believe that health plans should ask permission before supplying personally identifiable health information to their disease management contractors. Health plans have argued that part of the expertise of disease management firms is their ability to approach potential participants.

Others members of the Task Force are concerned about solicitations to doctors or patients from pharmaceutical companies based on claim data sent through pharmacy benefit management companies. The disclosure of personally identifiable health information from a pharmacy benefit management company to a pharmaceutical manufacturer to allow marketing to physicians or patients was considered by the Task Force to be a non-core use requiring notification and consent by the patient. The Task Force's opinion of this issue was the same for pharmacy benefit management companies that are subsidiaries or affiliates of pharmaceutical manufacturers.

Finally, some health care provider members were concerned about solicitations for new health care services to patients unless the service represents a proven advancement in service quality.

The Task Force also discussed medical research and health care data analysis. The Task Force concluded that these are not core uses, but would be covered by these principles based on whether or not the information used in research or analysis was personally identifiable. The Task Force agreed that notice should be given if personally identifiable information is used for research or analysis. Notice would not need to be given for uses of information that is not personally identifiable.

This principle is less restrictive, in some ways, than the HIPAA regulations released in December. HIPAA requires notification of even the routine uses described above. However, providers or health plans may refuse service if the patient customer refuses to allow use of information for treatment, payment and routine operations. On the other hand, current HIPAA regulations allow providers to use personally identifiable health information for a variety of marketing purposes. The Iowa Task Force principle would require providers to obtain patient approval before releasing personally identifiable information to non-affiliated marketing organizations.

3) Individuals should have a right to decline "non-core" uses of personally identifiable health information and should be notified of that right, unless release of such information is required by law.

This principle is intended to be consistent with GLB and the NAIC model act as these regulations apply to financial institutions that hold health information. As noted above, it is somewhat more narrow than HIPAA, which requires patient approval for some "core" uses of data. Any entity handling personally identifiable health information should obtain patient approval for any use or release of personal health information beyond the core functions required for the service sought by the

individual. This notice needs to be easily identifiable and easily understandable by the individual consumer. The Task Force does not want to impose additional burdens on providers, payers and other covered entities and the Task Force agreed that covered entities that follow HIPAA guidelines on the content of notices and consent forms would meet the requirements of the Iowa principles. Again HIPAA requires a signed approval from patients for all uses of information except some marketing and research purposes.

The Iowa Insurance Division is currently seeking to adopt privacy of consumer health information regulations. These regulations from a National Association of Insurance Commission model were drafted in response to requirements set forth in Title V of the Gramm-Leach-Bliley Act that was signed into law by President Clinton in November 1999. The proposed regulations provide protection for health information about consumers held by insurance companies, agents, and other entities engaged in insurance activities. In general, the regulations require insurers to notify consumers about the insurer's privacy policies and obtain affirmative consent from consumers before sharing protected health information with any other party. There are exceptions to the general rule so that information can be disclosed for legitimate business purposes, such as claims handling, underwriting, and fraud investigation, and for legal and regulatory purposes. The Iowa Privacy Task Force is supportive of the intent of the Iowa Insurance Division and believes that the proposed regulations are consistent with this principle.

4) Privacy protections should follow personally identifiable health or financial information as it moves from one entity to another.

Health information typically passes through many hands during the course of "core" health treatment and payment functions. For example, a physician office may send patient visit information to a billing service that handles its insurance claims. This billing service may send the completed claim form electronically through one or more claim clearinghouses on its way to an insurance company. The insurance company may, in turn, use an outside company for data processing. This principle suggests that each of these entities would be bound by the requirement to notify consumers of any non-core use of the personally identifiable data they handle. Similarly, if a patient agreed to use of personal data for medical research, the medical research organization would need to seek approval for re-release of the information for another purpose.

Two concerns were voiced on this principle in the Task Force. First is a concern about creating multiple levels of approval requirements. A key to this issue is how "core" functions are defined. If all of the functions listed in the first example above are considered core, then patient approval may not be required at all, or it may be required only at the physician office for release of data for payment.

A second concern is for liability for downstream use. In other words, is the physician liable if the data processing organization in the example miss-uses data? Under proposed HIPAA rules, if a health insurance company outsources its data processing function, the data processing organization is included only through contract with the health insurance company. Under the principles proposed here, the data processing

company is covered directly. This should reduce liability of covered entities for the behavior of their business partners, since these business partners would be covered directly by Iowa policy. .

A key issue is the release to business partners such as disease management companies. The group did agree that release of personally identifiable information to many business partners involved in core activities, such as billing agencies, clearinghouses and data processing companies would not require additional approval.

Employers noted concerns about their fiduciary obligations under workers compensation laws. These laws require employer involvement and knowledge of claims.

5) Personally identifiable health information should be handled in a manner so as to protect its confidentiality and necessary information shared on a need to know basis.

This principle is intended to limit the number of persons seeing personally identifiable health information on a need to know basis. It suggests that even within an organization (a physician office, hospital or health plan) such information should be shared only with those persons with a need to know and only the minimum amount of information required to perform the particular function.

This implies that the receptionist in a doctor's office should not have access to the content of patient records. The laboratory in a hospital may not need to know the patient's name (an identifying number or bar code may be used instead). An insurance agent would not be provided with a report on high dollar claims that includes patient names. Some providers indicate that such processes are in place already. Others are concerned that these measures would be difficult to implement. The Task Force concluded that all providers and other covered entities should use their best efforts to limit the use of personally identifiable information on a "need to know" basis to the greatest extent practicable.

This principle is not intended to hamper the free flow of information among health professionals treating a patient. Nor it is intended to prevent a patient from authorizing a second treatment professional to have access to information held by a first treatment professional or for a patient to authorize access to personal health information by a relative or other caregiver.

6) Organizations handling personally identifiable health information should have a balanced and objective review process for use of such information in research.

Federal regulation requires health care providers to use an Internal Review Board process for certain types of formal medical research. However, this may not cover all types of research conducted in health services organizations and these rules do not cover research by health plans and other entities. The Task Force recommends that other covered entities that are involved in research (including health plans, pharmacy benefit management companies, disease management companies and others) follow the Internal Review Board processes required for providers and

medical research organizations.

7) Personally identifiable health information should not be released to law enforcement agencies without approval of the patient or as required by law.

Task Force members supported this principle and indicated that it reflects current practice.

8) Health privacy protections should complement existing anti-discrimination laws.

The Task Force agreed with this principle, but there were differences of opinion on implementation. Much of the discussion centered on employer access to personal health information. Consumer representatives were concerned that employer access to health information could result in job discrimination. An example used was a plumber with a back problem that the plumber viewed as minor, but the employer viewed as an impediment to doing the plumbing job. Employers responded saying that they need to know physical limitations of employees in order to assign job duties safely. Many employers have extensive access to personal health information through health, disability and workers compensation insurance programs. HIPAA regulations suggest that employers must limit their use of health information to administration of health programs and to making reasonable accommodations under the Americans with Disability Act. HIPAA does not cover worker's compensation programs and it is the intent of the Task Force for these principles to cover all uses of health information including workers' compensation.

Financial Information Privacy Principles

1) Iowa financial information privacy policy should weigh the costs and benefits of the policy for individual persons and covered entities and its impact on the economy of Iowa and freedom of the press. Iowa financial information privacy policy should also consider existing requirements under state or federal law.

Information privacy policies must seek to balance two important and sometimes competing needs. It is clear from public opinion polls in Iowa and elsewhere that many citizens are deeply concerned for their personal privacy. At the same time, the free flow of information is critical to a thriving and efficient economy. Moreover, individual citizens do not all agree on the acceptable level of privacy. For example, direct consumer solicitations that target individual consumers based on that individual's spending habits are considered an invasion of privacy by some consumers and a convenience by others. Iowa policy needs to recognize these competing needs and perspectives and seek a balance that allows for economic growth while protecting essential citizen privacy.

2) Iowa financial information privacy policy should cover a broad definition of personally identifiable financial information.

The Iowa Privacy Task Force has identified a broad range of information that it

believes should be covered by an Iowa privacy policy. A list of information that should be covered is included in Appendix E. This list is meant to be comprehensive and at the same time it may not be exhaustive. Nevertheless, this list should provide policymakers with a good indication of the types of information the Task Force believes should be addressed.

3) Individuals should be given notice of the privacy policies of covered entities to whom they disclose personally identifiable financial information if the entities disclose such information to affiliates and nonaffiliated third parties. There may be other situations where notice of privacy policies or practices is also appropriate.

This principle is somewhat different than Gramm-Leach-Bliley. The Iowa Privacy Task Force recommends that Iowa policy cover a variety of entities that are not covered by GLB. This principle would be applied to these additional entities as well. For example, if a retail store were to sell information about the credit card purchases of an individual to an affiliate or an unrelated third party, this principle would require the retail store to notify the individual of this practice. Similarly, if a college were to disclose student or parent financial information to affiliates or an unaffiliated third party, the college would be subject to the same requirements.

In addition, the Task Force policy does not require covered entities to disclose privacy policies unless the entity discloses financial information to affiliates or non-affiliated third parties. GLB requires that financial institutions notify customers of their privacy policies regardless of whether or not the entity discloses personal financial information to any other entity. The Task Force chose this approach because of the broad scope of entities covered by this proposed policy. The Task Force did not wish to require that retail stores, for example, provide notice of privacy policies unless they are disclosing personally identifiable financial information to affiliates or nonaffiliated third parties. The Task Force was conscious of this difference with GLB and a majority of members voted to keep the principle as stated rather than adopt language that is strictly consistent with GLB.

Some members of the Task Force would prefer to see broader notification policies. Some consumer members would like to see notice of privacy policies regarding any use of personally identifiable financial information beyond what is required for the completion of the specific purchase or transaction that the individual citizen has initiated with a covered entity. Business representatives on the Task Force vigorously opposed any notice requirements on use of information within the covered entity itself.

The survey of a statistical sample of 207 Iowa residents indicates that many Iowans are concerned about certain uses of information. For example, ninety-seven percent (97%) of individuals surveyed agree or strongly agree that businesses that share or sell the names, addresses and phone numbers of their customers to other businesses should be required by law to notify their customers of this practice. Sixty-six percent (66%) of survey respondents do not agree that businesses like retail stores should be allowed to use the names and addresses on checks written by their customers to update their mailing lists. Ninety percent (90%) agree that businesses that do use check information to update mailing lists should be required by law to notify their customers of this

practice.

On other issues, consumers were more open to information practices of businesses. Sixty-nine percent (69%) of survey respondents believe that banks and insurance companies should be allowed to send their regular customers information about other products or services that might be valuable to them, while only thirty percent (30%) do not. Forty-six percent (46%) of respondents who have used a credit card are not concerned about anyone tracking the types of purchases they make with their credit cards, while thirty-seven percent (37%) of individuals surveyed were somewhat or very concerned.

Sixty-nine percent (69%) of Internet users surveyed did not think that businesses should use website registration information to market the businesses own products or services to them. Fifty-five percent (55%) of Internet users are somewhat or very concerned about their Internet activities being tracked and sold for marketing purposes. Nearly ninety-two percent (92%) of Internet users do not think that sale or disclosure of Internet activity records should be allowed.

4) Notice of privacy policies of covered entities should include:

   a) A description of the types of non-public personal financial information collected, the types of information disclosed and the types of parties to which this information is disclosed.

   b) A description of the steps the entity will take, if any, to attempt to maintain the security of non-public personally identifiable financial information.

   c) Information on options for individuals to restrict disclosure of non-public personally identifiable financial information to affiliates and non-affiliated third parties.

   d) Language that is plainly written so that such notices may be read and understood by average persons.

   This description of the content of privacy notices is intended by the Task Force to be consistent with the notices required under GLB[4]. Business members of the Task Force are particularly concerned that Iowa notice requirements not differ from federal notice requirements. Businesses that are multi-state in scope are concerned that if notice requirements vary by state, the cost of complying with these notice requirements will escalate. Even businesses whose operations and sales are entirely located in Iowa are concerned that differing federal and state notice requirements will complicate and raise the cost of the notice process.

   The content of privacy notices as outlined in parts a through d of this principle responds to the concerns of Iowans as indicated in the consumer survey. Consumer members were sympathetic with the argument that Iowa privacy notices should not vary from those required by federal law, but, as noted above, some consumer

[4] The Task Force believes that this principle is also consistent with the NAIC Model Act, but the Task Force did not study this Model Act in detail and did not specifically endorse the contents of the Model Act.

members wished to see notice requirements in many situations where notice is not required under GLB. This desire for broader notification was echoed in the consumer survey.

The Task Force also acknowledged that the vehicles for notice requirements might vary depending on the type of business. While financial institutions generally are required to provide written notices to each customer, retail establishments might only be required to post a notice if they disclose non-public personal financial information to affiliates or unrelated third parties.

Consumer members of the Task Force noted two concerns about the content of privacy notices. First, recent research[5] suggests that many financial privacy notices are too complex and written at a reading level that is too difficult for many consumers. While it is recommended that materials written for the general public be at the junior high school reading level, privacy notices being used by some financial institutions are written at a college reading level or higher. The Attorney General's office reported receiving calls from consumers expressing concern and a lack of understanding of privacy notices. In one instance, the office received a call from a County Sheriff on behalf of an elderly Iowan who was so frightened by a privacy notice that he thought someone was try to steal his personal information. Consumer members suggested that the Iowa financial privacy policy include consideration of mechanisms for attempting to ensure that the privacy policies of covered entities be written in simple language, understandable to average persons. Consumer members also expressed concern that some companies have been unfairly attempting to get customers not to opt out of third party information sharing by including tricky phrasing. For example, double negatives have been used so that consumers cannot reasonably determine how to opt out. Other notices require consumers to check a box indicating that they understand that they will not be receiving information about products and services that might benefit them as a condition of opting out.

On the other hand, financial institutions that are currently distributing privacy notices report that they have had few complaints that the notices are hard to understand[6]. Task Force members were also concerned whether privacy notices might create unintended obligations for covered entities. If privacy notices are phrased in simple language, will they be more open to various interpretations? Could these various interpretations hold covered entities to a higher standard than they intended or is required by law? This concern would suggest that privacy notices should provide a large amount of detail. While extensive detail can be presented in a simple and clear way, more detail will probably reduce the perceived readability of the document.

[5] Hochhauser, Mark, Ph.D., "Lost in the Fine Print: Readability of Financial Privacy Notices", posted on the Privacy Rights Clearinghouse Website, April, 2001.
[6] "Opt-Outs: Much Effort, Few Takers," *American Banker*, April 27, 2001.

5) When notifications of privacy policies of covered entities are required, these notices should be made at the time a continuing relationship is established and at reasonable intervals or when a substantial change in the entity's privacy policy occurs.

Again, this principle is consistent with GLB, but Iowa policy should cover entities not covered by GLB. The Task Force recognized that it might be difficult for some covered entities (e.g. retail stores, hospitals, charitable organizations) to identify when a continuing relationship has been established. In these situations, the Task Force felt that notice at the time of a service or transaction would be sufficient. Further this notice might be fulfilled by posting a notice rather than providing a written copy to each individual.

The Task Force also recognized that many of the covered entities were not directly represented on the Task Force and that they should be afforded an opportunity to express their views regarding financial privacy issues. The Task Force recommends that policymakers convene public meetings to allow covered entities that were not represented on the Task Force and consumers to express their views regarding these privacy proposals.

6) The financial account numbers of individuals should not be shared with an unaffiliated third party for marketing purposes except for situations expressly permitted by state or federal law.

Financial account numbers are an important key to very sensitive personal financial information. Federal law restricts the release of such information to unaffiliated third parties except in some clearly defined situations. For example, a retail store and a credit card company may jointly sponsor and administer a credit card that is specific to the retail store. Sharing of information between these two unaffiliated parties is permissible under federal law. The Task Force would like Iowa policy to extend the general prohibition on disclosure of financial account numbers to all of the entities listed in Appendix D, not just those covered by GLB.

The survey of Iowans did not ask about all types of financial account numbers, but it did ask Iowans about credit card account numbers. Thirty-seven percent (37%) of credit card users in the survey were somewhat or very concerned that their credit card number might be used without their permission. In contrast, forty-one percent (41%) were not concerned that their credit card numbers might be used without their permission and seventy-three percent (73%) of credit card users have given their credit card number over the telephone.

7) Individuals should have a choice on whether non-public personally identifiable financial information is disclosed to non-affiliated third parties except when such disclosures are expressly permitted by state or federal law.

This principle represents the issue with the greatest amount of controversy within the Task Force. Federal law, through the GLB, requires financial institutions to give consumers an "opt out" choice when they disclose non-public personal information with non-affiliated third parties, with certain exceptions. Under an "opt-out" provision, the institution must inform the consumer of his or her right to deny use of personal information for these additional purposes. If the consumer fails to notify the institution of their refusal of this additional use, the financial institution may go ahead with this use.

Industry groups strongly prefer the "opt-out" approach. Some consumer members of the Task Force prefer an "opt-in" approach. Under an opt-in, the covered entity would not be allowed to use the information for additional uses unless the consumer affirmatively allows them to use it. In other words, under opt-out, if the consumer says nothing, the entity can go forward. Under opt-in, if the consumer says nothing, the entity may not go forward. Consumer Task Force members argue that consumers do not always read or understand their options under privacy policy disclosures. They believe that opt-in provides greater assurance that the consumer is willing to share personal information for additional uses.

Industry representatives are concerned that opt-in would be very cumbersome and expensive. They also worry that an opt-in requirement would restrict them from marketing to interested consumers who did not respond to the opt-in offer. They believe that a majority of their current and potential customer base will not pay attention to an opt-in offer, but may, in fact, want the additional services that the institution could offer. As a result, industry representatives believe that information sharing is usually beneficial and useful to the consumer and that covered entities should not be restricted in their use of information due to lack of response by some consumers.

Consumer members attempted to offer opt-in methods that would be more acceptable to business. For example, they suggested opt-in be applied only when the business relationship is first established and when policies on uses of data change. Another idea suggested was an "opt-out registry." Such a registry would allow consumers to indicate that they wish to opt-out of all additional uses of their personal financial information by any covered entity. Covered entities would be required to check the registry for consumers who did not reply to an opt-out offer from their particular organization. This is similar to the registries for telephone solicitations. However, many organizations are exempt under some state telephone registry laws, limiting their usefulness.

Consumer representatives asserted that an "opt-out registry" might offer substantial advantages for consumers who are receiving multiple privacy notices and wish to opt out of all third party information sharing without having to spend the time and resources to send opt-out notices to each of their financial institutions. Such a registry may also benefit businesses by assisting them in targeting solicitations to

customers who wish to receive them. Consumer members also suggested another alternative – limited opt-in rights for consumers regarding the sharing of certain highly sensitive types of financial information such as Social Security numbers. Less sensitive financial information would still be subject to the opt-out standard.

In addition to the "opt-out" vs. "opt-in" issue, consumer representatives and business representatives differed on the exceptions to consumer choice allowed in the GLB regulation. GLB does allow disclosure of non-public personal financial information to non-affiliated third parties without consumer choice for certain types of marketing relationships. Some consumer members would like to see these marketing disclosures subject to consumer choice and preferably in their view, an opt-in choice. Business representatives point out that smaller Iowa financial institutions often must rely on third party relationships to bring the same range of services offered by larger national institutions. These members are concerned that Iowa businesses will be disadvantaged if they must abide by stricter rules than those required by GLB.

The Task Force examined summary information on laws in other states. The actions of states following the passage of Gramm-Leach-Bliley are influenced by the different regulatory processes used to implement GLB for the insurance and banking sectors. Since the insurance industry is regulated at the state level, GLB requires that each state insurance department adopt privacy regulations. For the banking sector, which is federally regulated, each state may adopt privacy rules that are more stringent than Title V of GLB, but these rules must be approved by the Federal Trade Commission. In addition, the examination of other state laws was complicated by differences in terminology and the entities covered by each state law.

Privacy regulation is the subject of a large number of bills being considered by state legislatures across the country and will likely be the subject of many more in coming years. As of the date of this report, the Task Force is not aware of any states that have enacted information sharing standards for insurers regarding her permitted sharing of financial information that deviate from GLB. In other words, GLB standards regarding privacy notice requirements and customer rights to opt-out for certain defined financial information sharing practices by insurers are apparently being followed in all states at this time. In the banking sector, seven states have had opt-in requirements. However, the opt-in requirements of some states appear to include broad exceptions that would exempt many routine business activities. In addition, two of these states, Florida and North Dakota have amended their banking laws to conform to GLB. The regulatory situation at the state level remains very fluid at this time.

The survey of Iowans conducted by the Task Force provided strong support for a broad "opt-in" requirement. Survey respondents were asked if they agreed or disagreed with statements that described both opt-out and opt-in approaches. Seventy-eight percent (78%) disagreed or strongly disagreed with the statement that businesses should be allowed to disclose information about customers unless the customer specifically tells them not to (opt out). In contrast, ninety-four percent (94%) agreed or strongly agreed with the statement that businesses should not be allowed to disclose information about customers unless the customer specifically gives them permission (opt-in).

The Task Force noted that the Iowa survey did not attempt to measure consumer preferences if the "opt-in" approach resulted in higher prices, fewer choices or less convenience for goods or services as a result of higher marketing costs and higher costs of complying with regulation. Industry representatives cited national research suggesting that nearly nine out of ten Americans worry about the potential misuse of their personal information[7]. However, sixty one percent (61%) of respondents to a national survey considered it acceptable that businesses compile profiles of their interests and communicate offers to them.

8) The State of Iowa should take additional steps to reduce identity theft, fraudulent transactions and other crimes against personal financial integrity and privacy. Included in these steps should be:

   a) The State of Iowa should require that merchants phase out the practice of placing full account numbers on receipts of credit or debit card transactions.

      Some Iowa merchants have changed their practices to print only the last 4 digits of a credit card number on receipts. Many Iowa businesses still print the entire credit card number, however. While this change was universally recognized as a desirable change, some members were concerned about potential costs in changing cash register systems to implement this change.

   b) Merchants doing business in Iowa should be prohibited from requiring disclosure of Social Security numbers as a condition for acceptance or negotiation of a personal check.

      Under Iowa law, the recording of a credit card number or expiration date or both in connection with the sale of goods or services in which the purchaser paid by check or share draft, or in connection with the acceptance of the check or share draft is a simple misdemeanor. This principle suggests that the same type of prohibition be applied to use of Social Security numbers. The reason for this suggestion is that Social Security numbers can be used to access many types of personal information. The Social Security Administration recommends restricted use of Social Security numbers as a form of identification.

      Iowa merchants frequently collect Social Security numbers when accepting checks by recording drivers license numbers on checks. This practice is necessary in order to show that the merchant sought identification prior to accepting the check. This request for identification is generally viewed by courts as necessary "due diligence" in cases where bad checks are prosecuted. Iowa has recently enacted legislation to phase out use of Social Security numbers on driver's licenses. This change will make this recommendation easier to implement without affecting Iowa merchant's legitimate need for identification.

      This principle was generally supported by the survey of Iowans. Sixty-five percent (65%) of Iowans surveyed who have checking accounts do not have their Social Security number on their checks. However, only twenty-five percent (25%)

[7] "Privacy & American Business", a survey by Louis Harris and Associates, published in Ameritech, June 23, 1998.

of Iowans surveyed have refused to provide their Social Security number when it was requested. The Task Force believes that consumers should be very cautious in the release of their Social Security number since it is a very important financial information key.

c) The State of Iowa should continue and expand education efforts to prevent crimes associated with the financial privacy of its citizens and enhance enforcement and outreach capabilities.

The State of Iowa is currently involved in education efforts to prevent identity theft. The Task Force recommends that these activities be expanded and intensified. The Task Force further recommends the creation of a privacy ombudsman position or positions within the office of the Attorney General. The privacy ombudsman would assist victims of identity theft or other citizens who may have other privacy concerns regarding personal financial or health information and covered entities. At the same time, the Task Force would want such an ombudsman to maintain a balanced perspective between the legitimate needs of both consumers and business.

9) Government should take steps to increase its respect for the sensitivity of personal financial information that it collects. These steps should include:

a) The collection of Social Security numbers by state and local governments, subdivisions and agencies should be reviewed to determine whether, in each case, such collection is necessary and conforms to federal law.

Just as merchants should not be requiring a Social Security number to complete a sale paid for by check, state and local governments should not be requesting Social Security numbers unless required by law or absolutely necessary for the performance of a government function.

b) The State of Iowa should phase in newly issued identification numbers in place of all Social Security numbers appearing on driver's license documents and identification cards issued to its citizens.

As this recommendation was being written, the Iowa legislature passed and the Governor signed into law House File 647, a measure to phase out the automatic use of Social Security numbers on driver's licenses. New and renewing driver's license holders will be issued a new driver identification number, unless they request to use their Social Security number. This measure would help limit the circulation of Social Security numbers and reduce the opportunities for identity theft.

c) The State of Iowa should prohibit disclosure of Social Security numbers and private financial account numbers in public documents except as required by law or where the lawful custodian of the information did not request, require or otherwise solicit the placement of the Social Security number or private financial account numbers on the document.

This recommendation would prohibit government entities from disclosing Social Security numbers and private financial account numbers in public documents. Government often has this personal information about individual citizens for good and legitimate purposes. However, there are few, if any situations, where public access to records would justify the release of this sensitive information. The exception to this rule would be in cases where the government entity did not request the Social Security number or financial account information from a citizen, but the citizen has included such information in the body of a communication with a government agency. The exception recognizes that it may be very difficult to scan all public records to exclude such unrequested information.

d) The sale, for commercial profit by state and local governmental agencies or subdivisions, of personally identifiable financial information collected by government agencies should be prohibited.

This principle suggest that the Task Force believes it is not appropriate for state or local governments to make a business out of the sale of personally identifiable financial information of its citizens. At the same time, the Task Force recognizes that in cases where such information is part of the public record (e.g. taxes paid based on the sale price of a house), government units may charge fees to citizens that want access to the information that are reasonably related to the cost of storage and retrieval of such information.

e) The lawful collection and non-public storage of personal identification numbers for legitimate governmental purposes such as law enforcement, tax collection or the tracking of entitlements should not be impeded.

This principle simply recognizes that state and local governments do collect and maintain personal identification numbers for legitimate governmental purposes. Nothing in this report is intended to impede governments in their performance of these legitimate duties.

f) Every state and local government, subdivision or agency that collects personal financial information should have and post a privacy and security policy explaining what information is collected and how it is disseminated and how it is protected.

This principle simply extends the notice requirements under principle 10 to state and local governments. The Task Force believes that citizens have a right to know how government entities are using personally identifiable information.

Appendix A

Privacy Task Force Members

Health Information Work Group, Industry Representatives

Bruce Braley	Dutton, Braun, Staack, & Hellman, P.L.C.
John Brinkman	Mercy Internal Medicine
Tammy Bullock	Osterhaus Pharmacy
Connie Delaney	College of Nursing, University of Iowa
Joe DuBray	Wellmark Blue Cross & Blue Shield of Iowa
Tim Gibson	John Deere Health
Todd Willert	Story County Hospital
Charese Yanney	Guarantee Roofing, Siding, Insulation

Health Information Work Group, Consumer Representatives

Carmela Brown	Consultant, Advocacy & Government Relationships Relating to Health Care
John "Pat" Dorrian	Former Mayor of the City of Des Moines
Lynn Ferrell	Polk County Health Services
Ernie Koltis	Standardbred Owner
Jan Laue	Iowa Federation of Labor, AFL-CIO
Veena Vallyathan	Buena Vista University

Finance Information Work Group, Industry Representatives

Howard Hagen	Dickinson, Mackaman, Tyler & Hagen, P.C.
Janet Hinrichs	Des Moines Metro Credit Union
Diane Kolmer	Retired from U.S. West
Patricia McFarland	Wells Fargo Financial
Mavis Merrill	Beacon MicroCenter
Merle Pederson	Principal Financial Group
Janice Towne	TD&D Financial Services, Ltd.
Peter Voorhees	Standard Golf Company

Finance Information Work Group, Consumer Representatives

Harvey Andersen	Retired Legal Assistant/Legal Investigator
William Brauch	Iowa Attorney General's Office
Vicki Duchene	The Maytag Corp/United Auto Workers
Karl Olson	Bradshaw, Fowler, Proctor & Fairgrave, P.C.
Rahul Parsa	Drake University
Mary Riche	Self-employed Psychotherapist
Randall Wilson	Iowa Civil Liberties Union
Sharon Zanders-Ackiss	Des Moines Citizens for Community Improvement

Health Information Work Group, Ex-Officio Members

Mariette Brodeur	Counsel to the Director, Iowa Department of Public Health
Darci Frahm	Attorney General's Office
Stephen Gleason	Director, Iowa Department of Public Health
Dennis Janssen	Iowa Department of Human Services
Joel Lunde	Iowa Department of Management
Jo Oldson	Governor's Office
Therese Vaughan	Iowa Insurance Division, Department of Commerce
Susan Voss	Iowa Insurance Division, Department of Commerce

Finance Information Work Group, Ex-Officio Members

Dodie Bauman	Iowa Bankers Association
James Forney	Credit Union Division, Iowa Department of Commerce
Holmes Foster	Banking Division, Iowa Department of Commerce
Scott Galenbeck	Attorney General's Office, Iowa Insurance Division
Kay Halloran	Professional Licensing, Iowa Department of Commerce
Justin Hupfer	Director of Regulatory Affairs, Iowa Credit Union League
Donald Senneff	Banking Division, Iowa Department of Commerce
Therese Vaughan	Iowa Insurance Division, Department of Commerce

Appendix B
Iowa Privacy Task Force
Survey of Iowans

Survey Methodology

The Iowa State University Statistical Laboratory conducted a statewide telephone survey of households on behalf of the privacy task force. The research study focused on the perceptions of Iowans on issues related to privacy. The ISU Statistical Laboratory staff in consultation with the financial sub-committee of the privacy task force developed the questionnaire for the survey. The ISU Statistical Laboratory used a sample of random-digit dialing (RDD) telephone numbers provided to them by the Survey Sampling, Inc. (SSI) to reach the respondents. The target population for this survey was all Iowa residents 18 years of age or older. The questionnaire used for the survey was reviewed and approved by the financial sub-committee of the privacy task force. Trained interviewers conducted the study under the supervision of Dr. J.D. Opsomer, D.G. Anderson, and L.L. Anderson.

Of the 597 telephone numbers selected in the sample, 527 were reached, and 402 were determined to be Iowa households. The overall response rate for all potential Iowa households selected was 51.4% and the cooperation rate for households screened was 85.8% resulting in 207 completed surveys. This scientifically conducted survey and the resulting data are a statistically valid representation of the true beliefs of the Iowa population. The margin of error for this study is ±7% with 95% confidence level. For instance, this means that if a sample proportion answering a certain question affirmatively is 54%, the true percentage in the overall population has a 95% chance to be between 47% and 61%. Results for subgroups within the population (for instance, all women or all people over 50 years old) will have a larger margin of error, depending on the size of the subgroups.

Weights were used to adjust for the fact that different demographic groups might not have been represented equally in the original sample, and might have different non-response rates. The weights were computed using the U.S. 1999 Census population estimates. This is a standard methodology that yields more reliable survey estimates. For each person in the data file, the weight can be interpreted as the number of people in the target population that are represented by that observation. Therefore, the sum of the weights for all the observations will sum to the population of Iowa that is older than 18 years of age.

Click here to view the PowerPoint slide presentation.

Case ID: ___ ___ ___ **SCREENING FORM**

Right to Privacy
Screening & Respondent Selection

Telephone Number (__ __ __) __ __ __ - __ __ __ __ Screen Interviewer ID __ __

Page # _____ Screen Date __ __ / __ __ / __ __

Selected Respondent's First Name _____

Outcome:

1 = Screened & Selected
2 = Screened, Refused Interview
3 = Other _____
(Explain)

Hello, this is (your name) calling from Iowa State University in Ames. I am calling about a research study we are conducting relating to privacy issues in the state of Iowa.

(First of all, are you one of the adults (age 18 or older) who lives in this household?

1 = Yes→ **GO TO TOP OF NEXT PAGE**
2 = No → May I speak with one of the adults please?
GO TO TOP OF NEXT PAGE

IF NONE ARE AVAILABLE, ASK FOR CALLBACK TIME.)

IF NON HOUSEHOLD: **Would you tell me if I've dialed correctly? Is this (telephone number)?**

1 = Yes→ Thank you, we are trying to reach people in households so I won't need to ask you any other questions.

2 = No → I'm sorry, I must have the wrong number. I'll try dialing again. Thank you. **[REDIAL NUMBER. IF SAME NUMBER IS REACHED, RECORD AS BAD CONNECTION.]**

(Hello, my name is (INT NAME). I am calling for Iowa State University in Ames about a research study we are conducting relating to privacy issues in the state of Iowa.)

Your household was selected at random to be contacted for this study. Before I ask any questions, I want to assure you that any information you provide will be kept strictly confidential by the researchers at Iowa State University. Also, if you feel any questions are too personal, you have the right to refuse to answer them.

In order to determine if anyone in your household is eligible to be included in our research study, I need a little information about your household.

S1. **First, can you tell me if I have dialed correctly? Is this (<u>telephone</u> <u>number</u>)?**

1 = Yes

2 = No → I'm sorry, I must have the wrong number. I'll try dialing again. Thank you. **[REDIAL NUMBER. IF SAME NUMBER IS REACHED, RECORD AS BAD CONNECTION.]**

S2. **Is this a residential phone line?**

1 = Yes

2 = No → I'm sorry, we are trying to reach people in households so I won't need any further information.

S3. **How many adults, who are 18 years or older, currently live in your household?**
__ __ adults [IF NONE, THANK RESPONDENT & EXIT CASE.]

a. What is the first name (or initial) of each of them, beginning with the oldest one?

b. RECORD GENDER. ASK IF UNSURE: Is (name) male or female?

(a) First Name	(b) Gender M	F
1.	1	2
2.	1	2
3.	1	2
4.	1	2

IF MORE THAN ONE ADULT, USE RANDOM CHART TO SELECT ONE. CIRCLE NUMBER OR NAME OF SELECTED RESPONDENT.

S4. **According to our scientific procedure, [NAME] has been selected for the study. (ASK IF NECESSARY: Are you [NAME]?)**

1 = Yes, Speaking with selected person
2 = No, Not speaking with selected person GO TO S6 NEXT PAGE

S5. **Because you have been selected to represent your household, I would like to interview you over the phone for about 5 to 10 minutes. As I mentioned, this research study relates to privacy issues.**

Is now a good time for you?

1 = Yes → **GO TO INTERVIEW Q1.**
2 = No → **IF CALLBACK NEEDED, SET APPOINTMENT.**
IF REFUSES OR UNABLE, RECORD AS NONRESPONSE.

S6. Is (he/she) at home now?

1 = Yes → May I speak to (him/her)? GO TO S8.
2 = No → When would be a convenient time for me to call back and talk to (NAME)? [SET APPOINTMENT] **We'll call back then to discuss the study with (him/her). Iowa State University appreciates your time today.**

S7**.** **(**WHEN SELECTED PERSON COMES TO THE PHONE:)
Hello, my name is (INT NAME). I am calling for Iowa State University in Ames about a research study we are conducting relating to privacy issues in the state of Iowa. You have been selected to represent your household in this study, and I would like to interview you over the telephone for about 5 to10 minutes.

Is now a good time for you?

1 = Yes → First I want to assure you that any information you provide will be kept strictly confidential by the researchers at Iowa State University. Also, if you feel any questions are too personal, you have the right to refuse to answer them. **GO TO INTERVIEW Q1.**

2 = No → **IF CALLBACK NEEDED, SET APPOINTMENT.**

IF REFUSES OR UNABLE, RECORD AS NONRESPONSE.

ID # __ __ __

Final Disp:_____

Right to Privacy Questionnaire

Respondent Name:_____ Interviewer ID:__ __

Phone # __ __ __ - __ __ __ - __ __ __ __ Int Date:__ __/ __ __/ __ __

Length:_____

Respondent Talked To? Yes No

Day	Date	Time	Talked To	Disp	Comments	Int ID

NA	No Answer	AM	Answering Machine	CB	Call Back	REF	Refused Interview
BZ	Busy	OTH	Other (Explain)	APT	Firm Appointment	40	Completed Interview

Hello, my name is (INT NAME). I am calling for Iowa State University in Ames about a research study we are conducting relating to privacy issues in the state of Iowa. You have been selected to represent your household in this study, and I would like to interview you over the telephone for about 5 to10 minutes.

Is now a good time for you?

1 = Yes → First I want to assure you that any information you provide will be kept strictly confidential by the researchers at Iowa State University. Also, if you feel any questions are too personal, you have the right to refuse to answer them.

2 = No → **IF CALLBACK NEEDED, SET APPOINTMENT.**
IF REFUSES OR UNABLE, RECORD AS NONRESPONSE.

Right to Privacy Questionnaire

A. Experiences.

First I have a few questions about your experiences with privacy issues.

A1a. Have you ever had a specific problem with a bank, insurance company, or other business that did not keep your financial information private (confidential)?

1 = Yes
2 = No → **GO TO Q. A2a**

A1b. What happened?

A2a. Have you ever had a specific problem with a hospital or doctor's office that did not keep your medical information private (confidential)?

1 = Yes
2 = No → **GO TO Q. A3a**

A2b. What happened?

A3a. Has any professional that you consulted with, such as an attorney, accountant, or investment counselor, ever shared your personal information with others or used it inappropriately?

1 = Yes
2 = No → **GO TO Q. B1**

A3b. Who did this and how was the information used?

B. Personal Activities.

B1. Do you currently have a credit card?

1 = Yes → **GO TO Q. B3**
2 = No

B2. Have you ever had a credit card?

1 = Yes
2 = No → **GO TO Q. B6 (next page)**

B3. How often have you given your credit card number to someone over the phone, either for purchases or donations? Would you say . . .

1 = never,
2 = seldom,
3 = occasionally,
4 = often, or
5 = very often?

B4. How concerned are you that your credit card number might be used by someone to charge items without your permission? On a scale of 1 to 5, where 1 means that you are not at all concerned and 5 means that you are very concerned, what number would you choose?

Not at all concerned				Very Concerned
1	2	3	4	5

B5. How concerned are you that your credit card number might be used by someone for other purposes, such as tracking the types of purchases you make?

(On a scale of 1 to 5, where 1 means that you are not at all concerned and 5 means that you are very concerned, what number would you choose?)

Not at all concerned				Very Concerned
1	2	3	4	5

B6. Do you have your Social Security number printed on your personal checks?

1 = Yes
2 = No

B7. Have you ever refused to provide a business with your Social Security number when it was requested?

1 = Yes
2 = No

C. Internet Use & Concerns.

C1. Have you ever used the Internet?

1 = Yes
2 = No → **GO TO SECTION D**

C2. Do you use it for work, for personal use, or both?

1 = Work only
2 = Personal only
3 = Both

C3. Some Websites ask you to register with the site by providing personal information such as your name and e-mail address. Do you think that businesses should be allowed to use this information to market their own products or services?

1 = Yes
2 = No

C4. Do you think businesses should be required to ask your permission before they can share or sell this information to other businesses?

1 = Yes
2 = No

C5. Internet Service Providers can track which Websites are visited by an individual and sometimes this information is sold to interested businesses who use it for marketing purposes.

Are you concerned about this practice? On a scale of 1 to 5, where 1 means that you are not at all concerned and 5 means that you are very concerned, what number would you choose?

Not at all concerned				Very Concerned
1	2	3	4	5

C6. Do you think Internet Service Providers should be allowed to share or sell that information to interested businesses?

1 = Yes
2 = No

C7. Have you ever purchased anything over the Internet using your credit card?

1 = Yes
2 = No → **GO TO SECTION D, next page**

C8. Have you purchased items from more than one Website?

1 = Yes
2 = No

C9. When you make purchases on the Internet, how concerned are you that your credit card number might not be kept secure? On a scale of 1 to 5, where 1 means that you are not at all concerned and 5 means that you are very concerned, what number would you choose?

Not at all concerned				Very Concerned
1	2	3	4	5

D. Business Concerns.

D1. Next I have some questions about what you think businesses should be allowed to do with personal information that you give them. I will read a list of statements and please tell me if you Strongly Disagree, Disagree, Agree, or Strongly Agree with each one.

	Here's the first one.	**Strongly Disagree**	**Dis-agree**	**Neutral**	**Agree**	**Strongly Agree**
a.	Businesses like banks and insurance companies should be allowed to send their regular customers information about other products or services that might be valuable to them.	1	2	3	4	5
b.	Businesses like retail stores should be allowed to use the names and addresses on checks written by their customers to update their mailing lists.	1	2	3	4	5
c.	Businesses that update their mailing lists by using information from customers' checks should be required by law to notify their customers of this practice.	1	2	3	4	5
d.	Businesses that share or sell the names, addresses and phone numbers of their customers to other businesses should be required by law to notify their customers of this practice.	1	2	3	4	5
e.	Businesses that share or sell the names, addresses and phone numbers of their customers to other businesses should be required by law to obtain permission from their customers.	1	2	3	4	5
f.	Businesses should be allowed to share or sell contact information about their customers, such as names, addresses, and phone numbers, unless a customer specifically tells them not to.	1	2	3	4	5
g.	Businesses should **not** be allowed to share or sell contact information about their customers (such as names, addresses, and phone numbers) unless their customers specifically give them permission.	1	2	3	4	5

D2. How confident are you that banks and other financial institutions keep your personal information secure? Are you very confident, somewhat confident, or not confident at all?

1 = Very confident
2 = Somewhat confident
3 = Not confident at all

D3. How confident are you that doctors' offices and hospitals keep your personal information secure? (Are you very confident, somewhat confident, or not confident at all?)

1 = Very confident
2 = Somewhat confident
3 = Not confident at all

D4. How confident are you that retail stores keep your personal information secure? (Are you very confident, somewhat confident, or not confident at all?)

1 = Very confident
2 = Somewhat confident
3 = Not confident at all

D5. Next I will read a list of issues relating to privacy. Please tell me how concerned you are about each of these issues by using a scale from 1 to 5, where 1 means not at all concerned and 5 means very concerned.

	How concerned are you . . .	**Not at all Concerned**				**Very Concerned**
a.	that businesses you provide with personal financial information might sell or share that information with other businesses without your permission?	1	2	3	4	5
b.	that professionals you work with, such as attorneys, CPAs, or investment counselors, might share your personal financial information with others without your permission?	1	2	3	4	5
c.	that the State of Iowa puts Social Security numbers on Driver's Licenses?	1	2	3	4	5
d.	that more and more information about individual people is being gathered and shared without their knowledge or permission?	1	2	3	4	5
e.	that information about your purchases, group memberships, or interests might be sold to businesses for marketing purposes?	1	2	3	4	5

D6a. Do you think that current Iowa laws adequately protect people from the fraudulent use of personal financial information?

1 = Yes → **GO TO SECTION E**
2 = No

D6b. What is your biggest concern? (OPEN ENDED)

E. Demographics.

E1. Finally, I have a few background questions about you.
What is your current age, as of today?

__ __ Years

E2. RECORD GENDER. ASK IF UNSURE: Are you male or female?

1 = Male
2 = Female

E3. What is the highest level of education you have completed?

11 = Eleventh grade or less (PROBE FOR GED)
12 = High School (includes GED)
13 = Vocational or technical diploma/certificate
14 = Some college but no Bachelor's Degree
16 = B.A., B.S., or equivalent
18 = Graduate Degree, Master's, Ph.D., M.D., etc.

E4. Do you currently live . . .

1 = in a rural area,
2 = in a small town of less than 5,000
3 = in a town or city from 5,000 up to 20,000
4 = in a city from 20,000 up to 100,000
5 = or in a city of 100,000 or more?

That's all the information we need for our study.
Iowa State University thanks you for your time (today/this evening).

TIME: __ __ : __ __ (am / pm)

Appendix C

Summary of Iowa and Federal Privacy Laws and Regulations

General Principles

1. The State of Iowa should adopt a policy regarding the privacy of citizens' personally identifiable health or financial information.

A. Existing state and federal laws address the privacy of personally identifiable health and financial information and set a federal standard. Refer to Attachment A, a listing of some of the existing state and federal privacy laws and Attachment B, a copy of the November 1, 2000 memo from Bill Brauch regarding Privacy Protection for Iowans.

2. Implementation of Iowa's health and financial privacy policies should include a full range of options, such as legislation, market-based and educational solutions, enforcement and other appropriate means.

3. Iowa privacy policy should cover all persons or entities that hold, handle, store or transfer personally identifiable health or financial information.

A. Fed Law. 45 CFR 160.102 (a) (1-3) (HHS regs). The rules apply to health plans, health clearinghouses, and health care providers who conduct certain financial and administrative transactions and who transmit any health information in electronic form.

B. State law. Public hospital and medical records are confidential. Iowa Code sec. 22.7 (2). HMO's are required to hold provider communications confidential. Iowa Code sec. 514B.30. Practicing attorneys, counselors, physicians, physician assistants, mental health professionals and their clerks are required to keep all professional communications confidential. Iowa Code sec. 622.10.

C. NAIC Model. Sec. 2. Applies to all nonpublic personal financial and health information held by licensees of the insurance division.

4. Release or disclosure of health or financial information that is not personally identifiable or that is legally obtained from public sources is acceptable.

A. Fed Law. 45 CFR 164.514 (b) (HHS regs) Health information that does not identify an individual is not protected from either use or disclosure of the information. Examples include de-identified or encrypted information. GLB governs only the treatment of nonpublic personal information. 12 CFR 40.1.

B. State law. The Iowa Open Records law (Iowa Code Chapter 22) provides for general access to public records held by governmental bodies subject to specific limitations applicable to confidential records identified in sec. 22.7. In addition, medical research into the causes and treatment of substance abuse is addressed in Iowa Code sec. 125.37(2). However, information generated from such studies must be published in a manner that does not disclose patients' names or other identifying information.

C. NAIC Model Sec. 2. The law applies only to nonpublic personal health information, which, by definition, excludes public information.

5. Individuals should have a reasonable right to access personally identifiable health or financial information held by covered entities, the right to request corrections of inaccurate health or financial information.

A. The Fair Credit Reporting Act regulates a consumer's access to his or her own consumer reports. 15 USC sec. 1681 et seq.

B. State Law. 653 IAC 12.4 (32), (33) provides for the timely transfer of medical records to another physician upon request of the patient. AMA Ethical Opinion E 7.02 provides that upon a request, a patient should be given a copy or summary of their medical records.

C. NAIC Model. The model is silent on this concept.

6. There should be strong and effective remedies and enforcement procedures for privacy violations including meaningful penalties where appropriate.

A. Fed Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (secs. 1176 and 1177) establishes civil and criminal penalties. 12 CFR 40.17 (GLB) defaults to state law for imposition of penalties, including both civil and criminal penalties.

B. State Law. Iowa common law recognizes a private cause of action for the improper use or disclosure of health information.

C. NAIC Model. Sec. 24 subjects violation of the law to the state's unfair trade practices law.

7. Government should assist covered entities in maintaining high levels of security to ensure privacy of nonpublic personally identifiable health or financial information in their possession.

8. Covered entities handling personally identifiable health or financial information should adopt privacy and security policies and procedures for the collection, storage, access, use and disclosure of such information.

A. Fed Law. 45 CFR 164.530 (HHS regs) imposes a number of administrative duties on covered entities including a requirement to appoint a privacy officer and to have in place appropriate administrative, technical and physical safeguards to protect the information. 12 CFR 40.10-.11 (GLB) limits disclosure, redisclosure and reuse of nonpublic personal information

B. State Law. The insurance commissioner has rule making authority to require this notice and intends to do so by promulgating a rule adopting the NAIC model.

C. NAIC Model. Sec. 17 requires the authorization from the individual prior to use of the information.

<u>Health Information Principles</u>

1. Personally identifiable health information should be defined broadly to include all individual patient demographic information, individual and family health history, individual diagnosis, treatment, diagnostic tests or images, professional treatment notes and individual health insurance coverage information.

A. Fed Law. 45 CFR 164.501. (HHS regs) The law applies to individually identifiable health information, transmitted or maintained in any medium. The information protected is defined broadly to include all health information that relates to physical or mental health conditions. See also 12 CFR 40.3 (n) (1) (GLB) which defines broadly nonpublic personal information.
B. State law. Birth Defects Institute maintains a confidential central registry. Iowa Code sec. 136A.6. The Department of Public Health maintains a confidential central registry for brain injuries. Iowa Code sec. 135.22. Mental health information disclosure prohibited. Iowa Code sec. 228.2. HIV related information must be kept confidential. Iowa Code sec. 141A.9.
C. NAIC Model. Sec. 4 (U) Protects any information that could be used to identify an individual.

2. Individuals should be given notice of the core and non-core uses of personally identifiable health information. Core is that use required in order to obtain health services, for payment for health services, for the routine operations of a health service provider or payer, or as required by law. Non-core uses include all other uses of personally identifiable health information.
A. Fed Law. 45 CFR 164.520 (a) (HHS regs) requires an individual be given notice of the uses and disclosures of protected health information. 12 CFR 40.4-.6 (GLB). Requires both an initial and an annual privacy notice be given.
B. State Law. The insurance commissioner has rule making authority and intends to require this notice by promulgating a rule adopting the NAIC model.
C. NAIC Model. Secs. 5, 6 and 7 contain parallel provisions to the federal laws.

3. Individuals should have a right to decline "non-core" uses of personally identifiable health information and should be notified of that right, unless release of such information is required by law.
A. Fed Law. 45 CFR 164.522 (HHS regs) entitles an individual to restrict a covered entity's use of protected health information. See also 12 CFR 40.7 (GLB) for an individual's rights to restrict the use of the individual's information. The final regulations also limit the ability of nonaffiliated third parties who receive NPI to reuse or redisclose it in a manner inconsistent with the providing entity's authority to use or disclose the information. Financial institutions that receive such information from nonaffiliated third parties are similarly limited by the regulations in their ability to reuse or redisclose NPI.
B. State Law. The insurance commissioner has rule making authority to require this notice and intends to do so by promulgating a rule adopting the NAIC model.
C. NAIC model. Sec. 17 requires an insurer to obtain an authorization from an individual before protected health information is disclosed.

4. Privacy protections should follow personally identifiable health or financial information as it moves from one entity to another.
A. Fed Law. 45 CFR 164.504 (e) (2) (HHS regs) governs the conduct of health plans, health care clearinghouses and health care providers. In addition, 45 CFR 160.102 requires a covered entity to obtain a written assurance that a business associate safeguard the information. 12 CFR 40.10-11 (GLB) limits disclosure, redisclosure and reuse of nonpublic personal information.

B. State Law. The insurance commissioner has rule making authority to require these protections and intends to do so by promulgating a rule adopting the NAIC model.
C. NAIC Model. Sec. 17 requires authorization for disclosure of this information.

5. Personally identifiable health information should be handled in a manner so as to protect its confidentiality and necessary information shared on a need to know basis.
A. Fed Law. 45 CFR 164.502. (b) (1) and 45 CFR 164.514 (d) (1) (HHS regs) The law requires an entity to limit disclosure of the information to the minimum necessary to accomplish the intended purpose of the request. It also addresses safeguards in the handling of this information. Also 45 CFR 164.504-.514 (HHS regs) governs the uses and disclosures of the information and 12 CFR 40.10-.11 (GLB) limits disclosure, redisclosure and reuse of nonpublic personal information.
B. State law. Iowa Code sec. 228.7 provides specific safeguards in the handling and disclosure of mental health information by mental health providers to third party payers and peer review organizations. Sec. 228.8 further describes limitations on the disclosure of mental health information to family members. Iowa Code sec. 136A.6 authorizes the maintenance of a central registry of information relating to genetic disorders and birth defects and specifically provides such information shall remain confidential pursuant to Iowa Code sec. 22.7 (2) (Open Records). Iowa Code sec. 125.37 (1) directs that chemical substance abuse records shall remain confidential and are privileged to the patient. Finally, Iowa Code sec. 125.93 provides that records related to the identity, diagnosis, prognosis or treatment of a person committed for substance abuse treatment are confidential pursuant to sec. 125.37 and federal regulation under the Drug Abuse Office and Treatment Act (21 USC sec. 1175) and the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act (42 USC sec. 4582).
C. NAIC Model. Sec. 17 requires the authorization from the individual prior to use of the information.

6. Organizations handling personally identifiable health information should have a balanced and objective review process for use of such information in research.
A. Fed Law. 45 CFR 164.512 (i) (HHS regs) contains the requirements that must be met prior to using the information for research purposes.
B. State law. Birth Defects Institute maintains a confidential central registry. Iowa Code sec. 136A.6. The Department of Public Health maintains a confidential central registry for brain injuries. Iowa Code sec. 135.22. Mental health information disclosure prohibited. Iowa Code sec. 228.2. HIV related information must be kept confidential. Iowa Code sec. 141A.9.

7. Personally identifiable health information should not be released to law enforcement agencies without approval of the patient or as required by law.
A. Fed Law. 45 CFR 164.512 (HHS regs) lists the circumstances under which such information must be disclosed to governmental agencies, including law enforcement. Unless expressly permitted by applicable law or a signed authorization, protected information may not be disclosed to such government

agencies including law enforcement. 12 CFR 40.15 (a) (4) (GLB) addresses information which must be disclosed to law enforcement.

B. State Law. Iowa Code sec. 622.10 limits the situations where disclosure of this information may occur. See also Chapter 228 Mental health.

C. NAIC Model. Sec. 17.B permits the disclosure for purposes of determining fraud, misrepresentation or criminal activity.

8. Health privacy protections should complement existing anti-discrimination laws.

A. Fed Law. 45 CFR 164.530 (g) (h) (HHS regs) prohibits a covered entity from intimidating or retaliating against any individual for exercising any right created under the law. See also 45 CFR 164.502 (j) for the whistleblower protections. 12 CFR 40.17 (GLB) preserves from preemption state law which includes protections against discrimination.

B. State Law. Iowa Code sec. 507B.4 (7) prohibits unfair discrimination. Iowa common law recognizes liability for misuse of information through discriminatory practices in employment and health insurance, among numerous other instances.

C. NAIC Model. Sec. 23 specifically prohibits discriminating against an individual who has chosen not to allow the release of personally identifiable health information.

Appendix "C"
Attachment "A"
Listing of Some of the Existing Iowa and Federal Privacy Laws

The Iowa Code and Iowa Administrative Code contain protections relating to specific types of health information, such as mental health, substance abuse, and AIDS/HIV information. There are also statutes that allow for the disclosure of information to third parties. In addition, statutes and regulations relating to licensing of health care providers and other entities in the health care business as well as state-funded health care programs impose certain conditions regarding the confidential treatment of health records. Below is a listing of some of the existing state and federal statutes and regulations relating to the confidential treatment of individuals' health records. This is intended to be a survey of some of the existing laws and is not an exhaustive listing.

Iowa Laws

Mental Health and Psychological Information - Iowa Code Chapter 228;
Hospitalization of Persons with Mental Illness – Iowa Code Chapter 229

Privacy and disclosure of mental health information is comprehensively addressed under current Iowa law. Detail of the statutory protections presently in place regarding disclosure of mental health information is provided as an example of the manner in which Iowa currently addresses privacy of personal health information.

Under Iowa Code Chapter 228 (Disclosure of Mental Health and Psychological Information), mental health information of individuals receiving professional services relating to diagnosis, course of treatment, custody or care may not be disclosed by mental health professionals, data collectors, or employees or agents of such persons. Iowa Code section 228.2.

Upon disclosure of mental health information, the person disclosing the mental health information is required to enter a notation on and maintain the notation with the individual's record of mental health information, stating the date of the disclosure and the name of the recipient of the mental health information. In addition, the person disclosing the mental health information is required to give the recipient of the information a statement that informs the recipient that disclosures may be made only pursuant to the written authorization of an individual or such individual's legal representative, or as otherwise provided in Iowa Code Chapter 228, that the unauthorized disclosure of mental health information is unlawful, and that civil damages and criminal penalties may be applicable to the unauthorized disclosure of mental health information. Iowa Code section 228.2(2).

A recipient of mental health information may not disclose information received, except as specifically authorized for initial disclosure under the statute. In particular, mental health information may be disclosed in the following circumstances:

- Voluntary Disclosures: A voluntary release of information executed by the patient if the consent meets the following requirements: (1) identification of (a) information requested; (b) party to receive information; and (c) purposes for which information may be used; (2) statement advising patient of right to inspect the information at any time; (3) statement noting that waiver to release information is subject to revocation and specific conditions of such revocation; (4) length of time for which authorization is valid; and (5) date authorization is executed. Iowa Code section 228.3.

- Administrative Disclosures: (1) Release of mental health information to employees of a mental health facility or to other providers of professional services if and to the extent necessary to facilitate provision of services; (2) release of administrative information (defined as an individual's name, identifying number, age, sex, address, dates and character of professional services provided to the individual, fees for services, third-party payor name and number of patient, name and location of facility where treatment received, date of admission to facility and name of attending physician or mental health professional) for fee collection purposes (after a reasonable amount of time has lapsed and the fee has remain unpaid); and (3) scientific and data research, management audits, program or professional evaluations (without identification of the patient). Iowa Code section 228.5.

- Compulsory Disclosures: (1) Court-ordered examination; (2) civil commitment proceedings under Iowa Code Chapter 229; and (3) when the adult individual's mental or emotional condition is offered (by the individual or legal representative) as an element of a claim or defense in a civil or administrative proceeding. Iowa Code section 228.6.

- Disclosures for Claims Administrative and Peer Review: Mental health information may be disclosed, in accordance with a prior written consent of the patient or legal representative, by a mental health professional, data collector, or employee or agent of such, or a mental health facility to a third party payor or to a peer review organization if such third party payor or peer review organization has filed a written statement with the commissioner of insurance in which it agrees to: (1) instruct its employees and agents to maintain the confidentiality of mental health information and of the penalty for unauthorized disclosure; (2) comply with the limitations on use and disclosure of the information specified in the statute; and (3) destroy the information when it is no longer needed for the purpose set forth in the statute. Iowa Code section 228.7.

- Disclosure to Family Members: A mental health professional or an employee of or agent for a mental health facility may disclose mental health information to certain defined family members if all of the following conditions are met: (1) disclosure is necessary to assist in provision of care of individual; (2) family member is directly involved in care of individual; and (3) involvement of family member is verified by attending physician, mental health professional or a person other than a family member providing care

to the individual. Iowa Code section 228.8. A request for mental health information by a family member shall be in writing, except in an emergency. Unless the individual has been adjudged incompetent, the person verifying the involvement of the family member shall notify the individual of the disclosure of the mental health information. The information disclosed is limited to: (1) a summary of the individual's diagnosis; (2) a listing of medication which the individual has received and is receiving; and (3) a description of the individual's treatment plan. Iowa Code section 228.8.

- Disclosure of Psychological Test Material: A person in possession of psychological test material shall not disclose the material to any other person, including the subject to the test. Such test material shall not be subject to disclosure in any administrative, judicial or legislative proceeding. Upon request of the individual tested, the records of the test may be disclosed to a licensed psychologist designated by the individual. Iowa Code section 228.9.

Under Iowa Code Chapter 229 (Hospitalization of Persons with Mental Illness), the records maintained by a hospital or other facility relating to the examination, custody, care and treatment of any person in that hospital or facility are deemed confidential, except that the chief medical officer shall release appropriate information under any of the following circumstances: (1) information requested by licensed physician, attorney or advocate who provides the chief medical officer with a written waiver signed by the individual about whom the information is sought; (2) court order; or (3) hospitalized person or guardian signs an informed consent. Iowa Code section 229.25. Records may be disclosed by the chief medical officer for purposes of research as described below. Id. In addition, when the chief medical officer deems it to be in the best interest of the patient and the patient's next of kin to do so, the chief medical officer may release appropriate information during consultation which the hospital or facility shall arrange with the next of kin of a voluntary or involuntary patient, if requested by the next of kin. Id.

Substance Abuse – Iowa Code Chapter 125
Acquired Immunity Deficiency Syndrome (AIDS) – Iowa Code Chapter 141A
Health Maintenance Organizations - Iowa Code Chapter 514B
Open Records Law – Iowa Code Chapter 22
Hospitals – Iowa Administrative Code 481-51
Nursing Homes – Iowa Administrative Code 481-57
Other State Regulations

The Iowa Department of Public Health has implemented regulations relating to laboratories (IAC 641-12.6 (730)); pregnancy termination (IAC 641-106.3 (144)); and vital records (IAC 641-103 (144)). The Iowa Department of Human Services has issued regulations on this matter relating to mental illness (IAC 441-22 (225C)); providers of medical and remedial care (IAC 441-77.39 (225C)); medical assistance – conditions of eligibility (IAC 441-75.22 (249A)); the HAWK-I program (IAC 441-86 (514I)); health maintenance organizations (IAC 441-88.9 (249A)); and rehabilitative services (IAC 441-152 (234)). The Iowa Department of Inspections and Appeals has issued regulations

relating to birth centers (IAC 481-52 (135G)). The Iowa Department of Elder Affairs has issued regulations addressing the privacy of patient records (IAC 321-22 (231A)). The Iowa Insurance Division also has issued regulations regarding privacy of medical information relating to AIDS/HIV testing (IAC 191-15 App. III); group self-funded plans (IAC 191-35.20) (509A)); third-party payor's use of utilization review contractors (IAC 191-70.7 (565, 514F)); health insurance purchasing cooperatives (IAC 191-73.12 (75GA, CH 158)); Iowa individual health benefit plans (IAC 191-75.9 (513C)); external review (IAC 191-76.9 (78GA, SF 276)); and financial information (IAC 191-90 (505)) (described below).

Disclosure of Medical Records Without Patient's Consent

Under Iowa law, there are certain situations where the disclosure to third parties of health information relating to an individual does not require the consent of such individual.

Child Abuse: Iowa Code Chapter 232.
Dependent Adult Abuse: Iowa Code Chapter 235B.
Communicable Diseases and Sexually Transmitted Diseases: Iowa Code sections 139.2 and 140.4; IAC 641-1.2 et seq.
Wounds and Other Serious Bodily Injuries: Iowa Code section 147.111.
Medical Research:
Morbidity and Mortality Research: Iowa Code section 135.41.
Chemical Substance Abuse: Iowa Code section 125.37.
Mental Health: Iowa Code section 229.25.

Consent Statutes

Under Iowa law, there are certain situations where disclosure of health information relating to an individual may be made to a third party based on consent procedures established by statute.

- Durable Power of Attorney for Health Care: Iowa Code section 144B.7.
- Advocates - Hospitalization of Mentally Ill Persons: Iowa Code section 229.25.
- Long-Term Residents Advocates: Iowa Code section 231.42.
- Workers' Compensation: Iowa Code section 85.27.

Federal Laws

There are various federal statutes that relate to the privacy of individuals' health records. Below is a listing of certain federal statutory and regulatory requirements.

A. Medicare 42 C.F.R. section 482.24
B. Substance Abuse Drug Abuse Prevention, Treatment, and Rehabilitation Substance Act, 21 U.S.C. section 1175; 42 C.F.R. sections 2.1 and 2.2.
C. Health Insurance Portability and Accountability Act of 1996 – P.L. 104-191
D. Other Federal Laws

There are other federal laws that have potential application to the privacy of health records. The Privacy Act of 1974, 5 U.S.C. section 552a, prohibits the disclosure of records contained in a system of records maintained by the federal government. The Freedom of Information Act, 5 U.S.C. section 552, allows any person to request information in possession of the federal government, subject to certain exceptions. The Family Educational Rights and Privacy Act, P.L. 106-102 ("FERPA") provides parents of students and eligible students with privacy protections and rights for records of students maintained by federally funded educational institutions. The Clinical Laboratory Improvement Amendments Act, 42 U.S.C. section 263a and related regulations, require clinical laboratories to, among other things, disclose test results or reports only to authorized persons, as defined by state law.

D. Gramm-Leach-Bliley Act of 1999 – P.L. 106-102; Iowa Administrative Code 191-90 (effective July 1, 2001)

M E M O R A N D U M

TO: Privacy Task Force - Financial Privacy Subgroup

FROM: Bill Brauch, Director-Consumer Protection Division

DATE: November 1, 2000

RE: Privacy Protection for Iowans

At the initial meeting of the Privacy Task Force -- Financial Privacy Subgroup, I agreed to prepare a memo summarizing privacy protection under Iowa law relating to financial matters. Following is a short listing and description of Iowa law that relates to some degree to individual, financial privacy. This is not intended to be a complete list of all Iowa laws that may apply. These are listed in no particular order.

1. Ban on Unreasonable Searches and Seizures -- Iowa Constitution, article one, section 8

Similar to US Constitution.

2. Identity Theft -- Chapter 715A, Section 714.16B

Creates the offense of identity theft if a person with the intent to obtain a benefit fraudulently obtains identification information on another person and uses or attempt to use that information to obtain credit, property, or services without the authorization of the other person. "Identification information" means the name, address, date of birth, telephone number, driver's license number, nonoperator's identification number, Social Security number, place of employment, employee identification number, parent's legal surname prior to marriage, demand deposit account number, savings or checking account number or credit card number. Violation is a class "D" felony if the value of the credit, property, or services exceeds $1000. Those who violate the law may also be sued civilly by the victim for $1000 or three times the actual damages, whichever is greater, plus reasonable attorney fees and court costs.

3. Credit Card Numbers as a Condition of Accepting a Personal Check -- Section 537.8101

Prohibits requiring as a condition of acceptance of a check or share draft, or as a means of identification, that the person presenting the check provide a credit card number or expiration date, or both. Recording a credit card number or expiration date, or both, in connection with the sale of goods or services in which the purchaser paid by check or share draft, or in connection with the acceptance of the check or share draft, is a simple misdemeanor. But it does not prohibit requiring a person to display a credit card as indicia of creditworthiness and financial responsibility or as additional identification.

4. Regulation of Automatic Dialer Devices -- Section 476.57

Makes it is serious misdemeanor to use automatic dialing -- announcing device equipment for the purpose of automatically selecting or dialing telephone numbers without the use of a live operator to disseminate prerecorded messages. Exceptions include calls by nonprofit organizations; calls that do not involve the advertisement or offer for sale, lease, or rental of goods, services, or property; calls relating to payment for, service of, or warranty coverage of previously ordered or purchased goods or services; calls made by persons or organizations with a prior business relationship with the persons or organizations using the calls; debt collection calls; calls to members or employees of the organization making calls; calls made with an initial prerecorded message of a duration no longer than seven seconds prior to a live operator intercept; or, calls which involve an initial message from a live operator.

5. Prohibition of Electronic Surveillance of Telephone Use -- Chapter 808B, Section 727.8

Makes it unlawful for a person who is not a party to a communication to intercept a wire or oral communication without consent of a party to the communication. "Oral communication" means oral communication uttered by person exhibiting an expectation that the communication is not subject to interception, under circumstances justify that expectation. "Wire communication" means a communication made a whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception. A person whose wire communication or oral communication is accepted, disclosed, or used in violation of the law has a civil cause of action against any person who intercepts, discloses, or uses or procures any other person to intercept, disclose or use such communications to obtain actual and punitive damages, plus attorney fees.

6. Motor Vehicle and Driver License Records -- Section 321.11

Prohibits release of personal information in connection with motor vehicle and driver's license records. "Personal information" includes a person's photograph, Social Security number, driver's license number, address, telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver status or a person's zip code. Note: the federal law is summarized below.

7. Reports to Government Officials -- Chapter 22

Chapter 22 governs the confidentiality of records that come into the possession of, or are created by, public entities, such as the state, a county or a city. The chapter presumes records are open for public inspection unless specifically deemed confidential in chapter 22 or other law. Additionally, citizen reports to certain state agencies may be deemed confidential by the laws that specifically address those agencies.

8. Income Tax Information in Possession of Tax Preparers -- Chapter 423A

Section 423A.2 provides that a person who obtains any information in the course of or arising out of the business of preparing or assisting in the preparation of the tax return of another person may not disclose any of the information obtained. Exceptions include where the taxpayer has consented to the disclosure in writing, or state or federal law expressly authorizes the disclosure, where the disclosure is necessary to the preparation of the return, or pursuant to a court order. Violations are aggravated misdemeanors.

9. Internet "Spam" -- Chapter 714E

Chapter 714E addresses unsolicited e-mail advertisements and, in part, requires that an unsolicited e-mail include an address where recipients can write to decline future e-mail from the sender. Persons who receive unsolicited e-mails in violation of the chapter may sue the sender for monetary damages or $500, whichever is greater, plus costs and reasonable attorney fees. Internet service providers also have a cause of action if they are injured by the unsolicited
e-mails to sue and receive a minimum of $25,000, or actual damages. In addition, violations are per se violations of the Consumer Fraud Act, enforced by the Attorney General.

10. Right to get an Assigned DL in Lieu of using Social Security Number – Section 321.189(2)(c)

Provides that a citizen may ask for an assigned number other than the citizen's Social Security number as a driver's license number.

11. Mortgage Lenders Barred from Using Credit Status Info for Solicitations by an Affiliate -- Section 535A.9

The section provides that a financial institution which makes or offers to make real estate mortgage loans may not use confidential credit status information that is used for qualifying a person for the purchase of real property for solicitation purposes either directly or indirectly by an affiliate subsidiary. Violations are serious misdemeanors and aggrieved parties can file civil lawsuits to obtain actual damages and attorney fees and punitive damages of up to $1000.

12. Voter Registration Forms -- Section 48A.11

Provides, in part, that providing a registrant's Social Security number or residential telephone number on voter registration forms is optional.

13. Ban on Unlawful Debt Collection Practices -- Chapter 537

Article 7 of the Consumer Credit Code (Ch. 537) bars debt collectors from sharing information relating to a debt or debtor with a person other than the debtor or to a person who might reasonably be expected to be liable for the debt, with certain

exceptions. Those who violate the law are subject to civil lawsuits by the debtor and by the Attorney General as administrator of the Consumer Credit Code.

14. Consumer Fraud Act -- Section 714.16

This is Iowa's general consumer fraud statute. Among other things, it declares deception and unfair practices in connection with the sale or advertisement of merchandise to be unlawful. An "unfair practice" is an act or practice which causes substantial, unavoidable injury to consumers which is not outweighed by a competitive benefit. The Act is enforced through civil law enforcement actions by the Attorney General and permits our office to obtain reimbursement for consumers, enjoin unlawful acts, and obtain civil penalties and attorney fees and costs for the state. Certain practices which invade the privacy of individual Iowans may be found by a court to be unfair. This could include obtaining sensitive financial data about individuals and selling that data without notice and consent of the person who is the subject of the data. A good example is our action regarding U.S. Bancorp. All states have the equivalent of this law, but Iowa is the only state in the nation where consumers do not have a private cause of action for violations.

While the primary focus of this memo is on Iowa law, I thought it might be helpful to address some of the protection available under federal law. Federal laws that impact financial privacy include:

1. Gramm-Leach-Bliley Act -- Pub. L. No. 106-102, 113 Stat. 1338 (1999)

Summarized in detail in initial materials provided to Task Force members. The Act applies four new requirements to all financial institutions regarding privacy of customer information including that each financial institution must: (1) establish and annually disclose a privacy policy; (2) provide customers the right to opt out of having their information shared with nonaffiliated third parties (subject to many significant exceptions); (3) not share customer account numbers with nonaffiliated third parties; and (4) abide by regulatory standards to protect the security and integrity of customer information

2. Fair Credit Reporting Act -- 15 U.S.C. Section 1681 et seq.

Regulates consumer credit reporting agencies. Limits circumstances under which consumer reporting agencies may furnish consumer reports to those requesting access. Requires consumer notice and express consumer authorization in some circumstances. Regulates what may be included in a consumer report file. It regulates the dissemination and sale of consumer reports or information in consumer reports. It also regulates a consumer's access to his or her own consumer report. Enforcement is varied. The FTC may enforce as to credit reporting agencies and others, unless enforcement is specifically directed to other agencies, such as the OCC regarding national banks. States may also file civil actions against violators to obtain injunctions and damages for injured consumers. Consumers can file their own actions to recover damages of not less than $100 or more than $1000, plus attorney fees.

3. The Federal Driver's Privacy Protection Act -- 18 U.S.C. sections 2721 -- 2725

The law generally bars state motor vehicle departments from knowingly disclosing or otherwise making available to any person or entity personal information obtained by the department in connection with a motor vehicle record. The law covers information that identifies an individual, including an individual's photograph, Social Security number, driver identification number, name, address (but not the five digit ZIP code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status. The law applies to this information if it appears on or has been obtained in connection with a motor vehicle record. A motor vehicle record includes any record that pertains to a motor vehicle operator's permit, or vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles. However, the law includes a number of exceptions permitting a motor vehicle department to disclose the information in a variety of circumstances.

4. Regulation of the Use of Social Security Numbers

The Internal Revenue Code (26 U.S.C. 6109 (a)) and applicable regulations (26 CFR 301.6109-l(d)) require an individual to get and use an SSN on tax documents and to furnish the number to any other person or institution (such as an employer or a bank) that is required to provide the Internal Revenue Service information about payments to the individual. There are penalties for failure to do so. In addition, people filing tax returns for taxable years after December 31, 1994, generally must include the SSN of each dependent.

The Privacy Act regulates the use of Social Security numbers by government agencies. When a Federal, State, or local government agency asks an individual to disclose his or her Social Security number, the Privacy Act requires the agency to inform the person of the following: the statutory or other authority for requesting the information; whether disclosure is mandatory or voluntary; what uses will be made of the information; and the consequences, if any, of failure to provide the information.

If a business or other enterprise asks for a Social Security number, the person to whom the number is assigned can refuse to give it to them. However, that may mean doing without the purchase or service for which the number was requested. For example, utility companies and other services ask for a Social Security number, but do not need it; they can do a credit check or identify the person in their records by alternative means.

The Social Security Administration recommends that citizens who are asked for their SS# should ask why the number is needed, how the number will be used, what law requires the number to be given and the consequences if the citizen refuses to divulge the number, and reminds citizens that the decision whether to give out their SS#'s is strictly theirs.

5. Children's Online Privacy Protection Act -- 15 USC Sections 6501-6506

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. The new rules spell out what a web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.

6. Telephone Consumer Protection Act -- 47 USC Section 227

The Act authorized the FCC to adopt rules permitting telephone subscribers to ask telephone solicitors to put them on a “do not call” list and provide for private and government enforcement for violations. The Act also bans unsolicited faxes and has a provision similar to Iowa law regulating automatic dialer devices.

There are likely a number of other federal laws or regulations addressing privacy issues. Those listed above are several that quickly came to mind.

Appendix D

Entities to be Covered by
Iowa Financial Information Privacy Policy

a) Federal, state and local government, subdivisions and agencies
b) Banks, thrifts and credit unions
c) Mortgage lenders, finance companies, debt consolidation companies
d) Insurance companies, HMO's and employer sponsored insurance plans
e) Retailers that accept checks or credit cards or that issue credit cards or take credit card applications.
f) Utilities
g) Colleges and Universities
h) Charitable organizations
i) Health care providers
j) Real estate brokers and agents
k) Employers
l) Check cashers and payday lenders
m) Tax preparation firms, credit counselors, financial advisors
n) Debt collection companies
o) Distributors of financial information, data services and clearinghouses
p) Fraud detection organizations

Appendix E

Items Defined as Financial Information

- All personal identifiers including, but not limited to:
  - Name, postal address, phone numbers
  - E-mail addresses
  - Internet service provider screen names
  - Social Security numbers
  - Passwords for financial accounts
  - Personal identification numbers
  - Other identification tools including biometrics

- Personal income including but not limited to:
  - Wages, salary, tips
  - Interest income
  - Dividend income
  - Alimony and child support
  - Business income
  - Retirement program income
  - Social Security income
  - Insurance payments
  - Government program payments

- Personal expenditures including but not limited to:
  - Mortgage or housing rental payments
  - Retail store or wholesale purchases
  - Debt repayments
  - Insurance payments
  - Health care and other personal service expenditures
  - Any purchases made by check or credit card
  - Buying club transactions
  - Alimony and child support

- Personal assets including but not limited to:
  - Homes or other buildings
  - Investments
  - Bank account and investment account balances
  - Automobiles, boats, airplanes
  - Durable equipment
  - Retirement savings account balances
  - Government benefit program eligibility

- Personal liabilities including but not limited to:
  - Mortgages, auto loans and other indebtedness
  - Credit card balances
  - Student loans
  - Alimony and child support requirements
  - Liens or garnishments

- State and Federal income tax records

- Motor vehicle and property tax records

- Military records including military pension records

- Government benefit records including but not limited to:
  - Financial eligibility test information
  - Benefit payment history

- Employment based records including but not limited to:
  - Wages, salary, bonuses, commission or incentive payments, stock options, and tips
  - Benefit types and levels
  - Insurance claim and payment information
  - Workers compensation benefit payments
  - Pension funds, 401K and SEP contributions and balances

- Banking records including but not limited to:
  - Loan application information or information provided as a condition of other banking services.
  - Account numbers, transaction records and account balances for checking, savings, investment accounts or loan accounts.

- Credit Card information including but not limited to:
  - Credit card application information
  - Credit card numbers and PIN's.
  - Account balances
  - Purchase transaction records
  - Payment history

- Insurance policy records (whether employer sponsored, personally held or held by another person) including, but not limited to:
  - Policy numbers and descriptions
  - Premium levels and payment history
  - Insurance amounts or levels
  - Cash value in insurance policies
  - Insurance claim history
  - Insurance policy loan balances and transaction histories

- Stock brokerage or other investment company records including, but not limited to:
  - Account numbers, transaction records and account balances
  - PIN's, passwords
  - Investment mix and trading information

- Charitable contribution records

- Personal purchase records held by retail stores, credit card transaction clearinghouses, credit card companies or banks that issue credit cards or checking accounts.

- Buying club application information.

- Apartment or office rental application information.

- Financial information provided to hospitals or other health service providers in order to arrange for payment of such services.

- Information obtained by consumer use of the Internet, including but not limited to:
    - Screen names, passwords or PIN's
    - Web site browsing records
    - Advertisement browsing records
    - Any other web-click information
    - Credit card numbers
    - Retail purchase information