In general, the Ganske language may reach more entities than we are able to reach under our HIPAA regulatory authority; however, the language is so weak on key issues of medical privacy that it may actually threaten our ability to enact strong comprehensive medical privacy legislation. It would threaten enactment of strong, viable medical privacy legislation by giving members a sense that nothing more needs to be done while key sectors of the employer and business communities would be quite satisfied with the HR 10 provisions and have no interest in stronger standards.

It was Congressman's Ganske's intent that this language limit the sharing of information from insurers to their affiliates. This language does not accomplish that goal. In fact, the language is very clear that both medical and genetic information may be provided without the consent of the patient (consumer) for many purposes.

> "(a) IN GENERAL- A company which underwrites or sells annuities contracts or contracts insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death (other than credit-related insurance) and any subsidiary or affiliate thereof shall maintain a practice of protecting the confidentiality of individually identifiable customer health and medical and genetic information and may disclose such information only--
> **(1) with the consent**, or at the direction, of the customer;
> (2) for insurance underwriting and reinsuring policies, account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), *providing information to the customer's physician or other health care provider, participating in research projects*, enabling the purchase, transfer, merger, or sale of any insurance-related business, or as otherwise required or specifically permitted by Federal or State law; or . . ."

- Under (1) consent must be given by the consumer, but (2) then allows the information to be given out without consent for a whole host of purposes, many of which are not ever defined and which could be interpreted very broadly.

Other problems of this language include:

- The language will undermine HHS' rulemaking authority under HIPAA, limiting that authority to entities other than insurers because insurers would be governed by the language in HR 10.

- The language runs counter to where public health experts would want us to be and what is included in the comprehensive medical privacy bills -- permitting disclosures for public health. The Ganske language would not permit such disclosures.

- The Ganske provision creates a huge loophole with regard to research information. We

JUL.30.1999 12:24 202 690 8425 HEALTH LEGISLATION #0363 P.002/006

understand that it allows transfers of information for "marketing research." It has no standards for how medical research information should be protected, or who might be able to obtain particularly sensitive information in the name of 'research'. I think all of the comprehensive privacy bills have some level of protection of this information.

- While the financial privacy language includes prohibitions on re-use of data, those prohibitions do not apply to medical information. That means companies receiving sensitive medical data from insurers are then free to use and sell the data without any Federal legal restrictions whatsoever.

- There are no limits on re-disclosure of medical and genetic information. Not only could a credit agency receive information from an insurer, but reporting to such entities is permitted. The entities can then turn around and give it to anyone they desired. So, the results of your latest physical exam could be used to deny your application for a home mortgage or credit card. All of this happens without patient without a patient's consent or knowledge. The comprehensive privacy bills address include protections for re-disclosure.

- This language would permit life insurers or health insurers to share sensitive medical information with anyone purporting to be conducting a research project. This language is very broad, and would not be limited to behavioral or biomedical research. This would mean that a life insurer that conducts physical examinations could release medical information to someone conducting market research.

- Basic protections necessary to make health privacy provisions work are missing from the language. There are no requirements that a consent for release of information be limited to only the minimum of information necessary for the particular purpose. This means if a health insurer asked your physician for documentation of your blood type, the physician should not be permitted to give them every bit of medical information they have about you.

JUL.30.1999 12:24 202 690 8425 HEALTH LEGISLATION #0363 P.003/006

From Chai Feldblum
Re: Subtitle D--Confidentiality Provisions
July 29, 1999

Let me begin by thanking you for your willingness to consider my comments on your legislative provisions. Since I think we share the goals of protecting patient privacy as much as possible, I hope these comments are useful to you in your work. While these suggestions are my personal position, I anticipate that if *all* of these changes are made, then the language in the banking bill may be acceptable to consumer groups. If, however, these changes cannot be made, then I would say--to paraphrase your comment--that "something is *not* better than nothing," because the language would result in incredibly weak privacy protection and, thus, would create the adverse precedent of such weak protection at the federal level. (Moreover, as long as the non-preemption of state laws is not explicit, it would also result in fewer protections than are currently available.) Thus, if all of these changes cannot be made, I would recommend the language be removed from the bill and that we all continue to work on a comprehensive privacy bill.

At the outset, I emphasize that your language in the banking bill is quite broad in its scope. Since it involves insurers, their subsidiaries, and their affiliates, its reach extends to many financial institutions, managed care organizations, physicians and other providers, and medical suppliers and pharmaceutical companies. In many ways, although it is in the Banking bill, this language affects the core of medical privacy.

I. In general, the provisions of paragraphs (a)(1), (2), and (3) should be re-framed into two categories: Compelled Authorization and Voluntary Authorization.

A. Compelled Authorization means that the person whose identifiable information is at stake must agree to allow the company to use the information in the enumerated ways or else not get insurance.

1. Compelled Authorization would apply to the activities necessary for a company to decide to give insurance coverage, to administer the coverage, to protect against fraud, to meet government requirements, and to deal with mergers and transfers.

2. Disclosure of information under this provision should be limited to the purpose for which the information was first given. I would expect this to be for payment for health care services, for treatment of the patient, or for the business necessity of administering the individual account.

B. Voluntary Authorization means that the person whose identifiable information is at stake may decide to allow the company to use the information in the

enumerated ways, but that if that person decides not to do so, he/she will not be denied benefits or services.

1. Voluntary Authorization would apply to the activities that are not necessary for the individual insurance contract but which may be an appropriate use of information if the person consents, including providing information to the person's physician, research, sharing with other insurance companies, or reporting to consumer reporting agencies.

2. Disclosure of information under this provision should be limited to the purpose for which Voluntary Authorization was given.

II. Disclosure of information under both Compelled Authorization and Voluntary Authorization should be governed by the general principles of "Use Identifiable Information Only When Needed" and "Use Identifiable Information Only to the Minimum Extent Necessary" Without these principles, the Compelled Authorization would need to be written must more strictly to delineate levels of need-to-know.

A. "Use Identifiable Information Only When Needed" allows the company to disclose for a business necessity, but requires that the company consider and identify the necessity for identifiable--rather than aggregate or blinded--information. For example, it will be rare (if ever) that the processing of premium payments would require genetic information.

B. "Use Identifiable Information Only to the Extent Necessary" allows the company to disclose for a business necessity, but requires that the company consider and identify the amount of identifiable information that is needed. Thus, while it may be appropriate for a company to disclose identifiable information to an employee administering benefits, it will be rare (if ever) that the employee will need the entire medical record of the individual to process a discrete claim.

III. The provisions of Subparagraph (a)(3)(E) regarding authorized investigations are too broad as they are written and should be deleted. Current law in many situations gives the patient no notice that his/her records are being sought or disclosed and no rights to contest the decision of the record holder to disclose information. There is broad agreement among those working on privacy issues that some form of legal procedure is necessary before identifiable health information is released for law enforcement purposes. This language would not fill that gap.

Instead, I would suggest that you consider the language in Congressman Condit's bill (Section 305 of H.R. 1941).[1]

IV Your intent that your language not preempt State law should be made explicit. I would suggest something like: "Nothing in this section shall preempt any State law prohibiting disclosure of individually identifiable information."

IV In addition to State enforcement of these provisions, I would urge you to include a private right of action to allow individuals whose information is wrongly released to bring a suit to stop further release and to get damages. While I would be most supportive of an unrestricted private right of action, in discussing this issue with other Republican Members, they have offered the following:

A. Private actions to produce court-ordered injunctions to prohibit further disclosure
B. Private actions for economic damages as well as non-economic losses
C. Punitive damages for knowing violations
D. Attorneys' fees for actions

V. Finally, I would suggest that you add a provision to your sunset clause making clear that this language is not intended to preempt the authority of the Secretary of HHS under the Health Insurance Portability Act (HIPA) and that if the Secretary issues regulations that cover these issues, this language would sunset in the same manner as if the Congress acts.

Again, I would emphasize it is important for all these changes to be made to ensure that this legislation does not weaken the current effort to achieve strong federal privacy protection. If I can be of any assistance, please let me know. I would, of course, be happy to work with you on legislative language as well. Thank you again for your interest.

CRF

---

[1]SEC. 305. Law Enforcement

(a) In General.-A health information custodian may disclose protected health information to a law enforcement official for a law enforcement inquiry if the law enforcement official complies with the Fourth Amendment to the Constitution.

(b) Construction.-For purposes of subsection (a) , all protected health information shall be treated as if it were held in a home over which the protected individual has exclusive authority.

(c) Relationship to Health Oversight Activities.-This section shall not apply to a disclosure of protected health information for purposes of health oversight.

AMERICAN PSYCHIATRIC ASSOCIATION
DIVISION OF GOVERNMENT RELATIONS
1400 K STREET, N.W.
WASHINGTON, DC 20005
Phone: (202) 682-6060 Fax: (202) 682-6287

FAX COVER SHEET

TO: CHRIS JENNINGS

FAX #: 456-5557

FROM: William Bruno: Associate Director; Division of Government Relations

Please Contact me at (202) 682-6046 if there are any questions.

Number of pages transmitted 3 Date 6/29 Time _____
(Including cover sheet)

COMMENTS: Letter requesting deletion of medical records provisions in H.R. 10, signed by 34+ groups

Important Notice:
This message is intended for the use of the individual entity to which it is addressed, and may contain information that is privileged, confidential, and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original message to us at the above address via the U.S. Postal Service. Thank You.

June 29, 1999

Member of Congress
House of Representatives
Washington, DC 20515

Medical Records Provisions of H.R. 10 Undermine Patient Privacy

Dear Representative:

The undersigned physician, provider, patient, and other national organizations strongly support medical records confidentiality not only from a personal privacy perspective, but also because of the critical importance of patient privacy for high quality medical care. We greatly appreciate the well-intentioned efforts of the many members that have resulted in the medical records privacy provisions of H.R. 10. Nevertheless, we have both serious procedural and substantive concerns about these provisions and urge that they be deleted from the bill.

We are particularly concerned because Section 351 of the bill would allow the use and disclosure of medical records information without the consent of the patient in extraordinarily broad circumstances. To give just two examples, law enforcement entities would enjoy virtually unfettered access to medical records and insurance companies could review individual medical records in performing marketing studies. The list of entities that could obtain medical records is also extensive. Why should life insurers, auto insurers, and even insurers providing travel cancellation insurance be able to routinely access patients' entire medical records without patient consent or even knowledge?

To complicate matters further, the legislation establishes no limitations on subsequent disclosures of medical records to non-affiliated entities. Once a disclosure has occurred, there is no limitation on the types of disclosures that the recipient of this information may make. Thus, if an insurer contracts out a certain authorized service to a bill collection agency or an administrative support company, nothing in the legislation would prevent these organizations from disclosing or selling the information for a host of inappropriate purposes far beyond any legitimate health use.

The legislation lacks basic protections included in all the major confidentiality bills before the Congress. The legislation lacks specific requirements for physical, technical, and administrative safeguards to prevent unintended disclosures of medical records. Nor does the legislation encourage the use of deidentified medical records or insure that patients will receive notice of the confidentiality, use, and disclosure practices of the insurance companies.

Confidentiality between the doctor or other health care professional and the patient is an essential component of high quality health, and particularly mental health, care. Unfortunately, the medical records confidentiality provisions in H.R. 10 will deter many patients from seeking needed health care and deter patients from making a full and frank disclosure of critical information needed for their treatment.

We also have numerous procedural concerns. Because the Senate HELP Committee has not yet been able to report out comprehensive medical records privacy provisions, H.R. 10's provisions, intended as a temporary measure until comprehensive legislation is enacted into law, could now

become long-lasting. This is extremely troublesome because H.R. 10 is designed to address only certain narrow aspects of medical records privacy and leaves key issues unresolved. We are deeply concerned that passage of H.R. 10's current medical records privacy language has the potential to undermine enactment of comprehensive medical records privacy legislation.

Thank you for considering these important issues. For further information, please contact William Bruno of the American Psychiatric Association at (202) 682-6194.

Sincerely,

American Psychiatric Association
American College of Occupational and Environmental Medicine
American Academy of Child and Adolescent Psychiatry
American Academy of Family Physicians
American Association of Occupational Health Nurses, Inc
American Association for Psychosocial Rehabilitation
American College of Physicians - American Society of Internal Medicine
American College of Surgeons
American Counseling Association
American Family Foundation
American Federation of State, County, and Municipal Employees
American Lung Association
American Medical Association
American Occupational Therapy Association
American Osteopathic Association
American Psychoanalytic Association
American Psychological Association
American Society for Gastrointestinal Endoscopy
American Society of Clinical Psychopharmacology
American Society of Cataract and Refractive Surgery
American Thoracic Society
Anxiety Disorders Association of America
Association for Ambulatory Behavioral Health
Association for the Advancement of Psychology
Bazelon Center for Mental Health Law
Corporation for the Advancement of Psychiatry
Federation of Behavioral, Psychological and Cognitive Sciences
International Association of Psychosocial Rehabilitation Services
National Association of Developmental Disabilities Councils
National Association of Psychiatric Treatment Centers for Children
National Association of Social Workers
National Council for Community Behavioral Healthcare
National Depressive and Manic Depressive Association
National Foundation for Depressive Illness
National Mental Health Association
Renal Physicians Association
Service Employees International Union

HEALTH PRIVACY PROJECT

INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

best principles FOR HEALTH PRIVACY

A REPORT OF THE
HEALTH PRIVACY WORKING GROUP

WITH SUPPORT FROM
THE ROBERT WOOD JOHNSON FOUNDATION

THE HEALTH PRIVACY WORKING GROUP

The Health Privacy Working Group is an initiative of the Health Privacy Project of Georgetown University's Institute for Health Care Research and Policy. The Working Group is funded through a generous grant from the Robert Wood Johnson Foundation.

The Working Group is staffed by Janlori Goldman, Director, and Zoe Hudson, Policy Analyst of the Health Privacy Project. The Project wishes to thank the Robert Wood Johnson Foundation, in particular Judith Whang, who recognized the importance of this challenge; the Glen Eagles Foundation and the Trellis Fund, most notably Betsy Frampton and Hope Gleicher, who saw the promise in this Project; Andy Burness, Linda Loranger, and the rest of the staff of Burness Communications for their guidance throughout the process; Scott Sanders of High Noon Communications, Audrey Denson of Denson Design, and Mike Heffner of 202 Design for their keen design skills; and our colleagues at the Institute for Health Care Research and Policy.

Our deep appreciation goes to the individual members of the Working Group, who dedicated themselves over the past year to this extremely daunting—and we hope just as valuable—endeavor. As Chair, Dr. Bernard Lo brought to bear his vast knowledge and talents as doctor, ethicist, teacher, writer, listener and refiner, all of which made this possible.

MEMBERS

Chair
Bernard Lo
Director, Program in Medical Ethics
University of California San Francisco

Paul Clayton
Professor of Medical Informatics
Columbia Presbyterian Medical Center and
Intermountain Health Care

Jeff Crowley
Chair, Privacy Working Group
Consortium for Citizens with Disabilities and
Deputy Executive Director for Programs
National Association of People with AIDS

John Glaser
Vice President and Chief Information Officer
Partners HealthCare System, Inc.

Nan Hunter
Professor of Law
Brooklyn Law School

Shannah Koss
Healthcare Security and Government
Programs Executive
IBM Corporation

Chris Koyanagi
Policy Director
Bazelon Center for Mental Health Law

John Nielsen
Senior Counsel and Director of Government
Relations
Intermountain Health Care

Linda Shelton
Policy Director
National Committee for Quality Assurance

Margaret VanAmringe
Vice President for External Affairs
Joint Commission on Accreditation of
Healthcare Organizations

© Health Privacy Project, July 1999

HEALTH PRIVACY WORKING GROUP
BEST PRINCIPLES FOR HEALTH PRIVACY

EXECUTIVE SUMMARY

Executive Summary

Privacy and confidentiality have long been recognized as essential elements of the doctor-patient relationship. Also essential to optimal care is the compilation of a complete medical record. But that same record is used for a wide variety of purposes—including insurance functions, coordination of care, and research. The long-standing friction between these two goals—patient privacy and access to information for legitimate purposes—has been heightened by the transition to electronic health information and a push toward integrated information in support of integrated health care delivery and health data networks. While these developments are intended to improve health care, they also raise many questions about the role of privacy in the health care environment.

Recent polls demonstrate that the public has significant concern about the lack of privacy protection for their medical records and that it can impact how they engage with health care providers. In order to protect their privacy, some patients lie or withhold information from their providers; pay out-of-pocket for care; see multiple providers to avoid the creation of a consolidated record; or sometimes avoid care altogether. Such "privacy-protective" behavior can compromise both individual care and public health initiatives.

The public has some reason to be concerned. Today, there is little consistency in approaches to patient confidentiality and no national standards or policies on patient confidentiality. The 1996 Health Insurance Portability and Accountability Act provides that if Congress fails to enact comprehensive health privacy legislation by August 1999, the Secretary of Health and Human Services must issue regulations. Therefore, either through legislation, government regulation, or self-regulation, there will be significant developments with regard to health privacy in the next two years.

What has been missing from the debate is a consensus document that offers policy recommendations regarding how best to protect patient confidentiality. To fill this void, the Health Privacy Project, with funding from the Robert Wood Johnson Foundation, created the Health Privacy Working Group in June 1998. Its mission was to achieve common ground on "best principles" for health privacy, while identifying a range of options for putting those principles into practice. The Working Group is comprised of diverse stakeholders, including: disability and mental health advocates; health plans; providers; employers; standards and accreditation representatives; and experts in public health, medical ethics, information systems, and health policy.

The Working Group spent the past year crafting a consensus document that reflects "best principles" for health privacy. This report outlines the 11 principles to which the Working Group agreed and details the rationale behind the recommendations.

Best Principles for Health Privacy

The principles represent significant compromises between Working Group members and should be seen as a framework that aims to accommodate the various information needs of diverse interest groups. The principles are designed to establish a baseline of

Executive Summary

protections that should be considered when implementing comprehensive patient privacy policies and practices.

The Working Group adopted the following 11 principles. Because these principles are intended to establish a comprehensive framework, they should be read and implemented as a whole.

1. **For all uses and disclosures of health information, health care organizations should remove personal identifiers to the fullest extent possible, consistent with maintaining the usefulness of the information.**

Generally, the use and disclosure of information that does not identify individuals does not compromise patient confidentiality. As such, the use and disclosure of non-identifiable health information should "fall outside" the scope of policies that govern personally identifiable health information. Health care organizations will need to take into consideration the practicality and cost of using and disclosing non-identifiable information. Ultimately, through the creation and use of non-identifiable health information, more people can have more information, without compromising patient confidentiality.

2. **Privacy protections should follow the data.**

All recipients of health information should be bound by all the protections and limitations attached to the data at the initial point of collection. Recipients of health information can use or disclose personally identifiable health information only within the limits of existing authorizations. Any further uses or disclosures require specific, voluntary patient authorization.

3. **An individual should have the right to access his or her own health information and the right to supplement such information.**

All patients should be allowed to copy their records and to supplement them if necessary. But supplementation should not be implied to mean "deletion" or "alteration" of the medical record. Furthermore, data holders may charge a reasonable fee for copying the records, but they cannot refuse inspection of the records simply because they are owed money by the individual requesting inspection.

In certain cases, patients may be denied access to their medical records. Such instances include if the disclosure could endanger the life or physical safety of an individual; if the information identifies a confidential source; if the information was compiled in connection with a fraud or criminal investigation that is not yet complete; or if the information was collected as part of a clinical trial that is not yet complete and the patient was notified in advance about his or her rights to access information.

4. Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.

The notice should tell the patient how information will be collected and compiled, how the collecting organization will use or disclose the information, what information the patient can inspect and copy, steps the patient can take to limit access, and any consequences the patient may face by refusing to authorize disclosure of information.

5. Health care organizations should implement security safeguards for the storage, use, and disclosure of health information.

Security safeguards consistent with the Secretary of Health and Human Service's standards, whether technological or administrative, should be developed to protect health information from unauthorized use or disclosure and should be appropriate for use with electronic and paper records. Any safeguards should recognize the trade-off between availability and confidentiality and should be tailored to meet needs as organizations adopt more sophisticated technologies.

6. Personally identifiable health information should not be disclosed without patient authorization, except in limited circumstances. Health care organizations should provide patients with certain choices about the use and disclosure of their health information.

Patient authorization should be obtained prior to disclosure of any health information. But, at the same time, some patient information needs to be shared for treatment, payment, and core business functions. With this in mind, the Working Group recommends a two-tiered approach to patient authorization.

The authorization structure allows for a health care organization to obtain a single, one-time authorization for core activities that are considered necessary or routine. These activities are directly tied to treatment, payment, and necessary business functions in keeping with medical ethics. The health care organization may condition the delivery of care—identified as Tier One—or payment for care upon receiving authorization for these activities, which can be obtained at the point of enrollment or at the time of treatment.

Any activities that fall outside this core group (sometimes commonly referred to as uses) must be authorized separately by the patient and fall under Tier Two authorization. The patient can refuse authorization for these activities without facing any adverse consequences. Activities in this category include, but are not limited to:

- purposes of marketing;
- disclosure of psychotherapy notes;
- disclosure of personally identifiable health information to an employer, except where necessary to provide or pay for care;
- disclosure of personally identifiable health information outside the health care treatment entity that collected the information, if other Tier One authorization(s) do not apply;

and
- disclosure of personally identifiable health information, if adequate notice has not been given at the point of the initial authorization.

The Working Group identified a limited number of circumstances in which personally identifiable health information may be disclosed without patient authorization. These include:
- when information is required by law, such as for public health reporting;
- for oversight purposes, such as in fraud and abuse investigations;
- when compelled by a court order or warrant; and
- for research, as described in Principle 8 below.

7. Health care organizations should establish policies and review procedures regarding the collection, use, and disclosure of health information.

An organization's confidentiality policies and procedures should be coherent, tying together authorization requirements, notice given to patients, safeguards, and procedures for accessing personally identifiable health information. Organizations should also establish review processes that ensure a degree of accountability for decisions about the use and disclosure of personally identifiable health information. During such a process organizations might, for example, wish to determine routine procedures and special procedures for some areas of health care where medical information is considered highly sensitive to the patient.

8. Health care organizations should use an objective and balanced process to review the use and disclosure of personally identifiable health information for research.

For some areas of research, it is not always practical to obtain informed consent and, in some cases, a consent requirement could bias results. Recognizing this, the Working Group advises that patient authorization should not always be required for research. However, any waivers of informed consent should only be granted through an objective and balanced process.

Currently, any federally funded research is subject to the "Common Rule," where an Institutional Review Board (IRB) is required to make a determination about the need for informed consent. An IRB can choose to give a researcher access to personally identifiable health information with or without informed consent. But some research falls outside the scope of federal regulations. In such circumstances, health care organizations should use a balanced and objective process before granting researchers access to personally identifiable health information.

9. Health care organizations should not disclose personally identifiable health information to law enforcement officials, absent a compulsory legal process, such as a warrant or court order.

Federal privacy laws generally require that some form of compulsory legal process, based on a standard of proof, be presented in order to

disclose to law enforcement officers. Law enforcement access to health information should be held to similar standards. In some instances, however, government officials may access health information with legal process for the purposes of health care oversight. In these instances, the information obtained should not be used against the individual in an action unrelated to the oversight or enforcement of law nor should the information be re-disclosed, including to another law enforcement agency, except in conformance with the privacy protections that have attached to the data.

10. Health privacy protections should be implemented in such a way as to enhance existing laws prohibiting discrimination.

Currently, there are state and federal laws that prohibit discrimination on the basis of a person's health status in areas such as employment or insurance underwriting. Confidentiality policies should be implemented in such a way as to enhance and complement these protections. In effect, privacy can serve as the first line of defense against discrimination, creating a more comprehensive framework of protection.

11. Strong and effective remedies for violations of privacy protections should be established.

Remedies should be available for internal and external violations of confidentiality. Health care organizations should also establish appropriate employee training, sanctions, and disciplinary measures for employees and contractors who violate confidentiality policies.

The 11 principles outlined above focus on information gathered in the context of providing patient care and are written to establish a broad framework for the use and disclosure of health information. Although the Working Group recognizes that the need for privacy protections in other areas is no less urgent, this consensus document does not address the following areas:

- special considerations about the needs of minors;
- information that locates an individual in a particular health care organization (sometimes referred to as "directory information");
- information provided to spouses, dependents, and other next of kin;
- public health reporting;
- fraud and abuse investigations; and
- the appropriate relationship between state and federal law.

These 11 principles are designed to serve as a baseline for establishing patient privacy protections. While we all agree that health information, used in the right hands and with the right safeguards, can lead to improved health and advances in research, this information should not be used with disregard for patient privacy. Patients need to know that adequate protections are in place to protect their health information. Our hope is that these principles will go a long way towards establishing appropriate protections and, in the process, help build public trust and confidence in our health care system.

DEPARTMENT OF THE TREASURY
LEGISLATIVE AFFAIRS
15TH & PENNSYLVANIA AVE., N.W.
WASHINGTON, D.C. 20220

DATE: 7/30/99 PAGES TO FOLLOW: 15

TO: Chris Jennings

FAX NUMBER: 456-5557

OFFICE NUMBER: _____

FROM: LEGISLATIVE AFFAIRS 622-1900 (office) 622-0534 (fax)

Marne Levin-The CRS study might have been requested by Ganske. The conclusions of the study are causing the House Dems to rethink their position on medical privacy. In other words, instead of striking medical from financial modernization, they might be inclined instead to ask for the strongest possible provision. Apparently insurance would be covered by Ganske but, not by HHS regulations/current authority. House is to appoint conferees on H.R. 10 today and therefore House Dems will do a motion to instruct today that will address medical privacy among other issues. Given that this differs from our position, HHS and WH need to contact LaFalce staff and Gephardt staff to explain our concerns about their change in position.

unclassified

July 29, 1999

Re: HHS authority to issue regulations relating to medical privacy

Anticipating that legislation addressing the confidentiality of medical information might not be completed by August 21 of this year, Congress included in Section 264 (c) of HIPAA (attached) a requirement for the Sec. of HHS to promulgate regs on medical privacy "in connection with the transactions described in section 1173(a) of the Social Security Act" (appearing in section 262 of HIPAA, attached). Section 1173(a), in turn, refers to data transactions such as health claims, health care payments, enrollment in a health plan, health care payment and remittance advice, health plan premium payments, health claim status, and "other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs." It should be noted that life insurers, disability insurers and long-term care insurers are not considered to be part of the health care system.

Section 264 of HIPAA required HHS to issue recommendations on medical information privacy to Congress. This report, issued September 11, 1997, describes the intended coverage of the proposed HHS regs on page 11(attached), and goes on to note:

> "The definition [of health care providers or payers under the provision] does not encompass liability insurers who receive health information, as needed, pursuant to claimants' authorization. Nor does it include life insurers, who receive information, with the patient's authorization, not as part of health care or payment, but to make underwriting decisions."

There are several instances since HIPAA was enacted in which the Secretary or other HHS officials have affirmed their interpretation that insurers other than health insurers would not be subject to the anticipated regulations. We have quotes if you would like them.

It occurred to that part of the problem the administration may be having with the Ganske language is that it applies to all insurers, which would include health insurers, and that may raise a question in some peoples minds whether the HHS regs would be preempted with respect to health insurers.

"(ii) the standard is promulgated in accordance with the rulemaking procedures of subchapter III of chapter 5 of title 5, United States Code.

"(B) NO STANDARD BY STANDARD SETTING ORGANIZATION.—If no standard setting organization has developed, adopted, or modified any standard relating to a standard that the Secretary is authorized or required to adopt under this part—

"(i) paragraph (1) shall not apply; and

"(ii) subsection (f) shall apply.

"(3) CONSULTATION REQUIREMENT.—

"(A) IN GENERAL.—A standard may not be adopted under this part unless—

"(i) in the case of a standard that has been developed, adopted, or modified by a standard setting organization, the organization consulted with each of the organizations described in subparagraph (B) in the course of such development, adoption, or modification; and

"(ii) in the case of any other standard, the Secretary, in complying with the requirements of subsection (f), consulted with each of the organizations described in subparagraph (B) before adopting the standard.

"(B) ORGANIZATIONS DESCRIBED.—The organizations referred to in subparagraph (A) are the following:

"(i) The National Uniform Billing Committee.

"(ii) The National Uniform Claim Committee.

"(iii) The Workgroup for Electronic Data Interchange.

"(iv) The American Dental Association.

"(d) IMPLEMENTATION SPECIFICATIONS.—The Secretary shall establish specifications for implementing each of the standards adopted under this part.

"(e) PROTECTION OF TRADE SECRETS.—Except as otherwise required by law, a standard adopted under this part shall not require disclosure of trade secrets or confidential commercial information by a person required to comply with this part.

"(f) ASSISTANCE TO THE SECRETARY.—In complying with the requirements of this part, the Secretary shall rely on the recommendations of the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)), and shall consult with appropriate Federal and State agencies and private organizations. The Secretary shall publish in the Federal Register any recommendation of the National Committee on Vital and Health Statistics regarding the adoption of a standard under this part.

Federal Register, publication.

"(g) APPLICATION TO MODIFICATIONS OF STANDARDS.—This section shall apply to a modification to a standard (including an additiom to a standard) adopted under section 1174(b) in the same manner as it applies to an initial standard adopted under section 1174(a).

"STANDARDS FOR INFORMATION TRANSACTIONS AND DATA ELEMENTS

42 USC 1320d-2.

"SEC. 1173. (a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE.—

"(1) IN GENERAL.—The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for—

"(A) the financial and administrative transactions described in paragraph (2); and

"(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

"(2) TRANSACTIONS.—The transactions referred to in paragraph (1)(A) are transactions with respect to the following:

"(A) Health claims or equivalent encounter information.

"(B) Health claims attachments.

"(C) Enrollment and disenrollment in a health plan.

"(D) Eligibility for a health plan.

"(E) Health care payment and remittance advice.

"(F) Health plan premium payments.

"(G) First report of injury.

"(H) Health claim status.

"(I) Referral certification and authorization.

"(3) ACCOMMODATION OF SPECIFIC PROVIDERS.—The standards adopted by the Secretary under paragraph (1) shall accommodate the needs of different types of health care providers.

"(b) UNIQUE HEALTH IDENTIFIERS.—

"(1) IN GENERAL.—The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system. In carrying out the preceding sentence for each health plan and health care provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for health care providers.

"(2) USE OF IDENTIFIERS.—The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.

"(c) CODE SETS.—

"(1) IN GENERAL.—The Secretary shall adopt standards that—

"(A) select code sets for appropriate data elements for the transactions referred to in subsection (a)(1) from among the code sets that have been developed by private and public entities; or

"(B) establish code sets for such data elements if no code sets for the data elements have been developed.

"(2) DISTRIBUTION.—The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1174(b).

"(d) SECURITY STANDARDS FOR HEALTH INFORMATION.—

"(1) SECURITY STANDARDS.—The Secretary shall adopt security standards that—

"(A) take into account—

"(i) the technical capabilities of record systems used to maintain health information;

"(D) shall be responsible generally for advising the Secretary and the Congress on the status of the implementation of part C of title XI of the Social Security Act."; and

(5) by adding at the end the following:

"(7) Not later than 1 year after the date of the enactment of the Health Insurance Portability and Accountability Act of 1996, and annually thereafter, the Committee shall submit to the Congress, and make public, a report regarding the implementation of part C of title XI of the Social Security Act. Such report shall address the following subjects, to the extent that the Committee determines appropriate: Reports.

"(A) The extent to which persons required to comply with part C of title XI of the Social Security Act are cooperating in implementing the standards adopted under such part.

"(B) The extent to which such entities are meeting the security standards adopted under such part and the types of penalties assessed for noncompliance with such standards.

"(C) Whether the Federal and State Governments are receiving information of sufficient quality to meet their responsibilities under such part.

"(D) Any problems that exist with respect to implementation of such part.

"(E) The extent to which timetables under such part are being met.".

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION. 42 USC 1320d-2 note.

(a) IN GENERAL.—Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.

(b) SUBJECTS FOR RECOMMENDATIONS.—The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

(c) REGULATIONS.—

(1) IN GENERAL.—If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b). Regulations.

(2) PREEMPTION.—A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State

law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.

(d) CONSULTATION.—In carrying out this section, the Secretary of Health and Human Services shall consult with—

(1) the National Committee on Vital and Health Statistics established under section 306(k) of the Public Health Service Act (42 U.S.C. 242k(k)); and

(2) the Attorney General.

Subtitle G—Duplication and Coordination of Medicare-Related Plans

SEC. 271. DUPLICATION AND COORDINATION OF MEDICARE-RELATED PLANS.

(a) TREATMENT OF CERTAIN HEALTH INSURANCE POLICIES AS NONDUPLICATIVE.—Section 1882(d)(3)(A) (42 U.S.C. 1395ss(d)(3)(A)) is amended—

(1) in clause (iii), by striking "clause (i)" and inserting "clause (i)(II)"; and

(2) by adding at the end the following:

"(iv) For purposes of this subparagraph, a health insurance policy (other than a Medicare supplemental policy) providing for benefits which are payable to or on behalf of an individual without regard to other health benefit coverage of such individual is not considered to 'duplicate' any health benefits under this title, under title XIX, or under a health insurance policy, and subclauses (I) and (III) of clause (i) do not apply to such a policy.

"(v) For purposes of this subparagraph, a health insurance policy (or a rider to an insurance contract which is not a health insurance policy) is not considered to 'duplicate' health benefits under this title or under another health insurance policy if it—

"(I) provides health care benefits only for long-term e, nursing home care, home health care, or community-based care, or any combination thereof,

"(II) coordinates against or excludes items and services available or paid for under this title or under another health insurance policy, and

"(III) for policies sold or issued on or after the end of the 90-day period beginning on the date of enactment of the Health Insurance Portability and Accountability Act of 1 discloses such coordination or exclusion in the policy's outline of coverage.

For purposes of this clause, the terms 'coordinates' and 'coordination' mean, with respect to a policy in relation to health benefits under this title or under another health insurance policy, that the policy under its terms is secondary to, or excludes from payment, items and services to the extent available or paid for under this title or under another health insurance policy.

"(vi)(I) An individual entitled to benefits under part A or enrolled under part B of this title who is applying for a h insurance policy (other than a policy described in subclause (III)) shall be furnished a disclosure statement described in clause (vii) for the type of policy being applied for. Such statement shall be

CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION

Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996

Submitted to:

The Committee on Labor and Human Resources and the Committee on Finance of the Senate

The Committee on Commerce and the Committee on Ways and Means of the House of Representatives

On September 11, 1997

CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION

Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996

I. INTRODUCTION

II. THE RECOMMENDATIONS

A. COVERAGE

1. PROVIDERS AND PAYERS, AND THOSE WHO RECEIVE INFORMATION FROM THEM

We recommend that Federal health privacy legislation apply primarily to health care providers and payers.

We recommend that persons receiving information under the provisions of such legislation without patient authorization for health oversight, public health, research, State data system purposes be subject to the requirements of the legislation.

We recommend that health care providers be defined as persons who receive, create, use, or maintain, health information while providing health care in the ordinary course of business or practice of a profession, pursuant to license, certification, registration, or other legal authorization.

We recommend that payers be defined to include persons who pay for health care through contracts of insurance or in connection with employment, and government programs that pay for care under a benefit plan.

Applies to providers & payers

The legislation we recommend should apply in the [redacted] They are at the heart of health care, and typically receive information directly from patients and generate health information. They are often one and the same.

In turn, [redacted] they are referred to as "those receiving health information under the provisions of the law without patient authorization."

others who get it w/o bound by reg-

Providers are persons -- individual and institutional -- who receive, create, use, or maintain, health information while providing health care (including preventive health services) in the ordinary course of business or practice of a profession, pursuant to license, certification, registration, or other legal authorization.

Health care payers pay for health care pursuant to advance agreements or statutory obligations -- the range of entities commonly described as "plans." They may include licensed insurance companies, hospital or medical service corporations, health maintenance organizations, or other entities licensed or certified by a State to provide health insurance or health benefits. They include employee welfare benefit plans and other arrangements that provide health benefits, whether or not funded through the purchase of insurance policies or contracts. They include public programs that pay for health care under a health benefit plan, such as Medicare, Medicaid, the health programs of the Veterans Health Service, and the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS). The term should not be defined to include individuals and families who pay for their own care.

(*) The definition does not encompass liability insurers who receive health information, as needed, pursuant to claimants' authorization. Nor does it include life insurers, who receive information, with the patient's authorization, not as part of health care or payment, but to make underwriting decisions.

We are making no recommendations with respect to including workers' compensation under Federal health privacy legislation at this time. Although workers' compensation carriers receive health care information in much the same manner as health plans, the need under workers' compensation systems to coordinate the health benefits provided with both the indemnity benefits (e.g., lost wages and disability payments) provided under the system and the determination of a worker's ability to return to work raises potential questions about the appropriateness of certain disclosures of medical information. We are continuing to review the need for federal privacy standards in this area and will inform Congress of any recommendations that we have in this area when we complete our review.

We do not recommend that employers as such be controlled by the legislation, But they should be considered health care providers or payers when they actually perform those activities, and obliged to conduct themselves accordingly. (Controls on employers' use of health information so obtained for other purposes is discussed below in LIMITATIONS ON USE).

2. COVERED ACTIVITIES

We recommend that health care be defined to include

-- any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body;

Order Code RS20282
July 29, 1999

CRS Report for Congress

Congressional Research Service · The Library of Congress

The Relationship Between the Medical Privacy Provisions in H.R. 10 and the Health Insurance Portability and Accountability Act (HIPAA)

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates significant changes in the health insurance industry, and includes requirements for the standardization of electronically transmitted health information for financial and administrative transactions. HIPAA required the Secretary of Health and Human Services (HHS) to make recommendations to the Congress by August 1997 on standards with respect to the privacy of "individually identifiable health information," and also provided that if legislation governing standards with respect to the privacy of individually identifiable health information that is electronically transmitted were not enacted by August 21, 1999, the Secretary of HHS must promulgate final regulations containing such standards by February 2000. Although several comprehensive medical records confidentiality bills have been introduced in the 106th Congress, none has been passed. The Senate Health Education Labor and Pensions (HELP) committee has crafted a draft bill that represents a synthesis of the three Senate bills, but attempts to mark up the Senate HELP committee draft have been unsuccessful.

The House passed H.R. 10, which is designed to modernize the financial industry by allowing mergers among insurance companies, banks, securities firms, and other financial institutions, on July 1st. S. 900, Financial Services Modernization, was passed by the Senate May 6th. Unlike the Senate version, the House bill includes provisions (section 351) regarding the disclosure of individually identifiable customer health, medical, and genetic information held by insurance companies that were introduced by Representative Ganske (R-Iowa). Section 351 of H.R. 10 provides that the section will not take effect, or will cease to be effective if legislation is enacted that satisfies section 264(c)(1) of HIPAA which requires the Secretary to issue final regulations containing privacy standards by February 2000 if legislation governing such standards is not enacted by August 21, 1999. This report will be updated as events warrant.

CRS

CRS Reports are prepared for Members and committees of Congress

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates significant changes in the health insurance industry,[1] and includes as part of the overall insurance reforms, requirements for the standardization of electronically transmitted health information for financial and administrative transactions.[2] All health care payers and providers who transmit financial and administrative transactions electronically are required to use standardized data elements.[3] The Secretary of the Department of Health and Human Services (HHS) is required to develop and adopt the standards to be used. The purpose of these HIPAA requirements is to reduce administrative costs and paperwork, improve the efficiency of the health care system, detect fraud and abuse, and facilitate access to medical information. HIPAA also required the Secretary of Health and Human Services to make detailed recommendations to the Congress by August 1997 on standards with respect to the privacy of "individually identifiable health information."[4] The recommendations were to address the rights that an individual who is a subject of individually identifiable health information should have, the procedures that should be established for exercise of those rights, and the uses and disclosures of such information that should be authorized or required.

Health Information Confidentiality Recommendations of the Secretary of HHS

On September 11, 1997, the Secretary of Health and Human Services delivered recommendations to the Congress for the establishment of federal privacy legislation to protect the confidentiality of health information.[5] The Secretary recommended that Congress enact national standards that provide fundamental privacy rights for patients and define responsibilities for record keepers. Specifically, the recommendations suggest that a federal privacy law should impose new restrictions on those who pay and provide for care, as well as those who receive information from them; prohibit disclosure of patient-identifiable information except as authorized by the patient or as explicitly permitted by the legislation. Disclosures without patient consent would be allowed only in specified situations: for health care, and for payment for health care; for oversight of the health care system, including audit, investigation, quality assurance, and licensure; for

---

[1]Pub. L. 104-191, 110 Stat. 1396.

[2]Pub. L. 104-191, §§ 261-264, 42 U.S.C. §§ 1320d to 1320d-8.

[3]See, CRS Report for Congress, *The Health Insurance Portability and Accountability Act (HIPAA): Summary of the Administrative Simplification Provisions*, No. 98-964 EPW by Celinda Franco (Nov. 18, 1998).

[4]"The term "individually identifiable health information" means any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental heath or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe that information can be used to identify the individual." 42 U.S.C. § 1320d.

[5]*Confidentiality of Individually Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996*, Submitted to the Committee on Labor and Human Resources and the Committee on Finance of the Senate (Sep. 11, 1997). Available at http://aspe.os.dhhs.gov/admnsimp/pvcrec.htm.

directory information, about presence in an institution; to next-of-kin, relating to current treatment if the patient has not objected; in emergencies affecting life or safety; for public health; for research, under conditions similar to those now imposed on such disclosures under Federal protection of human subjects requirements; to state health data systems, pursuant to state law; to law enforcement authorities, in accord with other law; in court proceedings in which the patient is a party; and in court proceedings, pursuant to court order. In most of these disclosure situations, recipients are to be bound by the restrictions on use and disclosure. The recommendations would also provide for punishment for those who misuse personal health information and redress for people who are harmed by its misuse; impose criminal penalties for obtaining health information under false pretenses, and for knowingly disclosing or using medical information in violation of the Federal privacy law; and allow individuals whose rights under the law have been violated to bring an action for damages and equitable relief.

The recommendations cover health care providers[6] and payers,[7] service organizations hired by providers and payers to work for them, those receiving information under the legislation without patient authorization, and those receiving information with authorization of the patient. The recommendations would not cover directly information obtained in underwriting life insurance or in processing claims in property and casualty insurance.[8] However, insurers are to be bound by the promises made when asking individuals to authorize disclosure of information by health care providers and payers. The Secretary's recommendations were addressed in hearings held by the Senate Labor and Human Resources Committee in the 105th Congress.

HIPAA provides that if legislation governing standards with respect to the privacy of individually identifiable health information that is electronically transmitted in connection with financial and administrative transactions[9] is not enacted by August 21, 1999 the Secretary of Health and Human Services must promulgate final regulations containing such standards by February 2000.[10] The regulations must address, at minimum, the rights that an individual who is a subject of individually identifiable health information

---

[6]"Health care providers" is defined as persons who receive, create, use, or maintain, health information while providing health care in the ordinary course of business or practice of a profession, pursuant to license, certification, registration, or other legal authorization. HHS Recommendations, *supra* note 5, at II. A.

[7]"Payers" is defined to include persons who pay for health care through contracts of insurance or in connection with employment, and government programs that pay for care under a benefit plan. Recommendations, *supra* note 5 at II. A.

[8]"The definition [of payers] does not encompass liability insurers who receive health information, as needed, pursuant to claimants' authorization. Nor does it include life insurers, who receive information, with the patient's authorization, not as part of health care or payment, but to make underwriting decisions." Recommendations, *supra* note 5, at II. A.

[9]As described in section 1173 of the Social Security Act (as added by section 262), the transactions relate to the following: health claims or equivalent encounter information, health claims attachments, enrollment and disenrollment in a health plan, eligibility for a health plan, health care payment and remittance advice, health plan premium payments, first report of injury, health claim status, and referral certification and authorization. 42 U.S.C. § 1320d-2.

[10] Pub. L. 104-191, 110 Stat. 2033 sec. 264(c)(1), 42 U.S.C. § 1320d-2 note.

should have, the procedures that should be established for exercise of those rights, and the uses and disclosures of such information that should be authorized or required. The regulations promulgated by the Secretary shall not supercede a contrary provision of State law, if the provision imposes requirements, standards, or implementation specifications that are more stringent than those imposed under the applicable regulations. To carry out this section [264], the Secretary is required to consult with the National Committee on Vital and Health Statistics and the Attorney General.

Congressional Response: Comprehensive Medical Records Privacy Legislation

Several comprehensive medical records confidentiality bills have been introduced in the 106th Congress: S. 573 (Leahy)/H.R. 1057 (Markey), H.R. 1941 (Condit), S. 578 (Jeffords), S. 881 (Bennett), H.R. 2404 (Murtha), H.R. 2455 (Shays), and H.R. 2470 (Greenwood).[11] The Senate Health Education Labor and Pensions (HELP) committee has crafted a May 19 draft bill, "The Health Information Confidentiality Act of 1999," that represents a synthesis of three Senate privacy bills: S. 573 (Leahy), S. 578 (Jeffords), S. 881 (Bennett).[12]

The Senate HELP bill's four titles address individuals' rights with respect to their medical records, restrictions on use and disclosure of personally identifiable health information, sanctions for violating the law, and preemption of state laws. Under each title, some specific provisions were taken from existing legislation. The bill would allow individuals to review, copy, and amend their medical records; require entities to establish information protection policies; and require appointment of an information officer to oversee the development and enforcement of those policies. Consolidated authorization would allow for the use of protected health information for treatment, payment, and health plan operations. Any activities outside of this area, including research, would require a separate authorization, with few exceptions. Medical records could be released to law enforcement officers subject to a subpoena or warrant, or as required by state or federal law. Criminal penalties for violating the law would range from $50,000 to $500,000, and civil penalties from $500 to $100,000. The bill would allow a civil right of action for people whose rights have been violated. Under the committee's draft bill, federal law would not pre-empt state laws passed before the federal law and deemed at least as protective as the federal law. States with less protective laws would be preempted.

Several attempts to markup the Senate HELP committee draft bill have been unsuccessful because of disagreements on a number of issues. Legislative markup was delayed on June 16th indefinitely to allow more time to reach compromise on the inclusion of a civil right of action giving individuals the right to sue for privacy breaches of their medical records, and on minors' rights to privacy from parental notification with respect to who can access minors' medical records (*i.e.*, whether medical record containing information on AIDS or pregnancy can be disclosed to parents). Other outstanding issues include the preemption of state laws, oversight of privately funded research, and law enforcement access.

---

[11] See, *Medical Records Confidentiality*, CRS Issue Brief 98002, Coordinated by Gina Marie Stevens (June 20, 1999).

[12] http://www.senate.gov/~labor/legisl/106a/106a.htm.

Section 351 of H.R. 10, the Confidentiality of Customer Health, Medical, and Genetic Information Held by Insurance Companies

The House passed H.R. 10, which is designed to modernize the financial industry by allowing mergers among insurance companies, banks, securities firms, and other financial institutions, on July 1st. S. 900, Financial Services Modernization, was passed by the Senate May 6th. Unlike the Senate version, the House bill includes provisions regarding the disclosure of medical records held by insurance companies that were introduced by Representative Ganske (R-Iowa), and approved by the House Commerce Committee.

Section 351 of H.R. 10, the Financial Services Act of 1999,[13] requires insurance companies and their subsidiaries and affiliates to protect the confidentiality of individually identifiable customer health, medical, and genetic information. The bill does not define customer health, medical, and genetic information. Individually identifiable customer health, medical, and genetic information held by insurance companies may not be disclosed without the consent of the customer unless the disclosure falls within one of several exceptions. Insurance companies are authorized to disclose such information without customer consent for the business of insurance (for purposes of underwriting, reinsuring, account administration, preventing fraud, administering benefits, etc.), or in connection with effectuating and enforcing the transaction, transferring accounts, auditing payment information, providing information to the customer's health care provider, research project participation, to enable the purchase, sale, or transfer of any insurance-related business, compliance with Federal or State law, credit card processing and other financial transactions, compliance with governmental investigations, fraud detection, risk control, resolving customer disputes, or reporting to consumer reporting agencies. Enforcement would be through existing state law or by a federal court enforcement action brought by a State. This provision would go into effect February 1, 2000. State insurance regulatory authorities, through the National Association of Insurance Commissioners, are required to consult with the Secretary of Health and Human Services.

Section 351 contains a sunset provision (c)(2), which provides that the section will not take effect, or will cease to be effective if legislation is enacted that satisfies the requirements of section 264(c)(1) of HIPAA.[14]

Proponents of section 351 have said that it is designed to address concerns that if banks and insurance companies merge, for example, a lender could contact its affiliated health claims processing entity and use medical information as a basis for offering a loan. Opponents say it offers little or no real protection for medical records because it addresses only certain narrow aspects of medical records privacy and leaves key issues unresolved. Proponents have opined that the provision would not impact the Secretary of Health and Human Services' ability to write regulations to protect medical information in the absence of federal legislation. Some opponents argue that the provision may replace current congressional efforts to pass medical privacy legislation to satisfy the Health Insurance Portability Act of 1996, frustrate other medical records privacy protections that already exist or that could be enacted in the future at the state and federal level, and undermine the Secretary's authority to issue regulations because the provision only sunsets when

---

[13] 145 Cong. Rec. H4950-51 (June 24, 1999).

[14] *Cf.* fn 10 & accompanying text.

legislation is enacted to satisfy HIPAA, but does not address what would happen if regulations are promulgated to satisfy HIPAA in the absence of legislation. It is argued that the Secretary's regulations could be meaningless because the provision may supercede the regulations.

At a July 21 hearing held by the House Banking Subcommittee on Financial Institutions and Consumer Credit a Treasury Department official testified that the Clinton Administration strongly opposes the medical privacy provisions in H.R. 10. Gary Gensler, Undersecretary for Domestic Finance, testified that although the bill requires consumer consent before their medical information can be shared, "these provisions contain significant exceptions that would, for example, allow re-use of medical information by companies with whom the information is shared, preempt state law, and allow an insurance company to ship information to other companies under the rubric of 'marketing research' in circumstances that neither current practice nor future regulations would likely permit."[15] Gensler said that the provisions would "create uncertainty" about the Secretary of Health and Human Services' ability to write stronger protections.

Generally accepted principles of statutory construction may inform congressional consideration of the issue of how the two acts, HIPPA and H.R. 10, relate to one another.

> If Congress intends one statute to repeal an earlier statute or section of a statute *in toto*, it usually says so directly in the repealing act. There are other occasions when Congress intends one statute to supersede an earlier statute to the extent of conflict, but intends the earlier statute to remain in effect for other purposes. This too is often spelled out, usually in a section captioned "effect on existing law," "construction with other laws," or the like. "[It] can strongly be presumed that Congress will specifically address language in the statute books that it wishes to change." Not infrequently, however, conflicts arise between the operation of two federal statutes that are silent as to their relationship. In such a case, courts will try to harmonize the two so that both can be given effect. A court "must read [two allegedly conflicting] statutes to give effect to each if [it] can do so while preserving their sense and purpose." Only if the provisions of two different statutes are "irreconcilably conflicting," or "if the later act covers the whole subject of the earlier one and is clearly intended as a substitute," will courts apply the rule that the later of the two prevails.[16] (Citations omitted)

In H.R. 10, Congress did not indicate an intent to repeal section 264 of HIPAA, enacted in 1996. Nor did Congress indicate an intent for § 351 of H.R. 10 to supercede § 264 of HIPAA to the extent that there is a conflict between the acts. Rather, Congress directly expressed its intention for § 351 of H.R. 10 to sunset if legislation is passed that satisfies the requirements of § 264(c)(1). However, Congress has not spoken as to the relationship between the operation of § 351 of H.R. 10, and the § 264(c)(1) HIPAA requirement that the Secretary issue final regulations in the absence of legislation.

---

[15] *Privacy Official Says Administration Opposes Medical Privacy Provisions in Banking Bill*, BNA Health Care Daily (7/23/99).

[16] CRS Report for Congress, *Statutory Construction: General Principles and Recent Trends 19-20* No. 97-589A by George Costello (Aug. 28, 1998).

015 TREAS LEG AFFAIRS 07/30/98 FRI 08:58 FAX 202 622 0534

ADDITIONAL VIEWS

During the consideration of H.R. 10, an amendment was offered to add a new section 351, entitled "Confidentiality of Health and Medical Information." While we support increased protection for medical information, we opposed this provision, because, unfortunately, the provision weakens existing protections for medical confidentiality, and establishes a number of poor precedents for private medical information disclosure.

While the provision at first blush appears to place limits on the disclosure of medical information, the lengthy list of exceptions to these limits leaves the consumer with little, if any protection. In fact, the provision ends up authorizing disclosure of information rather than limiting it.

In medicine, the first principle is "Do no harm." In crafting a Federal medical privacy law, this principle requires that state laws providing a greater level of protection be left in place. Yet section 351 could preempt the laws of 21 states that have enacted medical privacy laws. While we agree that genetic information should also be protected—in fact, should deserve a higher level of protection—this provision could also preempt 36 state laws which protect the confidentiality of genetic information.

The provision also lacks any right for the individual to inspect and correct one's medical records. As a result, an individual has greater rights to inspect and correct credit information than medical records.

There is no requirement that the customer even be told that his medical information is being provided to a third party. Thus there is no way that the customer could prevent the records from being disseminated if the customer believed that statutory rights were being violated.

An individual has no right to seek redress if the rights under this provision are violated. In fact, the customer is unlikely to even know that the rights were violated. The only enforcement authority is given to the states. If the individual is unlikely to have knowledge of the transfer of confidential medical records, it is hard to understand how the state Attorney General would know to bring an action as provided in subsection (b) of the provision. Even if the state brings an action, it can only enjoin further disclosures. The customer has no right to seek damages.

The provision places absolutely no restrictions on the subsequent disclosure of medical records by anyone receiving the records. Once the records are out the door for any of the myriad exceptions in this provision, they are fair game for anyone.

We agree that information should be disclosed only with the consent of t[redacted]stomer, as provided in (a)(1), but this right is rendered m[redacted]gless with the extensive laundry list of exceptions

that swallows this simple rule. We shall only discuss a few of these exceptions.

The provision allows financial institutions to provide medical records, including genetic information, for purposes of underwriting. As a result, customers could find themselves being uninsurable, or facing whopping rate increases for health insurance, based upon their genetic information, or health records. In addition, the information may be inaccurate, but the customer cannot correct it.

The provision allows financial institutions to provide medical records for "research projects." This term is undefined, and could include marketing research, or nearly anything else. For example, a customer's prescription drug information could be provided to a drug company doing marketing research on candidates for a new related drug.

Moreover, the provision establishes no research protections for individually identifiable records. The majority of human subject research studies conducted in this country are subject to the Common Rule, a set of requirements for federally-funded research. Analogous requirements apply to clinical trials conducted pursuant to the FDA's product approval procedures. The Common Rule dictates that a study must be approved by an entity that specifically examines whether the potential benefits of the study outweigh the potential intrusion into an individual's private records and whether the study includes strong safeguards to protect the confidentiality of those records. Two weeks ago at a hearing before the Health and Environment Subcommittee, witnesses from the National Breast Cancer Coalition and the National Organization for Rare Disorders testified that these Federal standards should be extended to all research using individually-identifiable medical records. Extending these protections would strengthen confidence in the integrity of the research community and encourage more individuals to participate in studies. Because this provision establishes no protections for individually-identifiable records, it could actually stifle research.

The provision allows the disclosure of confidential medical records "in connection with" a laundry list of transactions, most of which have nothing to do with medical records. The provision does not define who can receive the records, but instead allows disclosure to anyone, so long as it is "in connection with" a transaction. There was no explanation at the markup why medical records should be disclosed in connection with "the transfer of receivables, accounts, or interest therein." There is no definition of "fraud protection" or "risk control" for which the provision also authorizes disclosure. The provision gives carte blanche to financial institutions to disclose confidential medical records for "account administration" or for "reporting, investigating, or preventing fraud." Reporting to whom? An investigation by whom?

While most laws protecting medical records provide for disclosure in compliance with criminal investigations, those laws provide safeguards to permit the individual the opportunity to raise legal issues. This provision does not. In fact, as is the case with a[redacted]ther disclosures in this provision, the consumer would not ev[redacted]in-formed that the information has been disclosed. Thus, a cu[redacted]er's

medical records could be disclosed to an opponent in a civil action without the customer even knowing it.

Within hours of passage of this provision, we began learning from patient groups and others who have fought to improve the privacy rights of individuals that this provision is seriously flawed. These concerns demonstrate why Congress needs to deal comprehensively with the issue of medical confidentiality, not in a slapdash amendment that has received no scrutiny. The Health and Environment Subcommittee of the Commerce Committee has already held a hearing on medical privacy, and a Senate committee has held multiple hearings on the subject. We look forward to enacting real medical information privacy provisions that will truly protect individuals. Unfortunately, this premature move by the Committee will actually set back the health and medical information privacy rights of all Americans.

JOHN D. DINGELL.
HENRY A. WAXMAN.
EDWARD J. MARKEY.
RICK BOUCHER.
EDOLPHUS TOWNS.
FRANK PALLONE, Jr.
SHERROD BROWN.
BART GORDON.
PETER DEUTSCH.
BOBBY L. RUSH.
RON KLINK.
BART STUPAK.
TOM SAWYER.
ALBERT R. WYNN.
GENE GREEN.
TED STRICKLAND.
DIANA DEGETTE.
THOMAS M. BARRETT.
LOIS CAPPS.

O

016 TREAS LEG AFFAIRS 07/30/99 FRI 08:59 FAX 202 622 0534

Congress of the United States

Washington, DC 20515

July 22, 1999

will lose

Dear Democratic Colleague:

We write to urge your strong support for the Motion to Instruct Conferees on the Financial Services Act of 1999, or H.R. 10. The Motion to Instruct Conferees listed below has three elements critical to ensuring a balanced bill which adequately addresses the important issues of financial privacy, equal and non-discriminatory access to financial services, and medical privacy.

MOTION TO INSTRUCT CONFEREES ON H.R. 10

Mr. LaFalce moves to instruct the conferees on the part of the House on the Bill H.R. 10/S. 900 and the House amendment thereto, to ensure, consistent with the scope of the conference, that:

1. Consumers have the strongest consumer financial privacy protections possible, including protections against the misuse of confidential information and inappropriate marketing practices, and ensuring that consumers receive notice and the right to say "no" when a financial institution wishes to disclose a consumer's nonpublic personal information for use in telemarketing, direct marketing, or other marketing through electronic mail; and

2. Consumers enjoy the benefits of comprehensive financial modernization legislation that provides robust competition and equal and non-discriminatory access to financial services and economic opportunities in their communities; and

3. Consumers have the strongest medical privacy protections possible, and thereby prevent financial institutions from disclosing or making unrelated uses of health and medical and genetic information without the consent of their customers, and therefore agree to recede to the Senate on Subtitle E of Title III of the House amendment.

Should you have any questions regarding this important issue, please do not hesitate to contact us, or our staff members, Tricia Haisten (Banking Committee) x54248 or Consuela Washington (Commerce Committee) x53641.

Sincerely,

John J. LaFalce

John D. Dingell

Bruce F. Vento

Henry A. Waxman

Barney Frank

Edward J. Markey

United States General Accounting Office

GAO

Draft Report to Chairman, Subcommittee on Health, Committee on Ways and Means, House of Representatives

JULY 1999

MEDICARE

Improvements Needed By HCFA to Enhance Protection of Confidential Health Information

Notice: This draft is restricted to official use.

This draft report is being provided to obtain advance review and comment from those with responsibility for the subjects it discusses. It has not been fully reviewed within GAO and is, therefore, subject to revision.

Recipients of this draft must not, under any circumstances, show or release its contents for purposes other than official review and comment. It must be safeguarded to prevent publication or other improper disclosure of the information it contains. This draft and all copies of it remain the property of, and must be returned on demand to, the General Accounting Office.

B-282540

Insert Date

DRAFT

The Honorable Bill Thomas

Chairman, Subcommittee on Health

Committee on Ways and Means

House of Representatives

Dear Mr. Chairman:

The Health Care Financing Administration (HCFA) in the Department of Health and Human Services (HHS) processes the nation's largest collection of health care data, with information on 39 million Medicare beneficiaries. To discharge its responsibilities, HCFA must collect personally identifiable health information on Medicare beneficiaries. Such information includes names, addresses, and health insurance claim numbers as well as various diagnoses and types of treatment received by beneficiaries. This information is used by HCFA for a variety of purposes, including the payment of approximately 900 million Medicare claims annually and the conduct of research to evaluate policy, adjust payment rates, improve program operations, and make recommendations for legislative changes to the Medicare program.

DRAFT

DRAFT

Much of the personally identifiable information that HCFA collects on Medicare beneficiaries is protected by the Privacy Act of 1974. This law, which governs the collection, maintenance, and disclosure of federal agency records, balances the government's need to maintain information about individuals with their right to be protected against "unwarranted invasions" of their privacy. State laws also protect the privacy of certain personally identifiable medical information, but these laws vary greatly in their scope and the specific protections afforded. To create a more uniform set of protections that would affect all users of confidential medical information, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that unless the Congress enacts a health privacy law establishing standards for the electronic exchange of health information by August 21, 1999, HHS must promulgate health privacy regulations within the following 6 months.

In response to your request, we are reporting on four areas related to HCFA's use of personally identifiable health information: 1) the need for personally identifiable health information to manage the Medicare program and accomplish other purposes; 2) HCFA's policies and practices regarding disclosure of information on Medicare beneficiaries; 3) the adequacy of HCFA's safeguards for protecting the confidentiality of electronic information and the monitoring of others' protection of beneficiary information; and 4) the effect on HCFA of state restrictions on the disclosure of confidential health information. Appendix I contains a discussion of our scope and methodology. We conducted our work

DRAFT

DRAFT

from April through June 1999 in accordance with generally accepted government auditing standards.

RESULTS IN BRIEF

To carry out its legislated responsibilities, HCFA needs to collect and maintain personally identifiable health information on its 39 million Medicare beneficiaries. For example, it needs personally identifiable information about beneficiaries' demographics, enrollment, and utilization of health care services to pay claims, determine the initial and ongoing eligibility of beneficiaries, and review the access, appropriateness, and quality of care beneficiaries receive. In addition, HCFA uses this information for essential research activities that can lead to improvements in rate-setting, services provided, and quality of care.

HCFA's policies and practices regarding disclosure of personally identifiable health information are designed to be consistent with the provisions of the Privacy Act. For example, HCFA may disclose information without an individual's consent under certain circumstances which could include research purposes or authorized civil and criminal enforcement activities. In accordance with the Act, HCFA officials attempt to balance the information needs of data requestors with the need to protect the confidentiality of personally identifiable health information when determining whether to disclose information. HCFA screens requests for personally identifiable information on Medicare beneficiaries from non-HCFA

DRAFT

DRAFT

researchers more thoroughly than from HCFA staff who need the data to conduct the agency's business. For example, non-HCFA researchers, such as those funded by private foundations, must agree to a set of conditions specifying how they will use the data and protect beneficiaries' confidentiality as well as provide details on how the disclosure of information will address the goals of HCFA's research program. However, we found that HCFA does not have the ability to provide beneficiaries with an accounting of the disclosures it makes, a capability called for by the Privacy Act. Moreover, HCFA cannot provide oversight agencies such as the Office of Management and Budget (OMB) with complete information on its Privacy Act activities. In addition, HCFA does not always clearly inform Medicare beneficiaries of the purposes for which their information may be disclosed to other organizations as required by the Privacy Act. To address these issues, HCFA has established a new executive confidentiality board and initiated a number of actions in response to January 1999 OMB guidance to all agencies to review information practices for compliance with the Privacy Act.

Although few complaints about Privacy Act violations have been made to date, weaknesses in the implementation of HCFA's policies could potentially compromise the confidentiality of health information on Medicare beneficiaries. Specifically, HHS' Office of Inspector General (OIG) continues to find vulnerabilities in HCFA's and its contractors' management of electronic information that could lead to unauthorized individuals reading, disclosing, or tampering with confidential information. In addition, because HCFA does not routinely monitor contractors and others such as researchers who use personally identifiable Medicare

DRAFT

DRAFT

information, its ability to prevent unauthorized disclosure or use and to provide timely corrective action for those that might occur is not assured. HCFA officials told us they are in the process of addressing the OIG findings. However, HCFA's ability to make progress in this area is currently affected by the agency's efforts to direct resources to address computer requirements for the year 2000 so that there will be no interruption of services and claims payments for beneficiaries and providers.

Some states prohibit the disclosure of sensitive health related information, such as human immunodeficiency virus (HIV) status, except for specified purposes. HCFA officials told us these state laws have not prevented the agency from receiving information necessary for paying claims. HCFA's policy is to respect state laws regarding sensitive health information that are more restrictive than federal requirements, so HCFA has allowed states to withhold information on HIV and acquired immunodeficiency syndrome (AIDS) and sexually transmitted diseases (STD) for certain surveys of nursing home patients. However, HCFA may change its policy of allowing states to withhold this information as the agency moves toward payment systems that depend on diagnostic information. If HCFA were restricted in receiving uniform health information from across the country, it could adversely affect the agency's ability to set rates, monitor for quality, and conduct or support health-related research.

We are making a number of recommendations to HCFA to improve the protection of confidential information on Medicare beneficiaries.

DRAFT

DRAFT

B-282540
BACKGROUND

The Medicare Program, created by the Social Security Amendments of 1965 and administered by HCFA was initially established to provide health insurance for most persons aged 65 or older. In 1972, the program was broadened to cover the disabled and people with end-stage renal disease (ESRD) requiring dialysis or kidney transplants. Medicare is a combination of two programs, each with its own enrollment, coverage, and financing—Hospital Insurance (commonly referred to as Part A) and Supplemental Medical Insurance (commonly referred to as Part B). Medicare Part A helps pay for care in hospitals, hospice care, and post-hospital care in skilled nursing facilities and by home health agencies. Medicare Part B helps pay for doctors, outpatient hospital care, home health care not covered under Part A, and other medical services such as the services of physical and occupational therapists. In addition, the Balanced Budget Act of 1997 created a new Part C, establishing Medicare+Choice which provides coverage to beneficiaries through health insurance options such as managed care.

In protecting the confidentiality of health information of its beneficiaries, HCFA's activities, like those of other federal agencies, are governed by the Privacy Act of 1974. The Privacy Act requires that agencies limit their maintenance of individually identifiable records to those that are "relevant and necessary" to accomplish an agency purpose. Federal agencies store personally identifiable information in "systems of records." A system of records is a group of records under the control of a federal agency from which information can be retrieved by the name of an individual or an identifier such as a number assigned to the individual. The Privacy Act defines a record as any item, collection, or grouping of information maintained

DRAFT

DRAFT

by an agency that contains an individual's name or other identifying information. It could include information on education, financial transactions, and medical history. Under the Privacy Act, federal agencies must inform the public through publication in the Federal Register of any establishment or revision of a system of records. In the case of HCFA, 62 of its 81 systems of records relate directly to Medicare beneficiaries.[1] HCFA's systems of records contain information stored in electronic and paper form. HCFA stores personally identifiable data on a Medicare beneficiary's enrollment and entitlement to benefits; demographic information such as age, race, ethnicity, and language preference; and diagnoses and utilization of medical services.

The Privacy Act generally prohibits the disclosure of individuals' records without their consent. However, it allows the disclosure of information without an individual's consent under 12 circumstances called "conditions of disclosure," such as disclosure by a federal agency to its employees based on their need for records to perform their duties. Another condition of disclosure allows an agency to establish "routine uses". These are uses of the information that are determined by the agency to be compatible with the purposes for which it is collected and which are published in the Federal Register. Personally identifiable information can be disclosed when the agency determines that the disclosure is for an established routine use. While the Privacy Act permits agencies to disclose information, it does not require that they do so; they can, for example, determine that in a particular case the

[1]Its other systems of records contain information on Medicaid recipients, health care providers, and HCFA employees.

DRAFT

DRAFT

privacy interest outweighs the public interest in disclosure. However, an agency must always disclose information maintained about an individual to that individual at his request.

A beneficiary may bring a civil action against an agency for alleged Privacy Act violations. These violations may include failure to: grant an individual access to his record, amend a record as requested, or properly maintain an individual's record with adverse consequences resulting for the individual. Respective remedies include granting access to the record, amending the record, and awarding $1,000 or more in damages. In all cases, successful plaintiffs also can be awarded attorney fees and litigation costs.

Criminal penalties up to $5,000 may be assessed against an agency official or employee who: 1) willfully discloses material to an agency or individual not entitled to receive it, 2) willfully maintains a system of records without meeting the notice requirements of the Act, or 3) knowingly and willfully requests or obtains agency records about an individual under false pretenses.

HCFA NEEDS PERSONALLY IDENTIFIABLE INFORMATION ON MEDICARE BENEFICIARIES

For HCFA, personally identifiable health information is essential to the day-to-day administration of the Medicare program. Of most significance, HCFA and its contractors need to use personally identifiable information on patients and their diagnoses and treatments

DRAFT

DRAFT

received to pay approximately 900 million fee-for-service claims annually from providers, suppliers and others. HCFA also uses personally identifiable information to determine the initial and ongoing eligibility of Medicare beneficiaries, make monthly payments to over 390 Medicare managed care plans, and track which managed care plans have been selected by over 6 million Medicare beneficiaries.

HCFA and its contractors also use beneficiary claims data containing personally identifiable information to carry out essential program integrity activities by profiling patients and providers to identify inappropriate claims and inappropriate use of services, for fraud and abuse prevention, and investigations as well as other purposes. Other HCFA activities that rely on personally identifiable information include: coordinating with insurers, employers and others in administering the Medicare Secondary Payer program[2]; developing fee schedules and payment rates used in fee-for-service claims processing; reviewing the access, appropriateness and quality of care received by beneficiaries; and conducting research and demonstrations which include the development and implementation of new health care payment approaches and financing policies as well as the evaluation of the effect of HCFA's programs on beneficiaries' health status.

An example of how HCFA uses personally identifiable information to improve the health of Medicare beneficiaries is the agency's ongoing campaign to increase influenza vaccination

[2]The Medicare Secondary Payer provision limits payment under Medicare for otherwise covered items or services if that payment has been made or can reasonably be expected to be made from another source such as under a workmen's compensation law, automobile or liability insurance policy, or certain health plans. In such cases, Medicare payments for items or services are conditional payments, with Medicare entitled to reimbursement from the other sources for the full amount of Medicare payments.

DRAFT

DRAFT

rates. Using individual identifiers, HCFA links the bills it receives to its eligibility files to determine age, gender, race and geographic location of beneficiaries who have not received influenza vaccinations. HCFA then works with community groups to reach out to the specific groups and areas with low immunization rates. HCFA staff told us that this outreach is helping the agency make progress on meeting the Department of Health and Human Services Healthy People 2000 goals for immunization.

HCFA DISCLOSES INFORMATION ABOUT MEDICARE BENEFICIARIES FOR AUTHORIZED PURPOSES

In screening requests for identifiable information, HCFA determines whether disclosure is authorized by the Privacy Act. It also uses different levels of review depending upon the type of organization making a request for information. HCFA's policy and practice is generally to limit disclosures to information needed to accomplish the requestor's purposes. However, its recordkeeping system for tracking and reporting on disclosures and its notices to beneficiaries that their information could be disclosed have weaknesses.

HCFA Screens Requests for Personally Identifiable Information

In making decisions about whether to disclose information, HCFA's primary criterion is whether or not the request is permitted under one of 12 conditions of disclosure in the Privacy

DRAFT

DRAFT

Act. HCFA officials view the establishment of routine uses for each of its systems of records as a key protection of personally identifiable information that could be disclosed to federal agencies other than HHS or organizations outside of the federal government. In screening requests for personally identifiable information on beneficiaries, HCFA officials balance the information needs of data requestors with the need to protect the confidentiality of beneficiaries' health information. HCFA can disclose information for health services research projects to publicly and privately funded researchers and to public agencies such as the Agency for Health Care Policy and Research, and the Department of Veterans Affairs; to qualified state agencies for the purposes of determining, evaluating, or assessing cost, effectiveness, or quality of health care services provided in a state; to insurers, underwriters, employers who self-insure, and others for coordination of benefits with the Medicare Secondary Payer program; to the Bureau of the Census for census-taking purposes such as assuring an accurate count of the aged; and to congressional offices acting on behalf of beneficiaries.[3]

HCFA has different levels of review depending upon the type of organization making a request for information. Generally, the fewest requirements for justifying the need for personally identifiable information are placed on HCFA staff. According to HCFA policy, HCFA employees should access personally identifiable information on Medicare beneficiaries only when the use of such information is integral to the completion of their official duties.

[3] GAO also receives personally identifiable information from HCFA. GAO's right to receive such information from federal agencies is not restricted by the Privacy Act.

DRAFT

DRAF

The decision to permit access by HCFA staff is made by officials throughout the agency who are responsible for various information systems.

HCFA places additional requirements on other HHS employees and contractors before permitting disclosure of information to them. To receive HCFA data, they must submit written requests and signed data use agreements to HCFA's Office of Information Services. These signed agreements indicate their understanding of the confidentiality requirements of the Privacy Act and HCFA's data release policies and procedures. These policies and procedures include a requirement that the data user will not publish or release information that could permit deduction of a beneficiary's identity.

Other federal agencies and organizations such as state governments and law enforcement agencies that seek information on Medicare beneficiaries must meet another level of requirements to gain access. HCFA staff in the Office of Information Services first determine whether the request reflects a routine use or other condition of disclosure as allowed by the Privacy Act. If so, they determine whether the request is compatible with the purpose for which the information was originally collected. They also review the request to ensure that all Privacy Act requirements and HCFA's data release policies are met. HCFA officials told us that they rely on the requesting organization to provide the initial certification that its activities require the personally identifiable information it is seeking. To make these assessments, HCFA requires that the requesting organization submit a request on its letterhead providing the purpose for which the data are needed, a description of the methodology or the project in which the data will be used, the specific files being requested, the criteria for data

DRAFT

DRAFT

selections or searches and, in most cases, a signed data use agreement.[4] For civil or criminal law enforcement activities, HCFA requires a written request from the head of the law enforcement agency or delegated official which references the law to be enforced as well as the civil or criminal court case number. When information is requested pursuant to a court order, HCFA requires a copy of the court order and guidance from HCFA's Office of General Counsel before personally identifiable information is disclosed.

In screening requests for outside research projects, HCFA imposes yet another level of requirements. For research requests received from researchers not funded by an HHS agency, HCFA officials told us that they not only conduct a review to determine whether disclosure would be permitted under the Privacy Act, but they also evaluate the requests to determine if the purpose: 1) requires the use of identifiable data, 2) is of sufficient importance to warrant the risk to the individual that additional exposure of the record might bring, and 3) is likely to be accomplished because the project is soundly designed and properly financed. For these researchers, HCFA officials review a detailed protocol or study design to evaluate whether the proposed research will address the goals of HCFA's own research program and thus further knowledge of health care access, cost, quality, service delivery, or financing. In the case of research funded by other HHS agencies, HCFA requires, but does not itself review, a copy of the study protocol approved by project officers in agencies such as the National Institutes of Health and the Agency for Health Care Policy and Research.

[4] In the case of some organizations, such as the HHS OIG, the Medicare Payment Advisory Commission, and GAO, a data use agreement is requested, not required.

DRAFT

DRAFT

Approval by the HCFA Administrator is required when researchers request the names and addresses of Medicare beneficiaries from whom they wish to collect data. If the project is approved, the researcher must send potential participants a special notification letter signed by the HCFA Administrator, indicating that HCFA is cooperating with the researcher by providing a list of potential participants for the study. The letter indicates that the beneficiaries do not have to participate in the research project and their Medicare benefits will not be affected by their decision. Seven to ten days after the HCFA letter is mailed, the researcher can contact the beneficiaries directly to see if they wish to participate. In a recent example, the HCFA Administrator approved a request from a university researcher for a "names and addresses file" of Medicare beneficiaries in two Pennsylvania cities for a study entitled "Keeping Older Community Members Safe in Their Homes." This study, funded by the state of Pennsylvania, consists of surveys and in-home interviews and is being conducted to improve the in-home health and safety of the Medicare beneficiary population by developing community action programs in the two cities.

HCFA Generally Limits Disclosures to Information Needed to Accomplish Purposes

HCFA officials told us their practice is to disclose the least amount of personally identifiable information to a requestor that will accomplish the requestor's purpose. HCFA generally provides requestors one of three types of data files. These are public use files, which are stripped of identifying information on beneficiaries; beneficiary-encrypted files, which allow the potential identification of beneficiaries; and files which contain explicitly identifiable

DRAFT

DRAFT

information, such as health insurance claim numbers.[5] HCFA officials told us that they direct requestors whenever possible to either public use files or to beneficiary-encrypted files rather than to the files containing more identifiable beneficiary information. HCFA does not generally customize data files by removing elements for the specific purpose of reducing the amount of personally identifiable information disclosed.

Public use files include some of the most frequently requested HCFA data for analyzing health care spending trends and formulating programs to improve the quality and effectiveness of health care. Data elements that can directly identify an individual and elements or combinations of elements from which an individual's identity can be deduced have been removed from or modified in these files. For example, date of birth may be converted to an element containing 5-year age groups.

HCFA staff said that beneficiary-encrypted files may be sufficient to meet requestors' needs when public use files are not adequate. Beneficiary-encrypted files are data sets where HCFA has encoded or removed the health insurance claim number, date of service, beneficiary name, beneficiary zip code, provider information, or other such elements. For example, a beneficiary's health insurance claim number might be replaced by a randomly generated number. HCFA defines these files as "implicitly" identifiable because they contain data elements that could be combined or linked with other available information to possibly deduce a beneficiary's identity.

[5] A health insurance claim number consists of the Social Security number of the primary Medicare subscriber followed by a letter indicating whether the number belongs to the primary holder or the spouse as well as certain

DRAFT

DRAFT

Other requestors, however, may make a case to HCFA that they need files with "explicitly" identifiable information such as names, addresses or health insurance claim numbers. As mentioned previously, HCFA officials have approved the disclosure of files with the names and addresses of Medicare beneficiaries. HCFA has provided non-federally funded researchers with other data files containing health insurance claim numbers. For example, HCFA recently approved research requests for data from the Surveillance, Epidemiology, and End Results (SEER) joint project conducted by HCFA and the National Cancer Institute; the End Stage Renal Disease (ESRD) File on patients receiving treatment for renal disease; and a variety of "standard analytical files," describing inpatient and other types of care received by Medicare beneficiaries.

Before HCFA discloses implicitly or explicitly identifiable information to other organizations, it generally requires the requestors to sign a data use agreement. By signing, a requestor agrees to abide by HCFA's confidentiality requirements including safeguarding the data, prohibiting subsequent use of the data for a different purpose, and destroying or returning the data within a specified time period. For implicitly identifiable data (beneficiary-encrypted files), requestors also must agree that they will not attempt to identify any specific individual whose record is included in the file. Individuals receiving public use files are not required to sign data use agreements because these files do not contain personally identifiable health information.

---

other information such as whether the beneficiary qualifies because of age or disability.

DRAFT

DRAFT

B-282540
HCFA's Recordkeeping System for Tracking and Reporting Has Weaknesses

HCFA does not have the ability to provide beneficiaries with an accounting of the disclosures made of their personally identifiable information as required by the Privacy Act. In addition, the agency is unable to give oversight agencies information on related Privacy Act activities. HCFA's establishment of an executive-level beneficiary confidentiality board in May 1999 and actions it is taking in response to January 1999 guidance from OMB may help address these issues.

Although Medicare beneficiaries have the right under the Privacy Act to ask for an accounting of disclosures of their personally identifiable information and to examine or amend their individual records, HCFA's recordkeeping system is incapable of readily providing such information to beneficiaries. The Privacy Act requires that this accounting include information on the nature and purpose of the disclosure and the name and address of the person or organization to whom the disclosure was made. HCFA staff told us that the agency's computerized system for tracking disclosures does not have the capability to easily generate information for an individual beneficiary on disclosures made from HCFA's systems of records. HCFA's primary method of accounting for disclosures involves tracking data use agreements, which are filed by the names of requestors and not by HCFA's systems of records. HCFA officials told us that they were not aware of any beneficiaries having requested information from HCFA about disclosures involving their personally identifiable information.

DRAFT

DRAFT

In addition, HCFA officials told us that they are trying to develop a system that will not only allow them to meet current OMB requirements but also to better account for disclosures of personally identifiable information made to other organizations. HCFA officials told us that as directed by OMB, they have begun reviewing their recordkeeping of Privacy Act activities. In January 1999, OMB issued guidance as a result of a May 14, 1998, Presidential memorandum directing each agency to review its information practices to ensure compliance with the Privacy Act. The OMB guidance stated that agencies can protect individual privacy by limiting the amount of information they maintain about individuals and ensuring that such information is relevant and necessary to accomplish an agency purpose. OMB has asked agencies to reevaluate the relevance and necessity of personally identifiable information maintained on individuals, the appropriateness of current safeguards, and the continuing justification to disclose personally identifiable information for routine uses. OMB has also asked agencies to review their procedures for accounting for disclosures to improve individuals' ability to determine who has seen their records and when they were seen. HCFA has begun to address OMB guidance and officials told us they expect to reduce the number of routine uses permissible for HCFA's systems of records.

In May 1999, HCFA also established a Beneficiary Confidentiality Board to review issues relating to the protection of confidential information, including HCFA's policies and procedures for disclosing personally identifiable information. The Board will consist of selected members from HCFA's executive council and will review strategic issues relating to the protection of confidential patient information. It will focus on balancing the privacy

DRAFT

DRAFT

interests of Medicare beneficiaries with the public interest of HCFA's need to collect and release individually identifiable information.

Weaknesses in HCFA's recordkeeping system also affects its ability to report on its Privacy Act activities. The Privacy Act requires the President to report to Congress on the Privacy Act activities of the executive branch on a biennial basis. In implementing this provision of the Privacy Act, OMB requires reports from executive branch agencies. In the guidance sent to agencies for this report, OMB requires that agencies provide the number of individuals who have requested access to their files or have requested that the agency amend the information maintained in their files. However, HCFA officials told us they did not provide such information for Medicare beneficiaries in their reports to HHS for eventual submission to OMB. HCFA officials told us that as a result of our discussions with them, they have begun to revamp their information system to more effectively report on their Privacy Act activities in 2000, when the next biennial report is due.

Notifications to Beneficiaries that Their Information Could Be Disclosed Are Not Always Clear or Comprehensive

The Privacy Act requires federal agencies to permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by the agencies. The Act requires an agency to notify individuals of the following when it collects information: 1) the authority under which the Agency is collecting the information, 2) the principal purpose for

DRAFT

DRAFT

which the information is intended to be used, 3) routine uses that may be made of the information, and 4) whether the individual is required to supply the information and the effects on the individual of not providing the requested information.[6] Although we found that some of HCFA's Privacy Act notifications provide beneficiaries with all the information required by the Privacy Act, we found others to be deficient.

HCFA officials told us there are over a dozen different Privacy Act notifications that they use when collecting information from beneficiaries. An individual's first exposure to a Medicare-related Privacy Act notice is usually at the time of his application for Social Security retirement benefits. These applicants receive a multi-page Privacy Act notice providing the information required by the Privacy Act. Approved Social Security retirement benefit applicants are automatically enrolled in Medicare at age 65. HCFA officials told us that after enrollment in Medicare, beneficiaries should receive other Privacy Act notifications whenever the agency collects information about them. This can be if they separately enroll in Medicare Part B, receive medical care, participate in a survey or are enrolled in a demonstration testing a new delivery or payment system. For beneficiaries receiving ongoing care, providers must obtain signature cards from beneficiaries attesting that they have been advised of the collection and use of their information. In the case of physician services, this is usually done the first time the beneficiary sees the physician. In the case of other services, such as a hospitalization, the notification signature cards are obtained at each encounter. For the 15 percent of Medicare beneficiaries enrolling directly with a managed care plan, however, HCFA officials told us that

[6]The Privacy Act also requires a federal agency to permit an individual to gain access to information pertaining to him in the agency's records, to have a copy made of the record, and to seek correction or amendment of the

DRAFT

DRAFT

the agency does not require these plans provide a Privacy Act notification. HCFA officials told us that since all Medicare+Choice beneficiaries must also be enrolled in Medicare Parts A and B, HCFA relies on the Medicare Parts A and B enrollment notices as the primary vehicles through which these beneficiaries learn about Privacy Act requirements.

While some of the HCFA Privacy Act notification forms we reviewed contain the required information, we found others that do not tell beneficiaries the purposes for which their information may be disclosed outside of HCFA or do so in an unclear fashion. For example, a form for beneficiaries receiving services in skilled nursing facilities provided the required information by advising beneficiaries why the information was being collected and when the personally identifiable information could be disclosed outside the agency under the Privacy Act's routine uses provision. It advised that the information collected during a nursing home stay would be used to track changes in health and functional status over time to evaluate and improve the quality of care provided by nursing homes that participate in Medicare. In contrast, we found the wording of the Privacy Act notice for Medicare Enrollment Form for Part B services was cursory at best. The Part B form did not identify the routine uses that would be made of the beneficiary's information. Instead, it provided only a vague reference to the Federal Register as a source for such information. Specifics to help beneficiaries locate relevant sections of the Federal Register were absent. We also found problems in a form used to collect information on end-stage renal disease beneficiaries. This form did not mention routine uses for the information collected and did not refer beneficiaries to sources that could provide this information.

---

record.

DRAFT

DRAFT

INADEQUATE HCFA SAFEGUARDS COULD COMPROMISE CONFIDENTIALITY

HCFA's safeguards for protecting the confidentiality of Medicare beneficiaries' health information are inadequate. Several audits conducted by the HHS OIG point out weaknesses in how HCFA safeguards electronic information. In addition, HCFA has conducted only limited reviews of safeguards used by carriers and fiscal intermediaries in the last 2 years, and it does not routinely monitor the confidentiality protections of other organizations receiving personally identifiable Medicare information. Agency officials told us they are in the process of taking action to correct the weaknesses identified by the OIG. However, consistent with priorities established by OMB, HCFA has a moratorium on software and hardware changes until it is compliant with year 2000 computer requirements.

HCFA Systems Security Manual Generally Follows OMB Guidance For Safeguarding Electronic Information

Under the Privacy Act, HCFA must establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records. OMB Circular A-130 provides agencies with guidance for safeguarding federal information resources including paper and electronic records. Appendix III of the Circular provides detailed guidance for

DRAFT

DRAFT

safeguarding electronic records. This 1996 circular provides guidance on management controls, such as assignment of responsibility for security, the development of a security plan and ongoing review of security controls. It notes that a security plan should include mandatory periodic training in computer security and restricting users to the minimum access or type of access necessary to perform their jobs. A security plan is also expected to outline techniques for safeguarding the security of information and to establish a formal mechanism for responding to intruders or other incidents that can compromise the security of a computer system. HCFA's systems security manual generally adheres to OMB's guidance for safeguarding electronic information. In addition, HCFA's policy for Internet usage requires encryption to protect data. It calls for authentication or identification procedures to ensure that both the sender and the recipient are known to each other and are authorized to receive and decrypt such information.

Problems Exist with HCFA Safeguards Over Electronic Information

HHS' OIG has identified control weaknesses with HCFA's safeguarding of confidential information.[7] The fiscal years 1997 and 1998 financial statement audits conducted by the OIG identified a variety of problems with HCFA's safeguards for electronic information at HCFA's central office and for selected Medicare contractors. The OIG reported the need for HCFA to

[7] For a discussion of the OIG work, see Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, Sept. 23, 1998). In February 1997, we designated information security as a high risk government operation. Government operations have been identified as "high risk" because of their greater vulnerabilities to waste, fraud, abuse, and mismanagement. High-Risk Series, An Update (GAO/HR-99-1, January 1999).

DRAFT

DRAFT

implement an overall security structure to achieve security program objectives and discussed weaknesses in the following areas: computer access controls (techniques to ensure that only authorized persons access the computer system), segregation of duties (the division of steps among different individuals to reduce the risk that a single individual could compromise security), and service continuity (the ability to recover from a security violation and provide service sufficient to meet the minimal needs of users of the system). The OIG also reported problems with controls over operating system software integrity and application development and change controls. System software controls are critical in preventing unauthorized as well as authorized users from circumventing security controls that permit an organization to monitor access to systems programs and files. Application development and change controls ensure that only authorized programs and modifications are implemented. Without proper controls, there is a risk that security features could be omitted or turned off either inadvertently or deliberately.

As part of its work at 12 Medicare contractors for the fiscal year 1998 financial statement audit, the OIG noted that auditors were able to penetrate the security and obtain access to sensitive Medicare data at five Medicare contractors. The auditors' ability to do so without using their formal access privileges is of particular concern because unauthorized users can exploit this security weakness and confidential medical data may be compromised in several ways--unauthorized individuals could be reading confidential data, disclosing it to others, and tampering with it.[8]

DRAFT

DRAFT

Agency officials told us that they are in the process of taking actions to address the OIG financial statement audit findings. However, HCFA's ability to make progress is currently affected by the agency's efforts to address computer requirements for the year 2000 so that there will be no interruption of services and claims payments for beneficiaries and providers. HCFA, consistent with priorities established by OMB, has established a moratorium on instituting software and hardware changes because of the need for compliance with year 2000 requirements.[9] The OIG will evaluate the effectiveness of any corrective actions that HCFA is able to implement during its fiscal year 1999 financial statement audit.

HCFA Does Not Systematically Monitor How Organizations Protect the Confidentiality of Medicare Data

Although HCFA has a process for monitoring systems security at its claims administration contractors—carriers and fiscal intermediaries—agency officials told us that competing demands and resource constraints have prevented them from monitoring whether these

[8] See also Financial Audit: 1998 Financial Report of the United States Government (GAO/AIMD-99-130, Mar. 31, 1999) and Auditing the Nation's Finances: Fiscal Year 1998 Results Highlight Major Issues Needing Resolution (GAO/T-AIMD-99-131, Mar. 31, 1999).

[9] See Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999) and Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999).

DRAFT

DRAFT

organizations follow OMB guidance for protecting the confidentiality of information. In addition, HCFA officials told us that they do not check whether organizations outside of HCFA receiving personally identifiable health information are complying with the requirements of their data use agreements to protect the confidentiality of personally identifiable information.

HCFA's regional offices have oversight responsibility for Medicare contractors. These offices are required to designate Systems Security Coordinators who: 1) provide contractors with technical guidance as needed, 2) monitor compliance with systems security requirements, 3) report systems security problems and activities to central office as needed, and 4) coordinate external audits and respond to findings. In addition, regional offices could potentially evaluate systems security through the Contractor Performance Evaluation (CPE) review process. CPE reviews are intended to evaluate Medicare contractors' compliance with Medicare laws and regulations.

HCFA officials told us that, other than OIG reviews, there were no explicit on-site reviews of contractor's security protections in fiscal years 1997 and 1998 because of resource constraints and the assignment of regional staff to assessing contractor compliance with year 2000 computer requirements. HCFA officials told us that reviews of network security were conducted in 1998 for 12 Medicare contracts in place at four of its 60 claims processing contractors.

DRAFT

DRAFT

HCFA officials also told us that they do not have a system for monitoring whether organizations outside of HCFA have established safeguards for personally identifiable health information received from the agency. When organizations sign data use agreements with HCFA, they agree to establish appropriate administrative, technical and physical safeguards providing a level and scope of security that is not less than the level and scope of security established by OMB. HCFA relies on organizations to monitor their own compliance with the data use agreements.

Data use agreements include a requirement that those receiving information from HCFA can only use data for its HCFA-approved purpose. Without a new approval, researchers are not allowed to make subsequent use of data for a different purpose. An important provision of data use agreements calls for the return or destruction of data upon completion of each project. HCFA officials told us in the past that they tracked the expiration date of data use agreements to determine whether to follow up on the disposition of the data. HCFA officials stated that due to resource constraints, there is a backlog of about 1,400 expired data use agreements and users have not been contacted to establish whether they will return the data to HCFA or destroy it. HCFA officials told us that they plan to reduce the backlog by one-half by September 30, 1999, and continue to make progress on it thereafter. Although HCFA does not systematically monitor compliance with its data use agreements, HCFA officials told us that they scan Internet web sites to see if information is being disseminated without HCFA approval. In addition, they said HCFA staff review research journals and publications to determine if researchers have used HCFA data without appropriate authorization. However, such methods only identify problems after sensitive data have been inappropriately used, and

DRAFT

DRAFT

do not assure comprehensive oversight of the use of these data. In addition, the lack of HCFA monitoring of contractors and others who use personally identifiable Medicare information hampers HCFA's ability to prevent the occurrence of problems and provide timely identification and corrective action for those that have occurred.

Few Complaints of Privacy Act Violations Reported

The agency identified seven complaints of potential violations of the Privacy Act that it has received and resolved in the past 4 years. Six of the complaints involved contractors conducting research for HCFA, health data organizations, and individual researchers. These complaints were raised by similar organizations or other researchers and involved posting potentially identifiable Medicare billing information on an Internet web site; using data obtained for one research project for a second research project without authorization from HCFA and publishing the results of this study; and offering to share Medicare files at a national research conference. In these cases, HCFA provided direction to those involved to clarify and further sensitize researchers to Privacy Act requirements.

The seventh complaint was brought against HCFA and an individual researcher by a Medicare beneficiary. In this instance, the Secretary of HHS received a complaint letter from an attorney representing a Medicare beneficiary who objected to two letters sent to her by a researcher from a major university medical school. The letters asked her to participate in a follow up study of Medicare patients who had undergone a particular surgical treatment for

DRAFT

DRAFT

heart disease. The beneficiary believed that the letters implied that she was under an obligation to participate in the study and wanted to know how her medical history had been shared with the researcher. In an investigation conducted by HCFA, it was determined that data on this beneficiary and others had been released to the researcher. While HCFA determined that appropriate data use agreements had been signed for both sets of data, the agency's investigation also showed that the letters sent by the researcher may have been worded too strongly. In addition, the researcher failed to follow the HCFA notification procedure; instead of sending out the HCFA Administrator's letter in advance of his own mailing, he merely attached it to his first letter to the beneficiary. HCFA sent a letter to the beneficiary's attorney explaining the legal basis for the disclosure of the beneficiary's information and advised that participation in such research is completely voluntary. The letter also indicated that HCFA had taken steps to ensure that the beneficiary would not be contacted for further studies. HCFA received no further correspondence from the beneficiary or her attorney on this matter.

We found no cases related to the Privacy Act brought by Medicare beneficiaries against HCFA, nor from our discussions with HCFA officials are we aware of any cases settled prior to or during litigation. Similarly, we found no evidence of criminal prosecutions for Privacy Act violations.

HCFA reports that only one internal disciplinary action has occurred during the past 5 years related to violations of HCFA's confidentiality policies. The incident involved an agency employee who was accessing beneficiary files more frequently than appeared necessary for

DRAFT

DRAFT

performing his job functions. The employee admitted to looking at the files of "famous people" and he was placed on administrative leave. He eventually signed an affidavit stating that the files had not been sold or shared with other persons and he was allowed to resign.

HCFA staff stated that the agency has never terminated or modified a contract in response to a claims administration contractor's breach of Privacy Act standards. HCFA did report that in 1997, it received a report from one of its contractors that the contractor's director of Medicare payment safeguards had taken a file from the workplace and shared it with her spouse, a doctor employed by the contractor as part of its private line of business. The file concerned an active fraud investigation of another doctor. According to HCFA, the contractor issued a letter of corrective action to remain in the employee's record for one year.

SOME STATES RESTRICT DISCLOSURE OF SENSITIVE CONFIDENTIAL INFORMATION

In its oversight of the Medicare program, HCFA necessarily deals with beneficiaries and providers from every state. In addition to the federal government, the states have laws governing the confidentiality of health information. State laws vary significantly, resulting in what has been called a "patchwork" system of protections. For example, in Minnesota, health records may be disclosed by a provider to an external researcher only after a reasonable effort to obtain patients' consent has been made. The provider must also determine that individually identifiable records are necessary, the researcher's safeguards are adequate, and that the requester will not use the records for purposes other than the original request. In Florida, mental

DRAFT

health records are confidential and may be disclosed only under limited circumstances. In Vermont, all individually identifiable information reported to the state's cancer registry, used in cancer morbidity and mortality studies, is confidential and privileged and may be used only for the purposes of these studies.

In an effort to establish some degree of national uniformity in the area of medical records privacy, HIPAA requires that, unless the Congress enacts a health privacy law establishing standards for the electronic exchange of information by August 21, 1999, the Secretary of HHS must promulgate health privacy regulations within the following 6 months. The proposals Congress is considering differ in the extent to which federal privacy protections would preempt state laws.

Conflicts between HCFA and the states involving medical record disclosures have been minimal, and HCFA's administration of the Medicare program has not been hindered because HCFA officials believe all states permit release of information as needed for health care treatment and payment. If a state law prohibited disclosure of information to HCFA that was critical for treatment or payment purposes, and a federal statute required such disclosure, HCFA officials told us that it would rely on the Supremacy Clause of the U.S. Constitution[10] and its express statutory authority to obtain the necessary records.

[10] U.S.Const. art. VI, cl. 2. The Supreme Court has construed the Supremacy Clause of the U.S. Constitution to hold that federal legislation preempts state law where, for example: 1) the state law directly conflicts with federal law, 2) the federal legislative scheme leaves no room for state regulation, or 3) the state statute frustrates or conflicts with the purposes of the federal legislation.

DRAFT

DRAFT

HCFA officials told us that where information is not critical to HCFA operations, HHS policy is to respect and abide by state laws that provide greater protection for records than would otherwise be required by federal law or regulation. For example, when the states of California and Washington notified HCFA that the laws in their respective states did not authorize the disclosure of diagnostic information related to HIV/AIDS and STDs, HCFA changed the system used to collect and analyze certain nursing home information by allowing states to withhold diagnostic information collected about HIV/AIDS and STDs for their nursing home patients.[11] HCFA officials told us that as many as 19 states have exercised this option by blanking out HIV/AIDS or STD identifiable codes before submitting the requisite information to HCFA.

According to HCFA officials, the deletion of diagnostic information collected about HIV/AIDS and STDs for nursing home patients has not generally affected its operations. They said that when the agency developed its prospective payment system for skilled nursing facilities, it did not use data on beneficiaries with HIV/AIDS and STDs in nursing homes in setting nursing home payment rates. Since HCFA began phasing in the skilled nursing facility prospective payment system in 1998, however, the agency has received requests for additional payment from providers who care for HIV/AIDS patients. HCFA officials acknowledge that the agency now needs to have better information on this population as it refines the new payment system for skilled nursing facilities to ensure that beneficiaries with HIV/AIDS receive the level of care required and that rates are adequate to provide for that care. Similarly, HCFA officials told us that the agency will require diagnostic information as it refines its other payment systems.

[11] The information is used by HCFA to track changes in health and functional status of nursing home residents. The information system is known as the National Minimum Data Set (Resident Assessment Instrument) repository.

DRAFT

DRAFT

CONCLUSIONS

In its role as administrator and overseer of the nation's Medicare program, HCFA must collect and maintain personally identifiable information on millions of beneficiaries to effectively operate and manage the program. In addition, HCFA and others require this information for essential research activities that can lead to improvements in the nation's health care access, financing and quality. As the steward of this confidential information, HCFA must balance privacy concerns of its beneficiaries with its need to effectively manage the program. It must keep an individual's health information safe from inappropriate disclosure.

In carrying out this responsibility, HCFA has implemented policies and practices that are consistent with the Privacy Act and OMB guidance to reduce the likelihood of inappropriate or inadvertent disclosures. In addition, HCFA's protections may be strengthened by its recent establishment of a Beneficiary Confidentiality Board and actions taken in response to OMB guidance to reevaluate the relevance and necessity of personally identifiable information maintained on individuals. However, as the HHS OIG reported, HCFA continues to have vulnerabilities in its information management systems. In addition, HCFA has not consistently monitored its contractors' safeguards for protecting confidential information. As a result, even though few complaints have been made to date, confidential medical information may be at risk. We recognize that HCFA, consistent with priorities set forth by OMB, has focused its resources on ensuring that the agency and its contractors are compliant with year 2000 computer requirements. Nonetheless, we believe that reducing the

DRAFT

DRAFT

vulnerabilities in its information systems and monitoring of contractors are important concerns that HCFA must address.

HCFA lacks the ability to provide beneficiaries with an accounting of what information has been disclosed about them. The agency is also unable to inform oversight agencies about certain Privacy Act activities. In addition, HCFA does not have a system for monitoring organizations to whom it discloses personally identifiable information. As a result, after data are released to an organization, HCFA is unable to systematically reduce the likelihood of inappropriate use of the data or identify instances of such misuse. HCFA can also do a better job of informing beneficiaries that their information could be disclosed. In addition, the agency should be better able to track and report on disclosures of Medicare records. When new information is collected from beneficiaries and they are notified of their rights under the Privacy Act, some of HCFA's notifications are inadequate because they do not tell Medicare beneficiaries the purposes for which their information may be disclosed outside of HCFA or do so in an unclear fashion.

If HCFA were restricted in receiving uniform health information across the country, it could adversely affect internal operations such as rate-setting and monitoring for quality assurance. It could also affect the ability of analysts in HCFA, other federal agencies and non-governmental organizations to conduct policy analysis and health services research because of the difficulty of complying with varying state laws. If the same data elements and health information were not available from all states, it may compromise HCFA's ability to conduct research and analysis to improve Medicare policies.

DRAFT

DRAFT

B-282540

RECOMMENDATIONS TO THE ADMINISTRATOR OF THE HEALTH CARE FINANCING ADMINISTRATION

To improve HCFA's protection of the confidentiality of personally identifiable Medicare beneficiary information, we recommend that the Administrator 1) correct the vulnerabilities identified in its information management systems by the OIG; 2) systematically monitor contractors' safeguards for protecting confidential information; 3) develop a system to routinely monitor other organizations that have received personally identifiable information on Medicare beneficiaries to help ensure that information is used only as approved and identify instances of misuse; 4) ensure that all agency Privacy Act notifications contain the information required by the Act in a manner that is clear and informative to beneficiaries; and 5) implement a system that would permit HCFA to respond in a timely fashion to beneficiary inquiries about the disclosure of their information to others outside HCFA as well as to provide information on Privacy Act activities to OMB and others.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from its issue date. At that time, we will send copies of this report to other interested congressional committees, the Secretary of Health and Human Services, the Administrator of the Health Care Financing Administration, and other interested parties. We will also make copies available to others upon request.

DRAFT

DRAFT

Please contact me at (312) 220-7600 if you or your staff have any questions concerning this report. Staff contacts and other contributors are listed in appendix II.

Sincerely,

Leslie G. Aronovitz

Associate Director

Health Financing and Public Health Issues

DRAFT

APPENDIX I

DRAFT

SCOPE AND METHODOLOGY

We focused our work at HCFA on controls over the disclosure of personally identifiable information involving Medicare beneficiaries. We interviewed agency officials and reviewed documents they provided, including HCFA policies and procedures related to safeguarding and disclosing personally identifiable health information. We also reviewed OMB guidance related to the Privacy Act. We reviewed financial statement audits of HCFA from the Office of Inspector General of the Department of Health and Human Services and the HHS financial management FY 1998 status report and reviewed court cases related to the Privacy Act five-year plan. In addition, we examined the privacy protections of selected state laws and obtained comments from agency officials about the current and future effect of such laws on HCFA's management of the Medicare program. We conducted our work from April through June 1999 in accordance with generally accepted government auditing standards.

DRAFT

DRAFT

GAO Contacts and Staff Acknowledgments

GAO Contacts

Leslie G. Aronovitz (312) 220-7600

Bruce D. Layton (202) 512-6837

Staff Acknowledgments

In addition to those named above, Nancy Donovan, Bonnie L. Brown, Nila Garces-Osorio, Julian Klazkin, Mary Reich, and Craig Winslow made key contributions to this report.

DRAFT

B-282540
RELATED

DRAFT

GAO PRODUCTS

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, Apr. 27, 1999)

Financial Audit: 1998 Financial Report of the United States Government (GAO/AIMD-99-130, Mar. 31, 1999)

Auditing the Nation's Finances: Fiscal Year 1998 Results Highlight Major Issues Needing Resolution (GAO/T-AIMD-99-131, Mar. 31, 1999)

Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Is Limited (GAO/HEHS-99-55, Feb. 24, 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-50, January 20, 1999)

DRAFT

DRAFT

B-282540

Major Management Challenges and Program Risks: Department of Health and Human Services (GAO/OGC-99-7, Jan. 1999)

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, Sept. 28, 1998)

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, Sept. 23, 1998)

(101816)

DRAFT

TOTAL P.43

TOTAL P.43
TOTAL P.42

HIPAA PRIVACY REGULATION TIMELINE

As of July 16, slightly over half of the options papers have been reviewed. Many have been sent back to the working groups for further policy development. No preamble or regulation text has been drafted.

Backing up from an August 27th delivery to the Federal Register, the following time line would be required:

~~Wednesday~~ FRIDAY, July 23	- Deputies meeting about the regulation timetable
	consult w/ DES
Friday, July 30	- Drafting of regulation completed, draft circulated within HHS to oth agencies
Wednesday, August 4	- Comments due back from HHS components & agencies
Friday, August 6	- Meeting with Secretary Shalala to resolve all disputed issues
Tuesday, August 10	- NPRM sent to federal agencies for clearance
Thursday, August 12	- Comments due back to HHS from agencies
Tuesday, August 18	- Cabinet-level meeting to resolve all outstanding issues
August 18-25	- Revise regulation per outcome of Cabinet meeting
Wednesday, August 25	- Re-write complete, send to Federal Register
Friday, August 27	- Publication in Federal Register

Please note that this schedule is highly ambitious, and will require significant commitment by all Departments to achieve.

how many agencies?

State
CIA
Treasury

HHS DATA COUNCIL

Working Group on HIPAA Privacy Regulations

Subcommittee Roster

Last	First	Sub	Address
Block	Abby	3	Chief, Insurance Policy and Information Division, Office Of Personnel Management Phone: (202) 606.0004 Email: ALBlock@opm.gov
Bobroff	Rochelle	4	Office of the General Counsel Office of the Secretary Address: 7500 Security Blvd. C2-05-23 (410) 786-8261 rbobroff@os.dhhs.gov
Braithwaite	Bill	1	Office of the Assistant Secretary for Planning and Evaluation Address: Humphrey Building, Room 440D Phone: (202) 260-0546 Email: bbraithw@osaspe.dhhs.gov
Brice	Ebony	0	Secretary Office of the Assistant Secretary for Planning and Evaluation Phone: (202) 690-7100 Email: ebrice@osaspe.dhhs.gov
Briggs	Aimee	2	Office of the Assistant Secretary for Planning and Evaluation Address: Humphrey Building, Room 442-E Phone: (202) 205-8647 Email: abriggs@osaspe.dhhs.gov
Bruening	Paula	1	Department of Commerce (NTIA) Phone: (202) 482-1816 Email: PBruening@ntia.doc.gov
Brzostowski	John	0	Office of Legislative Affairs Social Security Administration john.brzostowski@ssa.gov

strategy mtg → on gun shot
press strategy

Callahan	Susan	1, 4	Office of the Inspector General Phone: (202) 205-0599 Address: Cohen Bldg. Room 570 Email: scallaha@os.dhhs.gov
Chapper	Amy	1	Center for Beneficiary Services HCFA Address: SOUTH Bldg., Rm. S1-04-25 Phone: (410) 786-0367, Email: achapper@hcfa.gov
Christie	Delores	2	Management Analysis Officer Office of Program Services SAMHSA Address: Parklawn, Room 13C-12 Phone: (301) 443-8859 Fax: (301) 460-7505 Email: Dchristi@samhsa.gov
Cirrincione	Ross	3, 4	Office of the Assistant Secretary for Public Affairs Address: Humphrey Building Rm. 645F Phone: (202) 690-7453 Email: rcirrinc@os.dhhs.gov
Claxton	Gary	0	Deputy Assistant Secretary for Planning and Evaluation (Health Policy) Address: Humphrey Building, Rm. 442E Phone: (202) 690-6870 Email: Gclaxton@osaspe.dhhs.gov
Conrad	Carol	1, 4	Office of General Counsel, PH Division 5600 Fishers Lane, Room 4A-53 Rockville, MD 20857 Phone: (301) 443-2006 email: cconrad@psc.gov
Crank	Dena	0	Chief, Professional Relations Branch Office of Disability, Division of Disability Process Policy Social Security Administration Phone: (410) 966-8198 Email: Dena.Crank@ssa.gov
Davis	Jeff	2	Office of General Counsel Email: jdavis2@os.dhhs.gov

Davis	Ruwanda	2	Federal Bureau of Prisons Freedom of Information and Privacy, OGC 320 First St. NW Washington DC 20534 Phone: (202) 514-6655 Email: RHDAVIS@BOP.GOV
Daynard	Matt	1	Federal Trade Commission mdaynard@ftc.gov (202) 326-3291
Dewaal	Ian	3, 4	Senior Counsel Dept. of Justice – Criminal Division Phone: (202) 514-0669 Fax: (202) 514-6118 Email: Ian.DeWaal3@usdoj.gov
Dorsey	James	2	Center for Health Plans and Providers HCFA Address: CENTRAL Bldg., C4-15-00 Phone: (410) 786-1143 Email: jdorsey1@hcfa.gov
Drew	Glen	3	Senior Policy Analyst FDA Address: Parklawn Bldg., Rm. 1522 (HFY-20) Phone: (301) 827-1695 Email: gdrew@oc.fda.gov
Eden	Donna	1, 4	Office of the General Counsel Office of the Secretary Address: 7500 Security Blvd. C2-05-23 Phone: (410) 786-8859 Email: deden@os.dhhs.gov
Espinosa	Diana	0	Office of Management and Budget Phone: (202) 395-7790 Email: Diana_Espinosa@omb.eop.gov
Fanning	John	2, 3	Privacy Advocate Office of the Assistant Secretary for Planning and Evaluation Address: Humphrey Building, Rm. 440D Phone: (202) 690-5896 Email: Jfanning@osaspe.dhhs.gov

Fischbach	Ruth	3	Senior Advisor for Biomedical Ethics NIH – Office of Extramural Research Building 1, Room 158 1 Center Drive, MSC 0152 Bethesda, MD 20892-0152 Phone: (301) 496-1414 Fax: (301) 402-7062 Email: rlfisch@nih.gov
Fitzmaurice	Michael	3	AHCPR Address: EOC, Rm. 600 Phone: (301) 594-3938 Email: Mfitzmau@AHCPR.GOV
Friedkin	Dawn	1	Department of Commerce Phone: (202) 482-0074 Email: DFriedkin@doc.gov
Golub	Melinda	4	Office of the Inspector General Cohen Bldg., Room 5527 (202) 205-9428 mgolub@os.dhhs.gov
Gottfried	Kate	3, 4	Senior Policy Advisor Office of Public Health and Science DHHS – Room 738G (202) 401-0735 Email: Kgottfried@osophs.dhhs.gov
Hastings	Bob		Social Security Administration Email: bob.hastings@ssa.gov
Heimlich	Judith	1, 2, 3, 4	Department of Labor Health Care Task Force (202) 219-7222 ext. 2177 *email: heimlicj@pwba.dol.gov*
Hennessey	Dorothy	2	Chief MHSAIS Security Program OASD (HA), TMA 5109 Leesburg Pike, #508A Falls Church, VA Phone: (703) 681-3983/8787 Email: Dorothy.Hennessey@tma.osd.mil

Hodahkwen	Lance	2	IHS 12300 Twinbrook Pkwy, Suite 450 Rockville, MD 20837 Phone: (301) 443-5938 Email: Lhodahkw@hqe.ihs.gov
Kaneshiro	Julie	3	NIH – Office of Science Policy Address: Bldg. 1, Rm. 218 Phone: (301) 496-0786 E-mail: KaneshiJ@od.nih.gov
Kaszynski	Mike	2	Insurance Policy and Information Division, Office Of Personnel Management Phone: (202) 606-1994 Email: mwkaszyn@opm.gov
Kelly	Richard	1	Federal Trade Commission rkelly@ftc.gov (202) 326-3304
Langer	Pamela	3	Office of Inspector General Cohen Building, Room 5527 (202) 205-0563 planger@os.dhhs.gov
Lease	Ken	4	Insurance Policy and Information Division, Office Of Personnel Management Phone: (202) 606-0004 Email: kenlease@opm.gov
Levario	Andrea	1	Office of the Assistant Secretary for Legislation Address: Humphrey Building Rm. 405H Phone: (202) 690-7538 E-Mail alevario@os.dhhs.gov
London	Paul	1	Department of Commerce 14th & Constitution Ave., NW, Rm 5039 Email: plondon1@doc.gov Phone: (202) 482-4730 Fax: (202) 482-3610
MacArthur	Anne	1	Office of the Inspector General Phone: (202) 205-9404 Address: Cohen Bldg, Rm 5570 E-mail: amacarth@os.dhhs.gov

Millas	Barbara	0	Assistant Director, VHA Health Information Program 1 Jefferson Barracks Drive St. Louis, MO 63125 Phone: 314-894-5790 Fax: 314-845-5099 Email: Barbara.Millas@med.va.gov
Morgan	Gaylee	0	Office of Management and Budget NEOB 7002 Phone: (202) 395-4908 Fax: (202) 395-5648 Email: Gaylee_L._Morgan@omb.eop.gov
Moushegian	Vahan		Department of Defense Email: moushegv@osd.pentagon.mil
Oslik	Norman	1	Office of Information Resources Management Office of the Assistant Secretary for Management and Budget Address: Humphrey Building, Rm. 531H Phone: (202) 690-8685 Email: noslik@os.dhhs.gov
Pagels	Mike	2	Center for Beneficiary Services HCFA Address: SOUTH Bldg., S1-04-24 Phone: (410) 786-5759 Email: mpagels@hcfa.gov
Peddicord	Joan	2	Social Security Administration Office of the Commissioner Disability Redesign Phone: (410) 966-6491 Email: joan.peddicord@ssa.gov
Pepper	Michael	0	Office of the Assistant Secretary for Planning and Evaluation 200 Independence Ave. SW, Room 447D Phone: (202) 401-7367 email: mpepper@osaspe.dhhs.gov
Perry	Kim	0	Office of Personnel Management Email: kwperry@opm.gov
Pestaina	Kaye	0	Department of Labor Email: PestainK@PWBA.DOL.GOV

Pirt	Nancy	3	FDA Address: Parklawn Bldg., Rm. 1522 Phone: (301) 827-1697 Email: npirt@oc.fda.gov
Powell	Mechelle		Office of the Chief Information Officer Veterans' Administration Phone: (202) 273-6926 Email: Mechelle.Powell@hq.med.va.gov
Rose	Bonnie	1	Insurance Policy and Information Division, Office Of Personnel Management Phone: (202) 606-1919 Email: brrose@opm.gov
Rovin	Lisa	0	Office of the Assistant Secretary for Planning and Evaluation Address: Humphrey Building, Room 431E Phone: (202) 690-7800 Email: lrovin@osaspe.dhhs.gov
Rumore	Joy	2	U.S. Navy Medical Information Management Center 8901 Wisconsin Ave, Bldg 27 Bethesda, MD 20889-5605 Email: Jrumore@us.med.navy.mil Email: Joy.Rumore@tma.osd.mil
Sanches	Linda	1	Office of the Assistant Secretary for Planning and Evaluation Address: Humphrey Building, Room 442-E Phone: (202) 690-7233 Email: lsanches@osaspe.dhhs.gov
Scanlon	Jim	1	Office of the Assistant Secretary for Planning and Evaluation Address: Humphrey Building, Room 440D Phone: (202) 690-7100 Email: jscanlon@osaspe.dhhs.gov
Sheehan	Sharon	1	Regulatory Counsel FDA Address: TW Bldg., Rm. 517 Phone: (301) 827-0412 Email: ssheehan@ora.fda.gov

Slade	Shelly	3	USDOJ, Civil Divison Room 9030 Patrick Henry Building 601 D Street N.W. Washington, D.C. 20004 Phone: (202) 307 0264 Voice Fax: (202) 616 3085 Fax Email: Shelley.Slade@usdoj.gov
Somers	Debbie	1	Office of the Commissioner Disability Redesign Social Security Adminstration Phone: (410) 966-8365 Email: Debbie.Somers@ssa.gov
Stewart	Frances		Program Director, Patient Advocacy/ Medical Ethics Office of the Assistant Secretary of Defense (Health Affairs) Phone: (703) 681-1703 ext. 5214 Fax: (703) 681-3658
Stockdale	Tim	1, 2	U.S. Marshals Service – Medical Records Bldg CS-3, Suite 200 600 Army-Navy Drive Arlington, VA 22202 Phone: (703) 416-8392 Fax: (703) 603-9156 Email: Tim.Stockdale@usdoj.gov
Stone	Walter	1, 2	Office of Information Services HCFA Address: NORTH Bldg., N2-20-16 Phone: (410) 786-5357, Email: wstone@hcfa.gov
Sullivan	Jeanne	1	Federal Trade Commission jsullivan@ftc.gov (202) 326-3160
Townsend	Jessica	2	Office of Planning, Evaluation, and Legislation HRSA Address: Room 14-36, Parklawn Phone: (301) 443-0371 Email: jtownsend@hrsa.dhhs.gov

Tress	Deborah	3	Office of General Counsel - CDC Address: 1600 Clifton Road, NE MS D-53 Atlanta, GA 30333 Phone: (404) 639-7206. Email: dew3@CDC.GOV
Turner	Amy	1, 2, 3, 4	Department of Labor, Health Care Task Force Room N5677 Phone: (202) 219-7222 x2715 Email: Turnera@pwba.dol.gov
Waldman	Priscilla	2	Center for Health Plans and Providers HCFA Address: NORTH Bldg., Rm. N2-19-18 Phone: (410) 786-1936. Email: pwaldman@hcfa.gov
Werner	John	2	Privacy Act Officer Department of Veterans Affairs VA Community Healthcare System Phone: (203) 932-5711 ext 3701 Email: werner.john_e@west-haven.va.gov Email: John.Werner@med.va.gov
Wetterhall	Scott	3	Office of Program Planning and Evaluation CDC 1600 Clifton Road, NE, MS D-24 Atlanta, GA 30333 Phone: (404) 639-7604 Email: SFW1@cdc.gov
Wilder	Marcy	1, 4	Deputy General Counsel Office of the Secretary Address: Humphrey Building Rm. 707F Phone: (202) 690.6318 Email: mwilder@os.dhhs.gov
Zarate	Al		NCHS/CDC Address: Room 1179, Presidential Building Phone: (301) 436-3238 Email azo1@cdc.gov

53589

DRAFT

FINANCIAL PRIVACY

DRAFT

Statement of the Honorable Gary Gensler

Under Secretary of the Treasury for Domestic Finance

before the

Subcommittee on Financial Institutions and Consumer Credit

Committee on Banking and Financial Services

United States House of Representatives

July 21, 1999

Madam Chairwoman, ranking Member Vento, and members of the Committee, I am pleased to have this opportunity to present the Administration's views on the protection of personal financial information. I know that this issue has been one of great importance to members of this Committee.

Privacy has been a cherished right to Americans since the founding of our nation. Originally, the idea was predominantly one of privacy from governmental interference: privacy in one's home and one's person. The citizenry's fear of governmental intrusions on privacy was rooted partly in American history -- our rejection of tyranny -- but also in practicality. Businesses had neither the means nor the incentive to invade one's privacy.

But over time, the notion of privacy has evolved. The right is no less cherished, but the threats to it are new. When, a century ago, Louis Brandeis

famously enunciated privacy as a "right to be let alone," he was referring to privacy from the press.

Today many Americans increasingly feel their privacy threatened by those with whom they do business. In particular, financial institutions are able to consolidate information about spending and investing habits. Americans want the ability to earn and spend their money without having to expose their lives to those who process their transactions. Americans deserve that right.

For much of our history consumers were justifiably confident about their financial privacy. Most of their day to day transactions were conducted in cash. They obtained financial services from local firms. Records were kept on paper ledgers rather than in computers. A small town banker, a local securities broker or an insurance agent knew the customer's financial circumstances and tolerance for risk, to best offer a loan or advice. Yet customers were confident that the banker, broker or insurance agent would not share that information. Doing so would have been considered a breach of personal trust. That confidence is understandably lacking today.

The first cracks in that confidence began to appear in the late 1960s, as unprecedented amounts of credit information were collected in new, national databases. Congressional hearings revealed that too many credit files contained inaccurate and damaging information, and that consumers often had no way to correct errors that could lead to a denial of credit.

The resulting Fair Credit Reporting Act of 1970 was the first federal law directed at financial privacy. The Act required customer consent before credit report information could be distributed, granted individuals access to their credit histories and the ability to correct errors. And it recognized that customer should have notice and the ability to opt out of certain information transfers -- be it with third parties or among affiliates. [Under the Fair Credit Reporting Act, however, there are no limits on sharing information about consumers' transactions with a firm, unless such information is aggregated at a credit bureau. Thus, financial institutions currently are able to treat what a person buys with checks and credit cards as information belonging to the institution, and are free to sell it.] *move?*

Much has changed since the Fair Credit Reporting Act was passed in response to the mainframe computers of the 1960s. We are in the midst of three important and significant transitions: a technological revolution, industry consolidation, and a move away from cash towards electronic transactions.

Today, an ordinary desktop computer is significantly more powerful than the mainframe of 30 years ago. Vast amounts of information can be stored, sorted, manipulated, and analyzed at lower and lower costs. Advances in telecommunications allows for this information to be sent virtually anywhere on the globe in a fraction of a second. Financial services firms are spending billions per year to further enhance their technologies.

A second key change is the growing integration and consolidation of financial services providers. Interstate banking and branching has allowed banks to

grow larger than ever before, and the removal of regulatory restraints have allowed banking organizations to offer insurance and securities products. Even those smaller banks that have avoided consolidation often broaden their services by contracting with other financial services providers. At the same time, insurance companies are offering deposit products, and investment banks are in the lending business in a major way.

This consolidation has brought benefits to consumers, in the form of operating efficiencies, new products, and better prices for customers. But the desire of large, integrated financial services firms to profit from their scale and cross-sell their products has created a powerful incentive to mine consumer data for a competitive advantage -- potentially appropriating personal information as a business asset. Consolidation and technology have also allowed the relationship between financial institutions and their customers to become increasingly impersonal. Fewer customers walk into branches to deal with a personal banker, as more customers drive up to ATMs or log onto the Internet.

Third, there is an increasing use of electronic means of payments and receipts. Americans increasing use of credit cards, debit cards and (more recently) electronic bill payment in lieu of cash now allows financial services companies to collect a far greater amount of information. Direct deposit now means that a bank knows not only what you spend but how much you earn, and from whom.

A generation ago, financial privacy meant keeping secret your salary, your mortgage and loan balances and your net worth. Today, financial privacy means

keeping secret your entire way of life. The typical credit report in 1970 would have shown only that a customer had received a total of, say, $5,000 of credit, and had repaid it on time. The credit card records of 1999, by contrast, can list each and every purchase ever made by that customer, sorted by date, location, and other details. Furthermore, if credit card companies work together with merchants, then the level of detail can become even more refined -- each dish ordered at a restaurant or each book title bought at a store.

Taken together, these three trends -- technology, industry consolidation, and the movement from a cash to electronic payment and receipt system -- are the means, motive, and opportunity for financial services firms to mine consumer information for profit. Our challenge, therefore, is to protect the privacy of consumers while preserving the benefits of competition and innovation.

On May 4, the President outlined the Administration's "Financial Privacy and Consumer Protection in the 21st Century" initiative. Protecting financial privacy led the list of key principles for consumer protection.

- First, the President recommended enactment of legislation to provide consumers notice and choice before their financial information is shared or sold -- the right to say "no."

  Central to this policy is the idea that the self-portrait painted by one's financial information belongs to the consumer, not the financial institution that processes the transactions.

- [Second, the President stated that consumers should not have to worry that the results of their latest physical exam will be used to deny them a home mortgage or credit card. As banks and insurance companies merge, lenders potentially can gain access to the private medical information contained in insurance forms. The President therefore recommended legislation that would impose special restrictions on sharing medical information within financial conglomerates and with third parties, consistent with the Administration's overall plan for protecting medical privacy.]

- Third, the President called for giving regulators broader authority to monitor compliance with privacy protections. Under the Fair Credit Reporting Act, for example, banking regulators generally may not examine banks for compliance with this statute, as they do for other consumer protection statutes. Surely there is no compelling reason for treating privacy less seriously than other statutory consumer protections.

When the President announced this agenda in May, some may have viewed his proposals as ambitious. Only two months later, however, the policy of notice and choice is gaining momentum. Presidential leadership, and the leadership of members of this Committee and the House, has sparked a debate on this issue that has educated policy makers and produced dramatic results. Most recently, the House of Representatives with overwhelming bipartisan support provided notice and choice before information can be shared with third parties. The House provided the enforcement mechanisms sought by the President. It also recognized the need to protect medical privacy, and generally prohibited the use of so-called

"pretext calling" -- although in these two areas, significant revisions are needed.

Acceptance of the idea of notice and choice is an important step in protecting financial privacy. For adequate privacy protections, however, consumer choice over third party sharing must be the floor, not the ceiling. We must move forward to consider how consumers can exercise choice over sharing within financial conglomerates -- especially conglomerates which, under H.R. 10 and S. 900, would be able to engage not just in financial activities, but also activities "incidental" and "complementary" to such financial activities. And we must consider how to make any privacy protection regime workable. With that in mind, I will address five basic issues that we believe the Congress ought to consider as it moves forward with financial privacy legislation: what information such legislation should cover; what notice is appropriate; what choice is appropriate; what exceptions may be appropriate from notice and choice; and how any privacy regime is to be administered.

Madam Chairwoman, you also requested that I discuss various privacy issues relating to the privacy practices of state governments and the federal government, and of the Treasury Department itself. I am attaching as an appendix a discussion of those issues not discussed in my testimony.

Scope

The first issue is what financial information should be protected. For reasons stated earlier, the limited protections of the Fair Credit Reporting Act are no longer

satisfactory. Transaction and experience data must be protected. [Personal or customer data protection must be enhanced as well.] Information held by any company engaging in financial activities, broadly defined should be protected. H.R. 10 adopts this sound approach. If a credit card company wishes to sell a customer's data, for example, the customer should have the same rights regardless of whether the card is issued by their insured depository institution or comes from a commercial enterprise like a department store or a phone company.

We must consider, though, a future where financial information may be consolidated -- and potentially mined -- at non-financial firms. Many of us already provide a list of our assets to Internet web sites, where daily performance can be monitored. Consumers might be surprised to learn that a list of stocks held at an Internet brokerage site is considered confidential, but a list of stocks at a portal may be freely sold without notice or consent.

Eventually, Congress may want to look beyond financial privacy. Like financial institutions, booksellers and other retailers can build considerable databases and, under current law, sell them without customer knowledge or consent. Your on-line bookseller may not only knows what books you read, but what books you considered buying, where you vacation, what music you listen to. The Administration continues to support efforts at self-regulation. Industry efforts over the past year have been impressive, but they still have a long way to go. We will want to continue scrutiny of these non-financial areas.

Notice

Notice is fundamental to privacy protection. The Administration believes that every financial institution should establish and disclose a privacy policy that encompasses information sharing with both affiliates and third parties. Disclosure of an institution's information practices is a precondition to consumers choosing how their information will be used, or choosing to do business elsewhere.

The Administration believes that a clear and conspicuous notice should be provided before a customer opens an account and at least annually thereafter. The contents of the notice must be sufficient to inform the customer of the uses that will be made of their information and to whom it will be transferred.

That said, the exact contents of a notice may be best left to a rulemaking process where public comment can be solicited, as provided for in H.R. 10.

Choice

The next issue is that of choice. Under what circumstances should a customer be able to restrict the uses a company makes of their data. The Administration believes that consumers should have the choice to opt out, that is prohibit, the use of their data by both third parties and affiliates. The practicality of notice and choice has been proven through the implementation of the Fair Credit Reporting Act. The FCRA has given consumers the right to notice and the opportunity to opt out before a company shares the consumer's credit information

with either an affiliate or a third party. We are simply recommending expanding the scope of the information covered. Financial firms have the ability to make this change. U.S. Bankcorp, in response to a suit brought by the Minnesota Attorney General, has agreed to notice and opt out before transaction and experience data can be shared with affiliates for direct marketing purposes and with unaffiliated third parties for purposes of marketing financial products or services of the unaffiliated third party. [ck]

Nonetheless, some have contended that customers need not have choice over information sharing because they possess the ultimate choice: the ability to take their business elsewhere.

We believe that the idea that customers will be able to "vote with their feet" on financial privacy is generally unrealistic. Changing one's bank or broker is not a simple matter. It requires a considerable investment of effort and time, as one checking account must be run off as another is created, as direct deposit orders must be reissued, as checks must be reprinted, as new codes must be memorized, as stocks must be transferred. It is a change that most of us make only when we are extremely dissatisfied with our current circumstances.

For that reason, the Administration believes that choice must be guaranteed by law. In general, we support the notice of "opt out" choice -- that the sharing may occur so long as the customer is given notice and the opportunity to object. In some cases, with particularly sensitive information, an "opt in" may be appropriate. We also believe that these choices should not be circumvented, as H.R. 10 would

allow them to be circumvented, by allowing the financial institution or an affiliate do the marketing itself, on behalf of the third party.

[Need to make case for affiliate opt-out]

Exceptions

While the Administration is firmly for choice, there is also a need for balance. There are some types of information sharing where customer choice may not be appropriate -- where allowing customers to opt out of information sharing is counterproductive or too costly. The most obvious case is sharing of information with appropriate law enforcement authorities. Another example is the sharing of information in order to facilitate the processing of individual transactions.

Other types of information sharing are more difficult. In approaching any exceptions and the general policy of choice, we think three questions are appropriate.

- First, what is the consumer's reasonable expectation of privacy? This in turn largely depends on the type and sensitivity of the information. Most people expect that their finances will be processed efficiently -- even if by third parties -- but not that anyone processing the data will be able to learn how they live their lives. They also don't expect that information to be sold without their consent.

- Second, what is the purpose of the transfer? Does it directly benefit the consumer or mostly just the company? Is the company using the information to directly serve the customer, or is the company primarily using or sharing the customer's information for another purpose?

- Third, what are the costs of allowing choice? Does it significantly(I) disrupt the functioning of the enterprise, (ii) raise costs to consumers or (iii) disrupt markets?

Any decision should be based on a balance of these factors. The Administration strongly believes that in most cases the balance counsels for choice, whether the sharing be with a third party or an affiliate.

Perhaps the clearest case for choice is in the area of medical privacy. Although a company may have economic incentives to share medical information, no consumer expects that in consenting to a physical examination for an insurance policy, they are endangering their ability to obtain credit or employment. For that reason, the Administration favors strong restrictions on the ability of any company, including insurance companies, to transfer medical information. We strongly opposed, however, the medical privacy provisions of H.R. 10. While appearing to provide greater protections than under current law, those provisions would in fact create uncertainty about the Department of Health and Human Services authority to establish stronger protections for customers of financial services companies, and diminish the chances for comprehensive legislation. H.R. 10 contains significant

exceptions that would, for example, allow re-use of medical information by companies with whom the information is shared, preempt state law, allow consent to sharing to be coerced, and allow significantly more sharing under the label of "research" than current practice allows or future regulations would likely permit.

The sale of marketing information to a third party -- or using such information on behalf of a third party -- also appears to be a clear case where no exception is appropriate. A consumer doing business with a financial institution would not expect the information generated through that relationship be sold for unrelated, especially non-financial, purposes. In such a case, the financial institution would be selling the information primarily for its own profit, not the customers.

In some cases, though, the case for an exception maybe stronger. Financial services firms may wish to provide customers a consolidated account statement including accounts from different affiliates within the organization. Here, the case for an exception from "opt out" appears appropriate. Customers could reasonably expect to have their financial information presented to them in a comprehensive way; the consolidated statement is done for the convenience of the customer, and the customer is able to correct any errors; and the cost of requiring separate mailings for each account could be considerable.

Other cases present more difficult tradeoffs. For example, with respect to risk management, one could conclude that a customer who has defaulted on one loan from a financial organization should not reasonably expect to be able to shield

that information from an affiliate considering a second loan. Allowing the information to be shared protects the depository institution from loss, and should result in lower prices for creditworthy borrowers. The same also could be said of information on the timeliness of a customer's payments to the institution (assuming that the customer receives notice that such information sharing is occurring and has access to and the ability to correct such information).

The idea that a sister bank could, however, deny a loan because a consumer's credit card reveals risk-taking *behavior* -- say, the recent purchase of a skate board or a sports car -- is far more troublesome. Thus, any information about where a consumer is spending money, or the purposes for which the consumer is obtaining credit, should remain subject to notice and opt out. How we live our lives, what we believe, the choices we make -- all of these very personal pieces of information should not be shared without our consent.

[Do we need anything on exceptions in H.R. 10?]

The Need for Regulatory Flexibility

Each of the issues we have just discussed is complicated, and the answers may well change as technology and business practices advance. The complexity and uncertainty of the task at hand suggest two further points.

First, we should allow many of the details to be worked out by the regulators that know the financial services industry best, after taking into account public

comment. The agencies that examine financial services firms and follow industry trends should be responsible for writing and enforcing privacy rules.

Second, a transition period may be appropriate so that financial institutions can reprogram their systems to take account of customer choices. Any such transition should extend beyond the end of this year, as programming resources are currently focused on the Y2K problem.

Conclusion

Thank you for allowing me to appear today on an issue of such importance to the Administration. I welcome your questions.

GREG GANSKE
4TH DISTRICT, IOWA

COMMERCE COMMITTEE
SUBCOMMITTEES:
HEALTH AND ENVIRONMENT
FINANCE AND HAZARDOUS MATERIALS
OVERSIGHT AND INVESTIGATIONS

CONGRESS OF THE UNITED STATES

HOUSE OF REPRESENTATIVES

July 12, 1999

Dear Colleague:

The medical privacy provision in H.R. 10 restricts disclosures of customer health and medical information by insurers.

Some concerns have been raised about the exceptions to the opt-in policy. I would like to take this opportunity to define some of the terms found in the exceptions and dispel the misinformation that is being circulated regarding these provisions.

Under current law, an insurance company obtains medical record information only with an individual's authorization. The medical privacy provision in H.R. 10 relates to how an insurance company shares the data after it has acquired it. The provision states that insurers can only disclose this information with an individual's consent except for limited, legitimate business purposes. These provisions would apply to all insurers who are currently engaged in the insurance business, and who have millions of contracts in force right now. Without these exceptions, these insurers would no longer be able to serve their customers.

The exceptions include ordinary functions that insurance companies are already doing in their day-to-day business. Such operations include:

Underwriting: Insurers use health information to underwrite. The price someone pays for insurance is based in part on an individual's state of health. Insurers gather medical information about applicants during the application and underwriting process. Underwriting is fundamental to the business of insurance. During the underwriting process, an insurer may use third parties, such as labs and health care providers to gather health information and/or to analyze health information. The insurer may also use third parties to perform all or part of the underwriting process and must disclose information to these third parties, such as doctors or third party administrators, so that they can enter into the contract in the first place.

Reinsuring Policies: Insurance companies sometimes assume a "risk" and then further spread the risk by "reinsuring" a policy. While often a "reinsurance" arrangement is made at the initiation of a contract, there are also times when reinsurance occurs after the policy is issued. The reinsurer needs access to the first insurer's underwriting practices

1108 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4426

FEDERAL BUILDING
210 WALNUT STREET
DES MOINES, IA 50309
(515) 284-4634

40 PEARL STREET
COUNCIL BLUFFS, IA 51503
(712) 323-5976

PRINTED ON RECYCLED PAPER

as part of its due diligence. Without this language, the wheels of the reinsurance industry could literally grind to a halt.

Account Administration, Processing Premium Payments, and Processing Insurance Claims: In order to pay a claim for benefits, the insurer has to process the claim. This is a basic business function. These activities are the very reasons an individual signs up for a policy in the first place. Companies may use third party billing agencies and administrators to process this information. A company that doesn't today, may tomorrow; and we need to ensure that they can, so that consumers can be served.

Reporting, Investigating or Preventing Fraud or Material Misrepresentation: There are certainly times when individuals may not want to disclose all of their health information for valid reasons. However, there are those that may try to hide health information relevant to whether a policy would be issued or what would be charged for that policy. For example, nonsmokers usually pay less for insurance than smokers. On the other hand, if you have a chronic illness your premium may be higher. If an individual is engaged in fraud of material misrepresentation, it is highly unlikely that they would give their consent so that the insurer could disclose this information, for example, to its law firm to undertake an investigation of the matter or to the insurance commissioner or other appropriate authorities.

Risk Control: Credit card companies and other financial institutions involved in billing, conduct internal audits to ensure the integrity of the billing system. During this process, the company verifies that merchants, credit card holders and transactions are legitimate. These audits are done on random samples in which transactions dealing with medical services are not segregated or treated differently from other types of transactions. However, if this exception were not included, the company would be prevented from verifying the validity of transactions dealing with medical services. This would open the door for much fraud and abuse or the inability for consumers to write checks or use credit cards to pay for medical co-payments.

Research: Insurers do research for many purposes. For example, life insurers will do research related to health status and mortality to help them more accurately underwrite and classify risk. This provision is needed so that insurers can continue to do research.

Information to the Customer's Physician: This exception is necessary to allow insurers to release information to an individual's physician. For example, during the underwriting process, an insurer may conduct blood test on an applicant. If the blood tests indicate that there may be something wrong, the insurer needs to be able to share the information with the individual's designated physician or health care provider so that they, together, can determine the best course of treatment.

Enabling the Purchase, Transfer, Merger or Sale of Any Insurance Related Business: No one has a crystal ball. A company does not know in advance when they will engage in these activities. It would be impractical if not impossible to obtain the tens of thousands of authorization forms signed and returned to the company so that a

company could purchase, transfer, merge or sell an insurance related business. Without this language, companies will not be able to serve their customers by forging new business frontiers. Since the privacy provision covers all insurance companies, the purchasing company will have to abide by the same restrictions as the original company.

Or as Otherwise Required or Specifically Permitted by Federal or State Law: There are some states that require or specifically permit the disclosure of medical information by insurance companies. For example, a company may have to disclose health information to a state insurance commissioner so that the commissioner can determine if the company is complying with state law banning unfair trade practices. A company may have information that would help the police in an investigation where they suspect an individual has murdered someone in order to collect life insurance benefits. This language is necessary for these and other important public interests.

I hope that this brief explanation of the exceptions to the strong "opt-in" provisions of the medical privacy provisions of H.R. 10 clears up some misperceptions. During floor debate, I said I would work to include explicit language stating that this provision does not prohibit the secretary of HHS from issuing regulations on medical privacy as specified by HIPAA.

Furthermore, I hope consensus can be achieved on a comprehensive medical privacy bill. However, I remain convinced that as new financial services entities that combine banking, securities and insurance are created by H.R. 10, it is important that personal health data can be shared inside, or outside, the company **only** with the patient's permission. That is what the Ganske Amendment did.

If you need additional information, please contact Heather Eilers at 5-4426.

Sincerely,

Greg Ganske

Greg Ganske
Member of Congress