Withdrawal/Redaction Sheet
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. letter	Chai to Chris re: phone number (partial) (1 page)	09/24/1999	P6/b(6)

COLLECTION:
Clinton Presidential Records
Domestic Policy Council
Devorah Adler
OA/Box Number: 20470

FOLDER TITLE:
Privacy [Folder 8]

2012-0463-S
rc821

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

GEORGETOWN UNIVERSITY LAW CENTER

Federal Legislation Clinic

Federal Legislation Clinic
111 F Street, N.W.
Washington, DC 20001
Phone (202) 662-9595
Fax (202) 662-9682

FAX COVER MEMORANDUM

DATE: 9/24/99

NUMBER OF PAGES, INCLUDING THIS SHEET: 4

TO: CHRIS JENNINGS

FAX NUMBER: 456-5557

FROM: CHAI FELDBLUM

COMMENT:

o:\wpdocs\fnxcover

111 F Street NW Room 340 Washington, DC 20001-2095
tel: (202) 662-9595 facsimile: (202) 662-9682
e-mail: feldblcr@law.georgetown.edu
www.law.georgetown.edu/clinics/flc

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. letter	Chai to Chris re: phone number (partial) (1 page)	09/24/1999	P6/b(6)

COLLECTION:
Clinton Presidential Records
Domestic Policy Council
Devorah Adler
OA/Box Number: 20470

FOLDER TITLE:
Privacy [Folder 8]

2012-0463-S
rc821

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

9/24/99

Chris--

Here's the language on minors that we sent to Paul Harrington at the end of last week to share with the "other parties" to the issue (as Paul calls them). The best, of course, would have been for Paul to present this approach as his own. Having not done that, my hope is that he will at least tell them this is something Jeffords would like to see, and force them to articulate a real policy problem with it. They are supposed to get back to Paul by the end of this week. Joanne Hustead (from National Partnership) and I stopped in at Paul's yesterday, and I strongly encouraged him to simply announce this as Jefford's compromise if the "other parties" didn't agree to it. We'll see . . .

As we discussed, however, for this compromise language to have any real traction, there needs to be something on the radar screen that more accurately reflects what we believe is the optimal privacy provision--so it becomes clear that this language is, indeed, a *compromise* position on our part. We think that the optimal policy position was well articulated in the Secretary's 1997 recommendations on minors--and we would suggest that the proposed HHS regulations hew as closely as possible to those 1997 recommendations. At a minimum, those regulations need to clearly retain the Secretary's 1997 approach that if a minor lawfully receives treatment on his/her own, the minor controls the records to that treatment.

As you suggested, I do think it makes sense to have an overall strategy conversation on this. I think Jeff Crowley (my client on this issue) was going to send you an official letter (although I'm not quite sure that's necessary, but anyway . . .) You can also always reach me on my cell phone at P6/(b)(6) Thanks for everything!

Cheers, (001)

Chai

PROPOSED COMPROMISE PROVISION ON MINORS' MEDICAL PRIVACY

Delete the current Rights of Minors' subsection from the Next of Kin provision and add the following subsection (d) to the Individual Representatives' section (new language is indicated by *italics*):

SEC. 213 INDIVIDUAL REPRESENTATIVES.

(a) IN GENERAL.-- Except as provided in subsections (b) and (c), a person who is designated by the individual, authorized by law (based on grounds other than the individual being a minor), or by an instrument recognized under law, to act as agent, attorney, proxy, or other representative of a protected individual, may, to the extent so authorized, exercise and discharge the rights of the individual under this Act.

* * *

(d) Protected Health Information About Minors.--

(1) IN GENERAL.-- A parent, guardian, or other person acting in loco parentis shall exercise the rights of an individual under this Act on behalf of a minor--

(a) when the parent, guardian, or other person acting in loco parentis has consented, as provided under applicable State or Federal law, to the provision of the health care that is the subject of the protected health information; or

(b) when emergency health care is rendered to a minor, and prior consent for such health care has not been given by a parent, guardian, or other person acting in loco parentis, but there would have been no legal alternative to the consent of such individual in a non-emergency circumstance.

(2) EXCEPTION.-- In any case not described in (1), the minor shall exercise the rights of an individual under this Act, except that a minor may not use any provision of this Act to prohibit a professional who has provided health care to that minor from disclosing protected health information relating to such care to a parent, guardian, or other person acting in loco parentis, if such professional, in the exercise of sound professional judgment, determines that disclosure to such individual is necessary.

(3) PROTECTED HEALTH INFORMATION REGARDING TREATMENT RECEIVED AS A MINOR.-- Once a minor has attained the age of majority, as determined by applicable State law, the minor shall exercise the rights of an individual under this Act with respect to protected health information concerning health care services rendered while the person was a minor.

(4) CONCURRENT RIGHTS.-- In any case described in (1), a minor may exercise the rights of an individual under this Act concurrently with a parent, guardian, or person acting in loco parentis if such individual authorizes the minor to exercise such rights. The Secretary shall promulgate an appropriate authorization form for such purposes.

Add to Definitions' section:

"Minor" shall be defined in accordance with applicable State law.

Amend the Relationship to Other Laws provision (a.k.a., preemption) to read as follows:

(d) Minors. This Act shall not preempt, modify, repeal, supersede or affect Federal or State law pertaining to minors.

Rationale For Proposed Compromise Provision:

- The proposed language clarifies prior unclear language which left open several issues regarding the rights of parents and minors to use the federal law to access or control access to a minor's protected health information.

- This provision establishes two clear default positions for access to a minor's protected health information: 1) the parents and 2) the health care professional who treats the minor.

- As a general rule, parents will exercise the rights of minors in any case in which the parent has consented to health care services rendered to the minor. This will be the situation in the bulk of cases in which minors receive health care. This establishes a clear default rule that **parents** exercise any new federal rights under this law on behalf of their children. The age at which a child is considered to be a minor will be set by applicable state law.

- In certain emergency circumstances, treatment may legally be rendered to a minor without the consent of the parent. In such cases, if the parent has not consented to the treatment on behalf of the minor, but there would have been no legal alternative to the consent of the parent in a non-emergency circumstance, the parent will exercise the rights of the minor with respect to the protected health information relating to that treatment.

- The second default rule is that, in limited circumstances, the treating professional will control access by parents to a minor's health information. Even when a minor lawfully receives treatment without the consent of a parent, the minor may not use the new federal law to prevent a health care professional from disclosing information about the treatment to a parent, if the professional believes, in the exercise of sound professional judgment, that such disclosure is necessary. Only when the professional believes that disclosure to a parent is not necessary will the minor be able to exercise rights under the new federal law to prevent disclosure to parents.

- Nothing in this section changes any existing rights or responsibilities governing parents, minors or health care professionals. Parents who may now access a minor's protected health information will continue to be able to access such information. Minors who may now restrict access to protected health information will continue to be able to restrict such access. And if a health care professional may now disclose information to a parent when the professional determines that disclosure is necessary, such professional would continue to have that ability under the new federal law.

- An adult who wishes to obtain protected health information pertaining to health care received as a minor will have access to records of such treatment. Once we establish a default to parents, we need to be clear that minors who attain the age of majority can exercise the rights of an individual with respect to protected health information relating to health care received as a minor.

- Although the provision defaults to parents, those parents who want to allow their minor children to exercise rights concurrently should be permitted to do so. This permits parents to involve their children in the health care process, to the extent the parents desire.

DATE: 9-24-99

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
ROOM 416G, HUMPHREY BUILDING
200 INDEPENDENCE AVENUE, SW
WASHINGTON, D.C. 20201

PHONE: (202) 690-7627 *FAX: (202) 690-7380*

OFFICE OF THE ASSISTANT SECRETARY FOR LEGISLATION
ROOM 416-G HUMPHREY BUILDING

TO: Chris J. 456-5557 / Dan M. 395-5631

OFFICE: _____

ROOM: _____

PHONE: _____

FAX: _____

TOTAL PAGES (INCLUDING COVER): 3

[X] RICHARD J. TARPLIN
[ ] KEVIN BURKE
[ ] HAZEL FARMER
[ ] ROSE CLEMENT LUSI
[ ] ALICE ARTIS
[ ] FRANKIE MELTON

REMARKS:

DATE: 9-20-99

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
ROOM 405H, HUMPHREY BUILDING
200 INDEPENDENCE AVE, SW
WASHINGTON, D.C. 20201

PHONE: (202)690-7450 *FAX: (202)690-8425*

TO: Chris Jennings

OFFICE: _____

ROOM: _____

PHONE: 456-5594

FAX: 456-5557

FROM:

[X] JANE HORVATH

[ ] SHARON CLARKIN

[ ] BOB GUIDOS

[ ] JOANNE JEE

[ ] GREG JONES

[ ] ANDREA LEVARIO

[ ] ROGER MCCLUNG

[ ] JACK MITCHELL

[ ] TANISHA PARKER

[ ] PAUL SELTMAN

[ ] STEPHANIE WILSON

[ ]

(INCLUDING COVER): 7

REMARKS:

STATE ATTORNEYS GENERAL

A Communication From the Chief Legal Officers Of the Following States

California•Connecticut•Hawaii•Idaho•Indiana•Iowa•Maine•Maryland Massachusetts•Minnesota•Mississippi•Missouri•New Hampshire•New York North Dakota•Northern Mariana Islands -Pennsylvania•Puerto Rico Rhode Island•Tennessee•Vermont•West Virginia•Wyoming

September 13, 1999

Re: Opposition to H.R. 10, the Financial Services Act of 1999

Dear Conferee:

The undersigned Attorneys General are writing to you regarding the Financial Services Act of 1999. As the states' chief legal officers, we have been asked to do a technical analysis of the Act's impact on our states' consumers. Based on our analysis, we strongly oppose provisions that will not provide adequate protection for private financial and medical records. This situation is not only bad for consumers, it fails to achieve the Act's goal of a "level playing field" between insurance companies that are affiliated with banks and those that are not.

In particular, we are concerned that the privacy provisions of the Act specifically allow practices that will further erode the rights of consumers to exercise some degree of control over their financial and medical records. H.R. 10 permits widespread use and disclosure of sensitive information without the individual's knowledge or consent, while providing only limited remedies for violations and no effective limitations on re-disclosure. The legislation provides that a financial institution need not give its customers a right to opt out of disclosure if a non-affiliated third party using the information is selling the financial institution's "own products or services."

We ask for your assistance in ensuring that Attorneys General can continue to help consumers. The attached position paper sets forth suggested changes to the language of H.R. 10 that would help achieve the goals of a more competitive financial market without sacrificing consumer welfare.

Thank you for your consideration of our views.

Very truly yours,

Bill Lockyer
Attorney General of California

Richard Blumenthal
Attorney General of Connecticut

Earl Anzai
Attorney General Designate of Hawaii

Alan G. Lance
Attorney General of Idaho

Jeffrey A. Modisett
Attorney General of Indiana

Tom Miller
Attorney General of Iowa

Andrew Ketterer
Attorney General of Maine

J. Joseph Curran, Jr.
Attorney General of Maryland

Tom Reilly
Attorney General of Massachusetts

Mike Hatch
Attorney General of Minnesota

Mike Moore
Attorney General of Mississippi

Jeremiah W. Nixon
Attorney General of Missouri

Philip T. McLaughlin
Attorney General of New Hampshire

Eliot Spitzer
Attorney General of New York

Heidi Heitkamp
Attorney General of North Dakota

Maya B. Kara
Attorney General of N. Mariana Isl.

mike Fisher

D. Michael Fisher
Attorney General of Pennsylvania

José A. Fuentes-Agostini
Attorney General of Puerto Rico

Sheldon Whitehouse
Attorney General of Rhode Island

Paul Summers
Attorney General of Tennessee

William H. Sorrell
Attorney General of Vermont

Darrell V. McGraw Jr.
Attorney General of West Virginia

Gay Woodhouse
Attorney General of Wyoming

H.R. 10 Lacks Meaningful Privacy Protections

In its current version, H.R. 10 not only fails to enact much-needed standards and requirements to protect the vast amount of sensitive personal data that is collected and disseminated, but appears to proceed in the wrong direction by specifically allowing practices that will further erode the rights of consumers to exercise some degree of control over their financial and medical records. We are most concerned with the four areas discussed below.

Sharing and Selling of Personal Information

The ability and willingness of financial, insurance and medical organizations to share consumer data and the uses to which such data can be put by means of various behavior modeling and scoring techniques, has grown rapidly, far outpacing what minimal consumer protections exist in this area. We believe most consumers would be very concerned to learn the extent to which their personal data are collected, tracked and used for commercial purposes, often by companies they have never heard of and with whom they have no relationship. Under these circumstances, it is unrealistic to suggest that concerns for consumer privacy can be dealt with by market forces. It seems far more likely, given the pervasiveness of data sharing and use that already exists, that market pressures will force virtually all companies to use consumer data to the full extent allowed by law, leaving consumers who are concerned about privacy without alternatives. In the case of H.R. 10, the affected businesses offer services that are essential to today's consumers who simply do not have the option of declining to purchase insurance, investment and banking services.

We strongly urge that consumers be given notice and a meaningful opportunity to choose whether or not their personal information can be provided either to affiliates or to third parties (other than legitimate law enforcement authorities). Given the sensitive nature of such data, we believe the only means of effectively controlling its use and dissemination is to require that companies obtain consumers' explicit permission prior to using, sharing or selling it for any purpose, other than legitimate law enforcement purposes, not directly connected to providing the services the consumer contracted for. We therefore urge adoption of an "opt-in" requirement with respect to the sharing of information with affiliates or with commercial third parties as the only effective means of providing consumers with a choice and with the degree of control they indicate they want and need with respect to their personal information. Although we believe an opt-in provision will best serve consumers' needs, any legislation should at least require that consumers be given notice and an opportunity to opt out with respect to the sharing of personal information.

The current language of H. R. 10 requires consumers to "opt out" of disclosure in order to avoid having their personal information shared by financial institutions with non-affiliated third parties. Yet even the minimal protection afforded by this "opt out" approach is eroded by an exemption that substantially weakens it. At Section 502(b)(2), the legislation provides that a financial institution need not give its customers a right to opt out of disclosure if a non-affiliated third party that uses the information (i.e. a telemarketer) is selling the financial institution's "own products or services." There is nothing in the

legislation that would prevent a financial institution from diversifying into the sale of non-financial services (such as discount buying clubs) and hiring third-party telemarketers to sell those services. In such cases, the exemption in Section 502(b)(2) would not prevent the unfettered sharing of private financial information with the telemarketers.

There is no reason to distinguish a customer's right to control private information in a situation where a non-affiliated telemarketer is selling a financial institution's services, rather than the telemarketer's own services. In either case, an entity other than the financial institution is obtaining access to the consumer's personal data. To draw a distinction based solely on the identity of the owner of services being sold is arbitrary and does nothing to address the deeper concern: the fact that an independent third party has access to information that the consumer may consider private. Accordingly, if Congress pursues an "opt out" approach to the disclosure of private financial information, we urge that the exemption at Section 502(b)(2) of H.R. 10 be stricken.

Additionally, we urge Congress to adopt privacy protections requiring notice and opt-out provisions which apply to information sharing among affiliated entities. As currently drafted, H.R. 10 at Sections 502 (a) and (b) only provides for the opportunity to receive notice of and opt out of information sharing among non-affiliated entities. Yet consumers do not differentiate between affiliates and nonaffiliates when seeking to protect against the sharing of personal financial information. Congress likewise should not differentiate between the two, and should provide equal privacy protections in both contexts.

Medical Information

No consumer information is more sensitive than medical records, yet there is no comprehensive system for protecting such information or ensuring its accuracy. It would seem more appropriate to deal with such a vital subject in a deliberate manner that focuses on the requirements relevant to this particular type of information, rather than in legislation revising the structure of the financial services industry. We agree with the instructions to the House conferees to recede to the Senate provisions on this issue, thereby allowing Congress to address the issue of medical privacy in a more deliberate manner, as contemplated by the Health Insurance Portability and Accountability Act of 1996.

If provisions regarding medical information privacy are retained in H.R. 10, we strongly urge adoption of requirements that will ensure consumers access to their own medical information and protect such information from disclosure, other than for legitimate law enforcement purposes, without the informed consent of the individual. The language currently in H.R. 10 would move in the opposite direction, permitting widespread use and disclosure of sensitive information without the individual's knowledge or consent, while providing only limited remedies for violations and no apparent limitations on re-disclosure.

Obtaining Information by Pretext

While H.R. 10 generally prohibits obtaining the customer information of a financial institution by false or fictitious statements or documents, there are a number of exceptions to this rule. The most troubling of these exceptions is that made for private investigators in connection with an attempt to collect child support. Although we do not quarrel with the

goal of facilitating collection of delinquent child support payments, we believe this portion of H.R. 10 is unnecessary and is subject to abuse. Given that the caller will be making fictitious statements, and no doubt using a fictitious name, it will be virtually impossible to ensure that those making such calls meet the criteria set forth in Section 521 of the bill. Accordingly, we urge that this section of H.R. 10 be deleted.

As an alternative, we suggest that disclosure of financial information that is reasonably necessary to collect delinquent child support payments be made an affirmative obligation of financial institutions. Specifying precisely who is permitted to receive such data and the criteria that must be met before disclosure can be made, and requiring that financial institutions ensure the criteria are met before making any disclosure, would facilitate collection but greatly reduce the opportunities for abuse.

Relation to State Laws

Consumers in our states are extremely concerned about privacy issues. The rapid development of technology has permitted the creation and manipulation of ever larger and more complex data bases. Revision of the structure of the financial services industry will almost certainly hasten this process. The states have traditionally served as an arena for developing and testing the means of assuring consumer protection in a changing environment. We strongly believe that an issue as fundamental as privacy requires the full efforts of the states as well as the Congress to deal effectively with the challenges presented. We therefore urge that any legislation affecting consumer privacy not preempt existing state laws or limit the ability of state legislatures to respond to the needs of their citizens in the future.

CALIFORNIA CODES
PENAL CODE
SECTION 1543-1545

1543. (a) Records of the identity, diagnosis, prognosis, or treatment of any patient maintained by a health care facility which are not privileged records required to be secured by the special master procedure in Section 1524, or records required by law to be confidential, shall only be disclosed to law enforcement agencies pursuant to this section:

(1) In accordance with the prior written consent of the patient; or

(2) If authorized by an appropriate order of a court of competent jurisdiction in the county where the records are located, granted after application showing good cause therefor. In assessing good cause, the court:

(A) Shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services;

(B) Shall determine that there is a reasonable likelihood that the records in question will disclose material information or evidence of substantial value in connection with the investigation or prosecution; or

(3) By a search warrant obtained pursuant to Section 1524.

(b) The prohibitions of this section continue to apply to records concerning any individual who has been a patient, irrespective of whether or when he ceases to be a patient.

(c) Except where an extraordinary order under Section 1544 is granted or a search warrant is obtained pursuant to Section 1524, any health care facility whose records are sought under this chapter shall be notified of the application and afforded an opportunity to appear and be heard thereon.

(d) Both disclosure and dissemination of any information from the records shall be limited under the terms of the order to assure that no information will be unnecessarily disclosed and that dissemination will be no wider than necessary.

This chapter shall not apply to investigations of fraud in the provision or receipt of Medi-Cal benefits, investigations of insurance fraud performed by the Department of Insurance or the California Highway Patrol and investigations and research regarding occupational health and safety performed by or under agreement with the Department of Industrial Relations. Access to medical records in such investigations shall be governed by all laws in effect at the time access is sought.

(e) Nothing in this chapter shall prohibit disclosure by a medical facility or medical provider of information contained in medical records where disclosure to specific agencies is mandated by statutes or regulations.

(f) This chapter shall not be construed to authorize disclosure of privileged records to law enforcement agencies by the procedure set forth in this chapter, where such privileged records are required to be secured by the special master procedure set forth in subdivision (c) of Section 1524 or required by law to be confidential.

1544. A law enforcement agency applying for disclosure of patient records under Section **1543** may petition the court for an extraordinary order delaying the notice of the application to the health care facility required by subdivision (f) of Section **1543** for a period of 30 days, upon a showing of good cause to believe that

notice would seriously impede the investigation.

1545. For the purposes of this chapter:

(a) "Health care facility" means any clinic, health dispensary, or health facility, licensed pursuant to Division 2 (commencing with Section 1200) of the Health and Safety Code, or any mental hospital, drug abuse clinic, or detoxification center.

(b) "Law enforcement agency" means the Attorney General of the State of California, every district attorney, and every agency of the State of California expressly authorized by statute to investigate or prosecute law violators.

Appointment of Conferees Fin Mod Act

enforcement of privacy rights.

The Senate financial modernization bill--S. 900--contains only minimal privacy provisions regarding pretext calling. This motion instructs the House conferees to insist on the House provisions and the strongest consumer financial privacy protections possible.

Secondly, H.R. 10 contains strong community reinvestment provisions that ensure that publicly insured financial institutions equally and fairly serve all members of their communities in the new financial system that this bill otherwise creates. H.R. 10 ensures that community reinvestment laws remain relevant and viable in a more integrated financial services system. These provisions have enjoyed bipartisan support throughout this process.

Community reinvestment legislation was passed by Congress over twenty years ago to combat discrimination by publicly insured financial institutions and provide equal access for all Americans who qualify for home and small business loans and to community groups seeking loans to revitalize poor neighborhoods.

H.R. 10 maintains the central importance of these laws in our financial services system. S. 900 contains three provisions which substantially weaken community reinvestment laws and render them virtually irrelevant in the changing financial marketplace. President Clinton has made it abundantly clear that he will veto any bill that contains the Senate provisions. In contrast, the Administration can strongly support the bill passed by the House and the community reinvestment provisions it contains. This motion instructs House conferees to insist on the strongest possible community reinvestment provisions, reflected in the House product.

LaFalce

Finally, H.R. 10 contains a provision authored by Congressman Ganske on medical privacy which the Administration, privacy groups, medical groups and many commentators argue contain substantial loopholes. In their current form, these provisions in fact represent less protection than what is available under existing law, and preempt strong privacy provisions available in the states. The Administration strongly opposes the Ganske provision. This motion instructs House conferees to insist that any medical privacy provisions give consumers the strongest medical privacy protections possible, prevent financial institutions from disclosing or making unrelated uses of health, medical and genetic information without consumer consent, and therefore recede to the Senate.

I urge my colleagues to support the motion.

Mr. Speaker, I reserve the balance of my time.

[Page: H6729]

Mr. LEACH. Mr. Speaker, I yield myself such time as I may consume.

First, Mr. Speaker, let me say I intend to yield 15 minutes to the gentleman from Iowa (Mr. Ganske) as a representative of the Committee on Commerce at the appropriate point.

Mr. Speaker, I agree with, in fact, the first two provisions of the motion to instruct and will reluctantly accede to the third, but I am compelled to note that the controversy over the medical privacy provisions that this motion to instruct seeks to strike from the bill presents one of the most ironic circumstances that I have dealt with as a committee chairman.

The same Members who have quite properly insisted on placing privacy protections for consumers of financial services in the bill are now strenuously insisting on deleting from it a provision that would offer consumers powerful new protections in an area where there is perhaps the greatest sensitivity

to privacy, that relating to personal health and medical records.

I continue to believe that the medical privacy provision championed by the gentleman from Iowa (Mr. Ganske) and others has been widely misunderstood both by Members of this body and outside groups that have expressed certain skepticism.

Here let me be clear. The provisions would block the sharing of the individually identifiable customer, health, medical, and genetic information by an insurance company either within an affiliate structure or with outside third parties unless the customer expressly consents to such disclosure with a limited number of exceptions related to medical research or normal and customary underwriting in business functions.

It should be emphasized that the Ganske language does nothing to undermine the more comprehensive medical privacy proposals being developed by other congressional committees or by the Clinton administration. The provision plainly states that it will not take effect or shall be overridden if and when Congress enacts comprehensive medical privacy legislation satisfying the requirements of the Health Insurance Portability and Accountability Act of 1996.

Moreover, as both the gentleman from Iowa (Mr. Ganske) and I made clear as legislative intent in House debate on the subject, the provision in no way undermines the authority of the Secretary of Health and Human Services to promulgate regulations in this area if the Congress fails to meet its statutory mandate by August 21 of this year.

In short, the provision was carefully designed to supplement rather than supplant or supersede other private and public sector legal and institutional barriers to the sharing of private health and medical information.

As I have repeatedly stated, I was prepared to work at conference to further clarify the bill's text. The future HHS rulemaking would not be preempted. I also agreed to seek to remedy any imperfections in language that might realistically be deemed to compromise patient confidentiality. However, in light of the controversy generated by the provision and because I would like to proceed in as bipartisan a fashion as possible in producing a financial modernization bill that the President can sign into law, I am prepared not to fight instruction that the House recede to the Senate position on this issue. But in so doing I would reiterate my belief that opposition to the Ganske approach is based upon an underlying premise that is frail and upon outside advocacy that may be misdirected.

Accordingly, it is my hope that those Members and outside associations that have so vehemently opposed addressing the issue of health and medical privacy in this bill will re-examine their positions. Little, after all, would seem more self-apparently appropriate than to prohibit sharing of medical records within or outside financial services companies without patient consent.

Future Congressional and administrative actions to fashion law and regulation in this complex area will no doubt be modeled in large part on the provision that this instruction is designed to delete. But here the irony should further be underscored that HHS discretion, which the gentleman from Iowa (Mr. Ganske) and I are totally willing to protect, in any event only goes to health insurance. So what is happening here is that the motion to instruct is knocking out legislative protections for all medical privacy without the prospect that privacy protections for life and disability insurance can be addressed through administrative action.

After all the contentions on the minority side that privacy protections should be in the bill, the argument now is that they should not be in the bill. I want bipartisanship and administration support for this legislation so I am willing to accede, but let me stress not without a degree of incredulity.

Mr. Speaker, I reserve the balance of my time.

[Page: H6730]

Mr. MARKEY. Mr. Speaker, I yield myself 3 minutes.

The SPEAKER pro tempore. Does the gentleman seek to claim the time allocated to the gentleman from Michigan (Mr. Dingell)?

Mr. MARKEY. I do, Mr. Speaker.

The SPEAKER pro tempore. Without objection, the gentleman from Massachusetts is recognized.

There was no objection.

Mr. MARKEY. Mr. Speaker, I rise in strong support of the LaFalce motion to instruct the House conferees. With this legislation the Congress will be breaking down the Glass-Steagall walls that long have restricted limited affiliations between banks, securities firms and insurance companies and allow these financial services institutions to merge and to affiliate with one another.

I support this effort. The gentleman from Michigan (Mr. Dingell) supports this effort. This is not really what we are debating here today. The great truth, however, of finance in the information age is that it is the telecommunication wires that have re-shaped the financial services industry. It is the telecommunications revolution which has made possible this global financial revolution. It is this telecommunications revolution which makes it possible for the first time to really bring together all of these various services in a way that can serve individuals and nations much more efficiently than they ever have in the past.

But, as I have said before, there is a Dickensian quality to this wire. It is the best of wires, and it is the worst of wires simultaneously. Yes, it can make the banking and insurance and brokerage industries more efficient, but yes, at the same time it can also compromise the privacy of every single family in the United States.

The LaFalce motion to instruct says that the conferees shall ensure, consistent with the scope of the conference, that consumers have the strongest consumer financial privacy protections possible, including protections against the misuse of confidential information and inappropriate marketing practices. The conferees must also ensure 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. Now I ask my colleagues what is wrong with that? What is wrong with that?

Second, the motion instructs the House conferees to ensure that 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 strike the flawed Ganske language that would weaken protections under current State or federal laws or regulations.

[TIME: 1300]

Finally, the motion by the gentleman from New York, the LaFalce motion, instructs the House conferees to ensure that consumers enjoy the benefits of comprehensive financial modernization.

These are critical issues that need to be properly addressed. There are tremendous opportunities for innovation and for entrepreneurship in finances, banking moves online. But we have a difference that is developing between the privacy keepers, on the one hand, and the information reapers on the

other.

The CEO of Capital One Financial recently noted, credit cards are not banking, they are information. And the data miners fully intend to exploit their access to and control of consumer personal information for fun and for profit.

We believe that is wrong. We believe that the LaFalce instructions are critical to ensuring that, as we move forward with all of the new efficiencies in the financial services world, that we also ensure that we are protecting individuals against those that might seek to take advantage of it.

Mr. Speaker, I reserve the balance of my time.

Mr. GANSKE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I think there has been a lot of miscommunication, misunderstanding about the medical privacy provisions that we passed here in the House. I will just briefly go over those.

Those medical privacy provisions would not preempt State privacy laws, they would not obstruct future State privacy laws, they would not allow insurance companies to sell medical information to drug companies, they would not block the Secretary of HHS from issuing provisions under HIPAA, which interestingly, as the chairman of the Committee on Banking and Financial Services pointed out, is limited to health insurance, whereas the provisions on medical privacy in the bill that we passed here in the House goes for all insurance. So it is more inclusive than what was in HIPAA. And it would say that, unless a customer specifically agreed, an insurer could not give any medical information to its affiliates, much less any third party; and I think that is important.

I think the bill would be better with that provision in there.

Now, there has been a lot of controversy about some of the exceptions in that provision, and I have shared with all of the colleagues in the House, Republican and Democrats, a `Dear Colleague' that goes into some detail on this, which I will insert into the Record at this time.

House of Representatives,
Washington, DC, 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 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

Community Reinvestment Act provide the bedrock, the foundation for such partnerships and we must work to strengthen CRA and other laws that help assure the creditworthy needs of communities are served fairly.

Veto!

Finally, Mr. Speaker, with regard to medical privacy, we seek to have the highest and best protections for consumers that have relationships with financial institutions that could receive and share confidential health and medical information. While I have differences regarding the language in the motion, we all agree that we must seek the strongest provisions that prevent the unrelated use or disclosure of health, medical and genetic information. Further we should not weaken any federal or state protections in law or regulation.

As most are aware, there is currently a much larger process outside of this bill. Many interested parties are working on either a legislative solution or the possibility of regulations from the Department of Health and Human Services to address comprehensively for all health industry businesses and entities, regardless of corporate structure, that will hopefully provide the framework for what is the definitive and proper practice for sharing medical information. To the degree that that process works to cover the affiliated structures, life insurance and property and casualty insurance entities that would affiliate with banks, we do not want to undermine it. Where it is not sufficient, we hope to complement and strengthen it.

This motion should not be out of line with what we have tried to do--in good faith--in the House-passed version of financial services modernization. The statements of so many members allude to their firm belief that we should not and would not supersede the work of HHS in response to the 1996 Health Insurance Portability and Accountability Act of 1996 (HIPAA), passed by this Congress and signed into law. We must assure that the language neither supplants nor has a negative effect on the law or the regulations. Moreover, we must be absolute in assuring that stronger state laws are not preempted. Finally, we must be diligent in assuring that we are prepared for the possibility that the HHS regulations or potential law passed by Congress regarding the health insurance industry will not entirely apply to other insurance entities. In that event, we must with no uncertainly, obtain the strongest possible medical privacy provision so that all Americans are not vulnerable to the misuse of such information in credit or other decisions made by affiliated companies.

I understand that this is a priority of the President, who spoke to this in his State of the Union address to the Nation. We share the goal that we must make true medical privacy a reality for all Americans as soon as is practically possible. Medical privacy should not be breached by financial modernization. The ultimate legislative and regulatory solutions must properly affect the structures we hope to create under financial services modernization so that we are not left with a void that leaves customers vulnerable to inappropriate medical information sharing.

So I rise in support, and I urge Members to give us this vote of confidence.

[Page: H6732]

Mr. LEACH. Mr. Speaker, I yield 2 minutes to the gentlewoman from New Jersey (Mrs. Roukema).

Mrs. ROUKEMA. Mr. Speaker, I find myself in agreement, mostly in agreement with what has been said on different sides of this subject today, and I certainly agree with my chairman and with what the gentleman from Iowa (Mr. Ganske) has stated in terms of conceding to this motion to instruct.

However, I think there are two important things that should be included here, and one is that when we are in conference, we not only have to look very carefully at whatever was done with the Ganske

amendment, as this motion instructs us to do; but also, we want to be very sure that in doing this, we are not opening up another loophole. I think we all have good intentions here and intellectual competence in this area so that we can constructively and honestly address that.

Mr. Speaker, I also want to state that I have been working for a long time, both in my subcommittee with hearings, as well as outside the subcommittee, with those medical groups that have raised some legitimate concerns on this subject. I am going to continue those hearings on privacy, whether it be financial privacy or medical privacy; but whatever is done here is only a first-step foundation. The issue of privacy, more comprehensive, will have to be addressed by this Congress across the board. I want to be part of that project.

Mr. MARKEY. Mr. Speaker, I ask unanimous consent to transfer control of the remaining time of the Committee on Commerce minority to the gentleman from Michigan (Mr. Dingell), the ranking member of that full committee.

The SPEAKER pro tempore (Mr. Pease). Is there objection to the request of the gentleman from Massachusetts?

There was no objection.

Mr. DINGELL. Mr. Speaker, I yield myself 3 minutes.

Mr. Speaker, I rise in support of the motion to instruct the conferees on H.R. 10, the Financial Services Act of 1999.

I support the idea that we should have responsible modernization legislation. That legislation must contain strong protection for taxpayers, consumers, investors, that ensures the safety and the soundness of the banking system, as well as the efficiency, competitiveness and integrity of the capital markets of the United States, and also fair and nondiscriminatory access to our economic opportunities by all Americans.

I voted against H.R. 10 on final passage earlier this month because it did not meet these tests, and I intend to work hard in the House-Senate conference to improve this legislation so that all Members can support it in good conscience. We cannot come back to the House with a conference report that does not give consumers adequate control over their private, financial, and medical records.

Mr. Speaker, I would note that the so-called health information protections in H.R. 10 serve only to protect the insurance industry, not consumers. Proponents of the medical privacy provisions of H.R. 10 contend that consent is required before the insurer discloses personally identifiable health information to another party, but they never note that there is a two-page list of exemptions to this rule that basically guts any real right of the consumer to be protected, or his right of consent.

In fact, there is nothing in H.R. 10 that would prevent insurers from selling one's health information for profit. Neither are there any restrictions whatsoever as to what people or companies that receive one's medical records may do with them. They are free to sell one's records to employers, information brokers, banks, pharmaceutical companies, or anybody else they please for good motive or bad. Once one loses one's medical privacy, they cannot get it back.

The medical privacy provisions of H.R. 10 would actually preempt stronger State protections already in effect. It would wipe out over 57 State laws, many of which have stricter safeguards for sensitive medical records such as mental illness or HIV. There is also a question of whether enactment of the medical privacy provisions of H.R. 10 would preclude authority otherwise already available to the Secretary of Health and Human Services, to go forward with the issuance of real consumer privacy protections that apply to health information held by doctors, hospitals, and

government agencies.

In addition, the bill contains some rather laughable financial privacy provisions that tell a bank simply to disclose its privacy policy, if it has one. H.R. 10 also gives very weak protection to investors for transfers of sensitive financial information to third parties, leaving the door wide open for sharing one's personal financial information with affiliated telemarketers and others.

By voting to instruct the conferees on this bill, the House will be on record in favor of the strongest possible provisions to protect consumer privacy, both with regard to financial records and health records. A vote in favor will also put the House on record in favor of ensuring that this legislation will allow all consumers to ensure not only the benefits of the legislation and nondiscriminatory access to financial services and their communities. I urge all of my colleagues to support this motion.

Mr. Speaker, I reserve the balance of my time.

[Page: H6733]

Mr. GANSKE. Mr. Speaker, I yield 3 minutes to the gentleman from California (Mr. Thomas).

(Mr. THOMAS asked and was given permission to revise and extend his remarks.)

Mr. THOMAS. Mr. Speaker, as chairman of the Subcommittee on Health in 1996 and working on the legislation commonly known as HIPAA, there was a clear understanding that more and more as we computerize records and indeed, even today with paper records, we need a greater degree of security to provide for confidentiality for patients. That is why we purposefully put Congress under the gun. That is, we said in that legislation in 1996 that Congress had 3 years to act. If Congress did not act in 3 years, the Secretary of Health and Human Services would then write the provisions.

One would think that Congress would act on its own. I have to tell everyone within my voice, Congress is an institution that almost always reacts instead of acts. One of the best ways to get Congress to act is to create a time anvil. That is exactly what we have here.

At the end of August, the Secretary begins promulgating confidentiality and privacy regulations, unless Congress acts. It creates a requirement that Congress act.

The gentleman from Maryland (Mr. Cardin), a member of the Committee on Ways and Means and myself have been working on confidentiality legislation which will be bipartisan and comprehensive.

[TIME: 1315]

What was placed in this financial services package because of the timing of the movement of this product is absolutely appropriate. It says that the paragraph will not take effect, or shall cease to be effective, on and after the date on which legislation is enacted that satisfies the requirements. It says, if Congress does its job, this provision does not do its job.

I want Members to understand what the Democrat motion does. It says, they will recede to the Senate on that provision I just read. What is in the Senate? Nothing. In other words, they are asking us to recede to the Senate on nothing.

Everybody knows the phrase, less is more. This drives it to the position that nothing is maximum. It removes the anvil. It means there is less pressure on us to do our job that we said we were going to do 3 years ago. Where is the pressure to force the appropriate compromise if we have no pressure at all on these Members, without the administration to write the regulations?

(Mrs. CAPPS asked and was given permission to revise and extend her remarks.)

Mrs. CAPPS. Mr. Speaker, I thank my colleague for yielding time to me.

Mr. Speaker, I rise in strong support of this motion to instruct the conferees on H.R. 10. In particular, I want to commend the gentleman from New York (Mr. LaFalce) and the gentleman from Michigan (Mr. Dingell) for the language contained in this motion regarding the importance of medical privacy.

Let me say first that I strongly believe this Congress should pass financial services modernization this year. Laws governing this industry are outdated and inefficient. They increase consumer costs and they limit consumer choices. They need to be changed. But in so doing, we must ensure that we protect not only the privacy of consumers' sensitive financial information, but also of their medical records, as well.

As a nurse, I know that in order to be effectively treated, patients must share all their health information with their doctors, therapists, and other providers. No diagnosis is complete without it. But if patients do not feel that their information will stay put with their health care provider or insurance company, if they cannot be sure that their most private and sensitive information will be kept confidential, they will not be so forthcoming. That would hurt patient care.

I wish to submit now for the Record a list of national organizations opposed to the medical records provisions in H.R. 10.

In contrast to the House version of H.R. 10, we must ensure that the financial modernization legislation that comes out of conference protects patient privacy. With that in mind, I urge a yes vote on this motion to instruct.

The list of organizations opposed to the medical records provisions in H.R. 10 is as follows:

Organizations Opposed to the Medical Records Provisions
in H.R. 10

PHYSICIAN ORGANIZATIONS

American Medical Association

American Psychiatric Association

American College of Surgeons

American College of Physicians/American Society of Internal Medicine

American Academy of Family Physicians

American Psychological Association

NURSES ORGANIZATIONS

American Nurses Association

American Association of Occupational Health Nurses

PATIENT ORGANIZATIONS

Mr. GANSKE. Mr. Speaker, I yield 3 minutes to the gentleman from California (Mr. Dreier).

(Mr. DREIER asked and was given permission to revise and extend his remarks.)

Mr. DREIER. Mr. Speaker, I thank my friend for yielding time to me.

Mr. Speaker, I am standing here because I think there has been a gross mischaracterization of the medical privacy provisions in this bill. When we had the debate on H.R. 10, legislation which I am very pleased got 343 votes when it was reported out of this House, criticisms that came from many on the other side, and frankly, from many in the media who took advantage of that mischaracterization, I think, make it necessary that we address it.

H.R. 10 and the provisions that were included here in fact will not, as we pointed out in the debate at that time, preempt State privacy laws. It does not in any way allow insurance companies to sell medical information to drug companies. It does not, as we found already in this debate, block the Secretary of Health and Human Services from issuing privacy regulations as required by current law.

I want to commend my friend, the gentleman from Iowa (Mr. Ganske), who has spent a long time working on this, and at the same time, my colleague, the gentleman from California (Mr. Thomas), the chairman of the subcommittee, does make a very valid point in his call to make sure that we continue to have that pressure point recognized there.

I think that the only real, legitimate debate here is whether the medical privacy issue is better addressed in H.R. 10 or in some other fashion. So I think we are going to see what obviously is going to be an interesting challenge here.

I think it is important for us to clarify exactly what the gentleman from Iowa (Mr. Ganske) was trying to do. Clearly we want to make sure that privacy is recognized and is in no way jeopardized.

The SPEAKER pro tempore. Without objection, the time previously claimed by the gentleman from Minnesota (Mr. Vento) will be reclaimed by the gentleman from New York (Mr. LaFalce).

There was no objection.

Mr. LaFALCE. Mr. Speaker, I yield 1 minute to the gentleman from North Carolina (Mr. Watt).

Mr. WATT of North Carolina. Mr. Speaker, most of the debate up to this point has been focused on the issue of privacy. That is, in fact, an important issue as we move forward to modernize financial services. We have to assure the protection of the privacy of consumers' financial and medical records.

I want to direct my colleagues' attention to paragraph 2 of the motion to instruct and rise in support of the motion to instruct conferees, because that paragraph gets to the heart of what financial modernization is about.

We are instructing the conferees to ensure that we come back with a bill that ensures consumers enjoy the benefits of comprehensive financial modernization legislation, that provides robust competition, and equal and nondiscriminatory access to financial services and economic opportunities in their communities.

As we move forward in this process, we are modernizing financial services, but we have to keep in mind that this is for the benefit of consumers and communities. Let us support the motion to instruct for that reason.

[Page: H6735]

Mr. LaFALCE. Mr. Speaker, I yield 1 minute to the gentleman from Connecticut (Mr. Maloney).

Mr. MALONEY of Connecticut. Mr. Speaker, I thank the gentleman for yielding time to me.

Mr. Speaker, I rise to commend the gentleman from New York (Mr. LaFalce) for his leadership on this issue, and to urge support of his motion to instruct conferees on H.R. 10.

Today's motion to instruct contains three important elements. It would ensure the strongest consumer privacy possible, it would provide equal and nondiscriminatory access to financial services, and it would protect medical privacy.

Unfortunately, the House hastily included medical privacy provisions in H.R. 10 that may actually be harmful to consumers because they do not rise to the level of basic protections afforded under any of the major medical confidentiality bills now being considered by Congress. That unintended result may in fact deter many patients from seeking necessary health care out of fear of disclosure.

The motion instructs the conferences to restore the confidence of the American public in the privacy of their sensitive health care information by removing medical-related provisions currently contained in H.R. 10.

Mr. Speaker, we have an historic opportunity to pass a balanced bill. I urge passage of the motion to instruct.

Mr. LaFALCE. Mr. Speaker, I yield 1 minute to the gentleman from New York (Mr. Meeks).

Mr. MEEKS of New York. Mr. Speaker, today we send our Members of the House to work with the members of the Senate to work out a compromise on the Financial Services Act of 1999. While we know, understand, and recognize that banks and other financial companies must be able to compete in an environment that will allow them to expand their powers and become competitive globally, and that our financial institutions are one of the most critical components to ensuring a healthy U.S. economy, our first and foremost responsibility is to those individuals who send us here to Washington each and every election day.

Therefore, we must ensure that consumers as well as financial institutions benefit from banking reform. It is meant to protect them from the misuse of their confidential personal information, this amendment, for marketing or other purposes, maintaining their medical privacy, and to make certain that our financial institutions that receive the benefit of government support continue to contribute to the economic health of low- and moderate-income communities.

Let me say, we must support CRA. It is an absolute necessity if we are to have a successful bill.

Mr. Speaker, today we send our members of the House to work with the members of the Senate to work out a compromise on the Financial Services Act of 1999. The purpose of this act is to provide banks and other financial companies with an environment that will allow them to expand their powers and become more competitive globally. Our financial institutions are one of the most critical components to ensuring a healthy U.S. economy. They are so critical that this Nation develop an independent body known as the Federal Reserve to regulate these institutions. Thus it is vital that this House and the Senate work diligently, and efficiently to develop a final version of the Financial Services Act that will make certain American

institutions have a fair opportunity to be the most competitive in the world. However, each of the conferees must remember that their primary goal as members of this House is to protect the interest of the individual citizens of this nation who send us to Congress and who own this nation.

Therefore, we must insure that consumers as well as financial institutions benefit from banking reform. It is meant to protect them from the misuse of their confidential personal information for marketing or other purposes, maintain their medical privacy, and make certain that our financial institutions that receive the benefit of government support continue to contribute to the economic health of low- and moderate-income communities.

Let me take a moment to emphasize the importance of the Community Reinvestment Act or CRA. There are some in the Senate who believe that CRA is a burden to banks. Let me assure those individuals that they are mistaken. The facts are clear, the overwhelming majority of evidence states that CRA has been a major success. It has been a benefit to low and moderate income individuals, their communities, and most of all to banks. Since 1977, banks and thrifts have made over $1.057 trillion in loan pledges to low-income areas. CRA investments have been widely credited with dramatically increasing home ownership, restoring distressed communities, helping small businesses and meeting the unique credit needs of rural communities. Financial institutions such as Citigroup, BankAmerica, Southwest Bank of Texas, Iron and Glass Bank, and a host of others have all made it clear that CRA is good policy and good for business.

I urge my colleagues to vote in favor of banking legislation that is good for banks and good for consumers. Vote for the motion to instruct.

Mr. GANSKE. Mr. Speaker, I yield 1 minute to the gentleman from Georgia (Mr. Linder).

Mr. LINDER. Mr. Speaker, this is getting curiouser and curiouser. In the Committee on Banking and Financial Services, when this bill was going through it was the Democrats, the gentleman from Washington (Mr. Inslee) who demanded privacy language, very strict privacy language.

It was the gentleman from Minnesota (Mr. Vento) who, with the gentleman from Iowa (Mr. Leach) late at night worked out a compromise on the privacy language, the first consumer protection language in the banking bill .

It got to the Committee on Commerce and the gentleman from Massachusetts (Mr. Markey) passed on a voice vote strong consumer privacy language, but even he was shocked it passed, and made it a huge point on the floor of the House that his language was not being adhered to. It had to be stronger.

Now they come out today and say, we do not want anything; accede to the Senate's nothingness, no consumer protection at all. Or is it maybe that they would rather have the administration write the language? They are acceding to a bill that is absent the language. They cannot have it both ways.

[TIME: 1330]

This banking legislation, as it left this House, had some of the best privacy language of any banking legislation, and now my colleagues want to walk away from it, and they ought to be ashamed.

The SPEAKER pro tempore (Mr. Pease). The Chair advises Members that the proponent of the motion is entitled to close debate. The Chair anticipates that Members controlling time will close in the reverse order of the manner in which time was allocated; to wit: the gentleman from Iowa (Mr. Ganske), the gentleman from Michigan (Mr. Dingell), the gentleman from Iowa (Mr. Leach), and

that we pass this motion.

Mr. GANSKE. Mr. Speaker, I yield myself 1 minute.

Mr. Speaker, I think the debate on the floor on this issue demonstrates what a Gordian knot the whole issue of medical privacy is.

The provisions that were in this bill on health care privacy are good ones. I think that if my colleagues look at the `Dear Colleague' that I have sent out, it explains it. It is not a comprehensive piece of medical privacy, but I thought it would improve the bill. The intentions were good for that.

However, a very large number of privacy groups have argued against this provision. I think it has been mischaracterized. It will be a serious impediment in terms of our getting the overall bill passed.

If, in fact, my colleague from California and others on the other side of the aisle can come up with a bipartisan agreement, then I am sure that it can be reintroduced at some time.

I am for a comprehensive bill. I will vote for the motion to instruct.

Mr. Speaker, I yield back the balance of my time.

Mr. DINGELL. Mr. Speaker, I yield myself 3 minutes.

Mr. Speaker, I would begin by expressing great respect and affection for everybody who has participated in this debate, especially the gentleman from Iowa (Mr. Ganske) who is an outstanding Member of this body in all particulars.

I do think it is important we understand what is at stake here. I will address only the question of protection of medical privacy.

Here is what the administration says. The administration strongly opposes the medical privacy provisions of the bill. Unfortunately, those provisions would preempt important existing protections and do not reflect extensive legislative work that has already been done on this complex issue.

The administration thus urges striking the medical privacy provisions and will pursue medical privacy in other fora.

Now listen to what some of the unanimous voices of all professional organizations in the field of medicine have had to say. First, the American Medical Association, I quote, `Medical records provision of H.R. 10 undermine patient privacy. The bill would allow the use and disclosure of medical records information without consent of the patient in extraordinarily broad circumstances. Unfortunately, the medical records confidentiality provisions of H.R. 10 will deter many patients from seeking needed health care and deter patients from making full and frank disclosure of critical information needed in their treatment.'

The American Nurses Association said this, `The proposed language would facilitate the broad sharing of sensitive health and medical information without the consent of the consumer.'

Here is what the American Civil Liberties Union said, `This proposal will preempt existing medical privacy protections and offers essentially no privacy rights to replace the ones which the amendment, if enacted, will usurp. It is deeply flawed.'

AFL-CIO: `This provision would facilitate the broad sharing of sensitive medical information in a matter that is harmful to health care consumers.'

That tells my colleagues what is said about this. I would urge the adoption of the motion.

[Page: H6737]

Mr. THOMAS. Mr. Speaker, will the gentleman yield?

Mr. DINGELL. I yield to the gentleman from California.

Mr. THOMAS. Mr. Speaker, I thank the gentleman for yielding. The consequences that the gentleman described, in fact, may take place if given this language as a sunset does not produce congressional legislation; is that correct?

Mr. DINGELL. Mr. Speaker, no, that is not correct.

Mr. THOMAS. Mr. Speaker, it is not a trigger that says it will sunset?

Mr. DINGELL. Mr. Speaker, what is correct, I would observe to the gentleman from California, is that, if this language is in here, the fears that I have expressed and the fears that are expressed by the professional health care organizations and individuals would occur.

Mr. THOMAS. But if we passed legislation, that language goes away, Mr. Speaker.

Mr. DINGELL. The way to address the matter is to take out unfortunate language and put in good language in a separate medical records privacy bill. At least, if we do not allow this language to remain in the legislation when it finally does go to the President, if that occurs, it would then assure that we would keep in place existing protections of patient privacy which are superior.

Mr. THOMAS. Mr. Speaker, if we pass better legislation, we will improve privacy.

Mr. LEACH. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, there are three aspects of this motion to instruct. As chair of the committee, I strongly support the first two. On the third, I remain somewhat bewildered.

What the third instruction suggests is that the committee should advance strong medical privacy provisions. Then it goes on to say that we should delete the title related to medical privacy and recede to the Senate which has no title on medical privacy. It is a conundrum, a logical inconsistency.

I would say to the gentleman in furtherance of certain earlier comments that only about 18 States have prohibitions on the sharing of information. This bill is not designed to supplant, replace, or weaken any State provision or deny future State provisions. It may not be quite as strong as the gentleman would prefer, but it is the first serious prohibition on an insurance company giving medical privacy information without patient consent to an affiliate or third party.

As chairman of the Committee on Banking and Financial Services and as a conferee, I am willing to accede to this motion under the understanding that it is a conflicted motion. There is a call for medical privacy and then a call for a deletion.

So what I think the gentleman and what this instruction is saying is that there should be a medical privacy provision in this bill. That being the case, I cannot object to this particular instruction as a conferee.

So I would urge my colleagues to recognize that the first two provisions are a call to support the

There was no objection.

The SPEAKER pro tempore. The question is on the motion to instruct offered by the gentleman from New York (Mr. LaFalce).

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. DINGELL. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Evidently a quorum is not present.

The Sergeant at Arms will notify absent Members.

The vote was taken by electronic device, and there were--yeas 241, nays 132, not voting 61, as follows:

Roll No. 355

[Roll No. 355]

YEAS--241

Abercrombie
Ackerman
Allen
Andrews
Baird
Baldacci
Baldwin
Barcia
Barrett (WI)
Barton
Becerra
Bentsen
Bereuter
Berkley
Berry
Biggert
Bilbray
Bishop
Blagojevich
Blumenauer
Boehlert
Borski
Boswell
Boyd
Brady (PA)
Brown (FL)
Brown (OH)
Campbell
Capps
Capuano

HIAA
Health Insurance Association of America

FAX TRANSMISSION

Date:	August 3, 1999 10:40 AM	**Pages:**	7
From:	Robin Bowen		
Phone:	**202/824-1669**	**Fax:**	**202/824-1651**

Deliver To: Chris Jennings

Company: White House

Phone: **Fax:** 202/456-5557

Message:
Per Sharon Cohen discussion of 8/2 -- medical confidentiality

June 25, 1999

The Honorable Thomas J. Bliley, Jr.
Chairman, House Commerce Committee
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

On behalf of the Blue Cross and Blue Shield Association (BCBSA) and Health Insurance Association of America (HIAA), we respectfully write concerning the Privacy of Consumer Information (Title V) and Confidentiality of Health and Medical Information (Title III, Section 351) provisions of H.R. 10, "The Financial Services Act of 1999," as reported by the House Commerce Committee.

We believe that consumers should have confidence that personal information shared with their insurer will be kept confidential. To achieve this goal, any federal confidentiality legislation should balance the need to safeguard consumers' personal and medical information while ensuring that financial institutions, including insurance companies, are able to efficiently provide services to customers. We appreciate your leadership on H.R. 10. However, we have significant concerns with the privacy and confidentiality provisions included in the bill reported by the Commerce Committee. Because these provisions may be considered in further deliberations on the bill, we wish to outline the serious problems that the provisions could pose for the delivery of health insurance services throughout the country. Some of those problems, as we view the matter, could be sufficiently severe as to fundamentally disrupt our health insurance system as we know it today.

Title V: Privacy of Consumer Information

We are concerned, first of all, that Title V (Privacy of Consumer Information), particularly the "opt-out" requirement in Section 501(b), could seriously affect the ability of health insurance companies to service their customers.

Health insurers commonly contract with or share information with affiliates, providers, contractors, and other third parties to perform essential functions on behalf of their subscribers. Such essential functions include quality assessment and improvement activities, reinsurance, audits, fraud and abuse detection, case management, claims processing, subrogation, research, and other services benefiting policy holders. As drafted, Title V, and the "opt-out" provision in particular, could prohibit health insurers from performing these basic functions on behalf of

consumers who choose to "opt out." These functions are integral to the delivery of health insurance benefits, and this barrier to their performance would be thoroughly disruptive.

Even if these basic insurance business functions were determined to fall within one of Title V's exceptions to the "opt-out" requirement, there is no workable exception for the Access and Correction requirements of the title included in Section 501(c). Pursuant to those requirements, insurance companies could face what would amount to an administrative nightmare. Each time a claim was sent outside the company for processing, utilization review, or other such functions (often accomplished electronically), a copy of such claim information would, upon the insured's request, have to be produced manually and sent to the insured. Further, the insurance company would be required to establish an additional process for receiving and responding to beneficiaries' questions concerning such claims. The very point of many of the outside processes referred to is to "catch" and correct errors in the claims-related information that under the legislation would become the subject of beneficiaries' complaints. Adding such an administrative burden in the midst of processing would be very costly and would undermine efforts to better serve consumers.

In addition, insurance companies should have a consistent set of confidentiality rules to follow if federal legislation is enacted. Another concern with Title V of H.R. 10 is how it relates to the requirements under Section 264 of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191; 110 Stat. 2033). Separate laws having different notice requirements and inconsistent access and correction rules would be problematic for our plans, as well as confusing for consumers.

Section 351: Confidentiality of Health and Medical Information

We are also significantly concerned about the potential adverse consequences of Section 351 of the Bill (Confidentiality of Health and Medical Information).

Section 351 only allows companies, including insurance companies, to disclose health and medical information if consent is given by the customer, or if the information is used for certain insurance-related functions. Moreover, Section 351(a)(2) attempts to establish a list of all of today's insurance-related functions. However, it appears that many current functions are not included under this section (e.g., coordination of care, risk assessment, disease management, appeals, and other policyholder functions).

We are concerned that specifically codifying current insurance-related activities would limit health insurance companies' roles as they seek to redefine themselves to meet consumer demands of the 21st century. To illustrate, if Congress codified the definition of insurance company functions ten years ago, they would have omitted wellness, disease management, and other quality programs that health insurers commonly provide today.

In addition, Section 351 refers to genetic information. However the term is not clearly defined. As the scope of health and medical information includes genetic information, this duplication leaves the term "genetic" open to interpretation through litigation and regulation. Such an open-ended term would leave insurers and consumers vulnerable to conflicting and confusing rules on what genetic information includes and its appropriate uses.

We appreciate the House Commerce Committee's efforts to address medical confidentiality standards in light of the August deadline for congressional action on this matter as detailed in Section 264 of the Health Insurance Portability and Accountability Act (HIPAA). However, Section 351 is both critically flawed and fails to meet the requirements of Section 264. The provision specifically includes a sunset so that it "shall not take effect" or "shall cease to be effective" if Congress approves legislation that satisfies Section 264. Rather than risk the harm Section 351 could impose on health insurers and their subscribers, we recommend that this provision be removed from H.R. 10.

Relationship Between Title V and Section 351

Perhaps our most serious concerns relate to the relationship between Title V and Section 351. The extent of the problems posed for the health insurance industry by Title V will depend largely on how the exception for transfers "necessary to effect or enforce the transaction" is construed. If that exception is construed narrowly, so as to exclude from the reach of the exception many aspects of the insurance business, the problems of the title will be magnified – since the "opt-out" provisions will then apply to transfers integral to the business of insurance. The report language of Section 351 strongly indicates that many aspects of the insurance business are to be considered distinct from "effectuating or enforcing a transaction," thus exacerbating our concerns as to the problems that could be posed by Title V.

We are concerned, moreover, that much of the medical information that is exempted from Section 351 will, notwithstanding that exemption, be regarded as falling under the provisions included within the reach of Title V. Customers, accordingly, can be expected to freely "opt out" under Title V with respect to transfers exempted from the "opt-in" provisions of Section 351. The result, once again, will be a serious impediment to the conduct of the business of insurance, as consumers routinely preclude transfers critical to the performance of that business.

We believe the relationship between these two portions of the bill has not been adequately considered. In light of this concern, as well as the other considerations mentioned above, we strongly urge you not to pursue these controversial provisions until there is ample opportunity to thoroughly analyze the potential impact of the provisions through hearings and other avenues of debate.

Moreover, we urge you to resist, both in the Rules Committee and, if necessary, on the House floor, certain related amendments to H.R. 10 that we understand could be proposed for

consideration. In particular, we would strongly oppose enactment of an "opt-out" provision of the sort included in Title V even if the "opt-out" authority provided does not pertain to transfers to affiliates of the transferring entity, but is instead confined to transfers to independent third parties. Health insurers rely — and for the foreseeable future can be expected to rely — on unaffiliated contractors for the performance of many of the functions discussed above that are essential to services delivered to policyholders. Further, certain functions critical to cost-effective health insurance programs include the sharing of information with third parties that are neither affiliates nor contractors. For example, all efficient health insurance plans rely on the ability to coordinate the delivery of benefits when more than one insurance plan may have responsibility for some portion of the coverage. Confining the "opt-out" provision to transfers to third parties thus will provide little relief from the adverse consequences of Title V that concern us. We are convinced that the best way to avoid those consequences is to reject any "opt-out" provision of the sort proposed, whether that provision is comprehensive or limited to third-party transfers.

We appreciate your leadership in this area and look forward to working with you further on this and other issues.

Sincerely,

Blue Cross and Blue Shield Association
Health Insurance Association of America

cc: Speaker of the House J. Dennis Hastert
The Honorable Jim Leach
The Honorable David Dreier

H:\POL&REP\W01\POLICY\PRIVACY\hr10ltr625.doc

DRAFT July 6, 1999

Concerns About the Confidentiality Provisions of H.R. 10 "The Financial Services Act of 1999"

H.R. 10 contains two sections relating to confidentiality of personal or health information. Section 351, "Confidentiality of Health and Medical Information," requires protective practices by companies which underwrite or sell insurance contracts indemnifying against illness or disability. These protections involve maintaining confidentiality of medical and genetic information and allowing disclosure only with the consent of the customer for activities such as underwriting and account administration. Section 501, "Protection of Nonpublic Personal Information," requires financial institutions to protect the security and confidentiality of customers' nonpublic personal information. Further, Section 501 contains an "opt out" provision allowing consumers to direct that such information not be disclosed.

HIAA has major concerns about the provisions for confidentiality of health information outlined in H.R. 10:

1. Conflicting federal laws. Health insurers that fall within H.R. 10's definition of "financial institution" will be subject to two sets of potentially conflicting federal regulations for confidentiality of health information: H.R. 10 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA or PL 104-191.) In fact, one of the key sponsors of H.R. 10's confidentiality language, Representative Ganske (R-IA) says that the provision intentionally does not discharge HIPAA's authority, therefore allowing the Secretary of HHS to promulgate federal regulations for confidentiality of health information.

2. No preemption of state laws. Because neither H.R. 10 nor PL 104-191 supersedes state laws, health insurers will be subject to numerous sets of laws: the two federal laws and various state laws.

3. "Opt out" is problematic. Section 502 of H.R. 10 contains an "opt out" provision enabling consumers to direct that confidential health information not be disclosed to some third parties. This provision would harm claims administration and other health plan operations such as quality improvement activities.

4. Internally inconsistent provisions. H.R. 10 has internal inconsistencies for the handling of confidential health information because sections 351 and 501 contain potentially contradictory provisions. For example, the "nonpublic personal information" that must be protected according to section 501 might not be the same as the "individually identifiable customer health and medical and genetic information" that may not be disclosed according to section 351.

In addition to these major concerns, the provisions of H.R. 10 raise numerous questions and issues for health insurers and health plans:

1. Confusion about whether or not various types of managed care plans fall within the definition of "financial institution."

    - If a company sells financial services, indemnity or indemnity-like health insurance and "pure" HMO (pre-paid health care) products, it is unclear whether the entire company is considered a "financial institution" and therefore subject to the requirements of H.R. 10

    - The status of stand-alone managed care plans that are not included in the definition of "financial institutions" is unclear because they may not be considered to be "indemnifying" against illness.

2. Many questions about specific language within Subtitle A—Disclosure of Nonpublic Person Information, as listed below.

    - Section 501 (a) refers to "security" of customers' nonpublic personal information. What is the definition of "security" and how does the term relate to "confidentiality?" Most importantly how does the term relate to the proposed HIPAA regulations, "Security and Electronic Signature Standards" which appeared on PP 43242 of the August 12, 1998 Federal Register?

    - The term "customers" in section 501(a) is not defined. As such, it is quite possible that this opt-out requirement would be read to allow each individual covered under a health plan or health insurance contract to object to the disclosure of their personal health information.

    - Section 502 (b) (2). What does the term "marketing" encompass?

    - Section 502 (e) (3). The provision refers to "fraud" but does not mention "abuse." Suggest that the term "abuse" be added.

    - Section 502 (e) (3). The provision refers to "persons holding a beneficial interest relating to the consumer." The term "beneficial interest" is vague and needs to be better defined.

    - Section 502 (b) (2). This section describes exceptions that prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party. Is the Medical Information Bureau (MIB) covered by this exception? Are contractors who perform anti-fraud and anti-abuse activities covered by this exception?

    - Section 505 (c). This paragraph deals with definitions and refers to definitions in the Federal Deposit Insurance Act and in the International Banking Act of 1978.

A rigorous review of all definitions is needed so that the intent of provisions is consistent with current technology.

- Section 509 (7) (C). This paragraph deals with disclosures but does not include important health care terms such as "abuse" and "disease management."

Medical Privacy Language in H.R. 10

General

The Ganske language may reach more insurers 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. Key provisions of the HR 10 medical privacy language step backwards from the agreement industry, consumer advocates, employers and government were able to reach in the Senate HELP Committee.

Intent

Congressman Ganske has stated that it was his intent to 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 either **"with the consent,** or at the direction, of the customer;" or for the purposes outlined without consent.

- HR 10 allows personal health 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. The practical effect is that health information can be disclosed for many more purposes, including research and underwriting. The American public would want to be informed about disclosures and to have control over such disclosures. **

Undermining HIPAA Authority

- Supporters of HR 10 say the language is a positive step because it goes beyond current HHS authority. The HHS regulatory authority under HIPAA would extend to health insurers, long-term care insurers, and disability health insurers. Therefore, the scope of authority to regulate insurers does not leave significant numbers of persons information unprotected.

- Retaining the medical privacy language in HR 10 would create unnecessary conflicts in the health care industry over which set of rules will be applied to medical information. The health care industry has been arguing for a single set of rules, when discussing the comprehensive medical privacy bills. Trying to figure out which set of rules apply and in what setting, will create significant burdens on the health care community. HIAA and Blue Cross Blue Shield opposed the medical privacy language in HR 10 for this very reason.

Unlimited Scope of Disclosure

- Basic protections necessary to make health privacy provisions work are missing from the language. In addition to allowing disclosure without consent of the subject, there are no requirements that a release of health 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 send them the entire medical record. These issues are being addressed in comprehensive medical privacy legislation which HR 10 would undermine.

Redisclosures Without Consent

- While the financial privacy language includes prohibitions on re-use of personal data, those prohibitions do not apply to medical information. Once personal health information has left the control of an entity with some level of responsibility to maintain its confidentiality, the information can be subsequently disclosed or used for any purpose at all. An entity could receive information from an insurer and it can reuse or redisclose to anyone without restriction. 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 a patient's consent or knowledge. The comprehensive privacy bills include protections for re-disclosure.

Research

- The Ganske provision creates a huge loophole with regard to research information. We understand that it would allow transfer of information without consent for "marketing research." Also, the provision has no standard for how medical research information should be protected, or who might be able to obtain particularly sensitive information in the name of 'research' including marketing. All of the comprehensive medical privacy bills have some level of protection for how health information is used in research, and marketing is typically excluded from research.

- The language in HR 10 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 as it is under most of the comprehensive medical privacy bills. This would mean that a life insurer that conducts physical examinations could release medical information to someone conducting market research.

**** Language from Sec. 351**

"(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 . . ."

- List of validators in talking points

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF THE ASSISTANT SECRETARY FOR LEGISLATION

FROM: Andrea S. Levario

Room 410H.2, HHH Building
200 Independence Ave., SW
Washington, D.C. 20201

PHONE: (202) 690-7538
FAX: (202) 690-8425

DATE: 10/18/99

TO: DEVORAH ADLER

OFFICE:

PHONE: 456-5560 **FAX:** 456-5557

TOTAL PAGES (INCLUDING COVER): 2

REMARKS:

Congressional Invitees for Privacy Event

Senate	Staffer
Kennedy	Cybele Bjorklund
Dodd	Jeanne Ireland
Leahy	Krissy Pisanelli
Frist	Anne Phelps
Jeffords	Paul Harrington
Bennett	Chip Yost

House	
Markey	Angelique Skoulas
Waxman	Karen Nelson
Condit	Mike Dayton
Dingell	Bridgett Taylor
Stark	Ann Montgomery
Cardin	Priscilla Ross
McDermott	Jennifer Crider
Greenwood	Joel White
Bilirakis	John Manthei
Thomas	Chris Carey
Brown	Ellie Dehoney

Privacy Groups Interested in Health Privacy Reg

Jan Lori Goldman, Zoe Hudson and Rodney Hudson
Georgetown Health Privacy Project
(202) 687-6323
(202) 687-3110 (Fax)

Chai Feldblum [check spelling]
Georgetown University Law School

Jerry Berman, Jim Dempsey and Dierdre Mulligan
Center for Democracy and Technology (CDT)
(202) 637-9800
(202) 637-0968 (Fax)

Marc Rotenberg and David Sobel
Electronic Privacy Information Center (EPIC)
(202) 544-9240
(202) 547-5482 (Fax)

Robert O'Harrow of the Washington Post
(212) 445-4885

Robert Ellis Smith - Privacy Journal
(401) 274-7861

Will Bruno - American Psychiatric Assoc.
(202) 682-6060
(202) 682-6287 (Fax)

David Korn - President, Association of American Medical Colleges
(202) 775-9067

Ronald Weich - Representing the ACLU
(202) 778-1818
(202) 822-8106 (Fax)

Joanne Hustead
National Partnership for Women and Families
(202) 986-2600
(202) 986-2539 (Fax)

Chris Koyanagi
Judge David L. Bazelon Center for Mental Health Law
(202) 467-5730
(202) 223-0409 (Fax)

Jeffrey S. Crowley
The National Association of People with AIDS
(202) 898-0414
(202) 898-0435 (Fax)

AFEHCT

Association For Electronic Health Care Transactions

Thomas J. Gilligan
Executive Director &
Washington Representative

3513 McKinley St. NW
Washington, DC 20015 - 2513
Tel 202 244 6450 Fax 202 244 6570
E mail afehct @aol .com

October19th, 1999

Christopher Jennings
Deputy Assistant to the President for Health Policy

The Association For Electronic Health Care Transactions (AFEHCT) is a trade association, the membership of which is involved in the electronic transmission of health care financial and administrative transactions such as those listed in section 1173(a)(2). (See attached membership list.

AFEHCT is actively and aggressively involved in several health care issues currently at the forefront of dialogue and debate at the federal level. They include:

Y2k
Privacy of health care information
Security of health care information
Administrative Simplification (transaction standards)
Use of the internet for the transmission of health care transactions including Medicare

On December 13th, 14th, & 15th 1999, AFEHCT will be holding its annual Washington Policy Forum at the Hyatt Regency on New Jersey Ave. in Washington DC. A working draft agenda is attached. If you or any of your staff have any interest in any or all of the issues we would be happy to have them attend. Free of charge, of course.

Interested parties should contact

Tom Gilligan
202 244 6450 or
afehct@aol.com

so that we can make arrangements for seating and food.

Please circulate this invitation among your staff.

AFEHCT

Association For Electronic Health Care Transactions

Working Draft Agenda for AFEHCT's Annual Washington Policy Forum

1999 WASHINGTON POLICY FORUM

Hyatt Regency Washington

December 12th, 13th 14th, & 15th, 1999

Monday
December 13, 1999

8:00 Continental Breakfeast

Registration

8:45 Introductions
House Keeping Details

9:00 Keynote

9:45 **Y2K**

What I want to do here is hold a round table
(actually semi round on a raised dais)

Participants,

Two people from HCFA
? Broseker
?Kathy King

Two people from AFEHCT who have had a "hands on" experience at their company
Pat Hamby HBO Confirmed
Lee Ledbetter SMS

Y2K committees on the Hill
Frank Reilly Senate Y2k Committee Confirmed
Matt Ryan House Gov Reform committee Confirmed

AMA Jack Emery Confirmed

10:45 Break

11:00 **Transaction standards & Code Sets**

12: 15 Lunch

1:15 **Provider id** **final rule expected 12/99**
Patricia Peyton, (410) 786-1812

2:00 **Unique patient identifier!!!**
On hold & Pending leg/reg

2:45 Working Break

3:30 **Claims Attachments**
NPRM expected to be published **11/99**

Steve Barr HCFA ???????????

Who Else

4:15: **Employer ID** **final rule expected** **12/99**
Mary Emerson, (410) 786-7065

5:00 PM Adjourn

6:00 --- 7:30 **Reception**

Tuesday
December 14

8:15 Continental Breakfat

9:00 AM **Privacy NPRM** **11/99**

Free an open discussion of issues reaction to the NPRM if published, by all participants

Moderated by Jean Scott National Data Corp.
& Pat Hamby HBOC

Participants

HHS

Gary Claxton **Confirmed**
Deputy Assistant Secretary for Health Policy

John Fanning **Invited**
HHS

OMB

Peter Swire **Invited**
Chief Counsel for Privacy
U.S. Government

House

Ways and Means subcommittee on Health
Staff **Chris Carey** **Confirmed**

Commerce Committee
Member staff Joel White **Confirmed**

Senate

H.E.L.P. Committee Staff
Kristin Welsh **Confirmed**

10:15 **Break**

10:30 AM **Work group review of the NPRM on Privacy**
Expexted to be published in "fall" 1999

- **Identify issues important to AFEHCT**
- **Formulate AFEHCT response to issues**

Moderatedby
Jeanne Scott National Data Corp
Pat Hamby HBO

Participants: **All Attendees**

12 30 PM Lunch

1 :45 • **Security** **final rule expected** **12/99**
Moderated by Shannah Koss IBM
Chuck Meyer HBO

Speakers John Parmagiani HCFA
Barbara Clark HCFA

3:00 PM **Medicaid ???** **???**
The head of the state Medicaid directors
Theprivate sector task group

4:00PM **The End of the Clinton Administration**
Year 2000 brings an end of the Clinton Administration. Who will be the next President be?

? **What would a Bush administration mean for our industry??**

? **What would a Gore administration mean for our industry??**

? **What would a Bradley administration mean for our industry??**

? **What would a McCain administration mean for our industry??**

Come to this meeting and hear from authoritative sources from each camp!!!!!!!!!

Wednesday
December 15, 1999

Internet Interoperability Pilot project

AGENDA

8:15	Continental Breakfast	
9:00	Internet Interoperability Pilot Project	Welcome Kepa Zubeldia, M.D., ENVOY
9:30	Batch Workgroup Report	_____,
10:00	Real Time Workgroup Report	_____,
10:30	Working Break	
10:30	Web Browser Workgroup Report	_____,
11:00	E-Mail Workgroup Report	_____,
11:30	Identification & Certification Authority Workgroup	Ruth Tucci-Kaufhold, Unisys
12:00	Working Lunch	
1:00	General Discussion	Kepa Zubeldia
2:00	Discussion of Deliverables	Bart Brown, UHIN
4:30	Determination of next steps	
5:00	Adjournment	

AFEHCT

Association For Electronic Health Care Transactions

Thomas J. Gilligan
Executive Director &
Washington Representative

3513 McKinley St. NW
Washington, DC 20015 - 2513
Tel 202 244 6450 Fax 202 244 6570
afehct@aol.com

MEMBERSHIP

The Association For Electronic Health Care Transactions (AFEHCT) is a trade association, the membership of which include:

- o health claims clearinghouses
- o health insurers
- o value added networks
- o software venders
- o health care data processing companies
- o practice management companies
- o data communications systems operators
- o credit card issuers

Each of these member companies is involved in the electronic transmission of health care financial and administrative transactions such as those listed in section 1173(a)(2):

- Health claims or equivalent encounter information
- Health claims attachments
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payment
- First report of injury
- Health claims status
- Referral certification and authorization.

AFEHCT MEMBERSHIP LIST

ANTHEM	Indianapolis, IN
ARCANVS	Salt Lake City, UT
BC / BS OF GEORGIA	Columbus, GA
BEACON PARTNERS	Hoffman Estates, IL
BLUE CROSS & BLUE SHIELD ASSOCIATION	Chicago, IL
CARE - FULL SOLUTIONS	Cecil, PA
CONSULTEC	Tallahassee, FL
DIFFERENTIAL INC	Cupertino, CA
EDI-COMM	Woodland Hills, CA
EDS	Plano, TX
ELECTRONIC CLAIMS SERVICE INC	Houston, TX
EMPIRE BLUE CROSS	Syracuse, NY
ENVOY CORPORATION	Nashville, TN
HBO & CO	Atlanta, GA
HDX	Malvern, PA
HEALTHEON	Santa Clara, CA
IBM	Tampa, FL
INTEGRATED VISION SYSTEMS	Sebastion, FL
IVANS	Tampa, FL
JOHN DEERE HEALTH CARE INC.	Moline, IL
MASTERCARD INTERNATIONAL	Purchase, NY
MEDIC COMPUTER SYSTEMS	Raleigh, NC
MEDE AMERICA INC.	Mitchell Field, NY
M & M COMPUTER SYSTEMS	San Antonio, TX
NATIONAL DATA CORPORATION	Atlanta, GA
PASSPORT HEALTH COMMUNICATIONS	Nashville, TN
PARAMORE CONSULTING	Louisville, KY
PENN STATE GEISINGER HEALTH SYSTEM	Danville, PA
PER SE TECHNOLOGIES	Atlanta, GA
POINTSHARE	Seattle, WA
PRAGMATIX	Elmsford, NY
QUADAX, INC	Cleveland, OH
STERLING COMMERCE	Dublin, OH
TERBUSH & PARKER SYSTEMS	Richmond, VA
THE CENTRIS GROUP	Atlanta, GA
THE HEALTH INFORMATION NETWORK CONNECTION(THINC)	New York, NY
UNISYS	Fairfax, VA
VISA INTERNATIONAL	San Francisco, CA
WELLPOINT	Los Angeles, CA

American Federation of Labor and Congress of Industrial Organizations

815 Sixteenth Street, N.W.
Washington, D.C. 20006
(202) 637-5000
http://www.aflcio.org

October 8, 1999

Mr. Chris Jennings
Deputy Assistant to the President
for Health Care Policy
The White House
Washington, DC 20500

Dear Mr. Jennings:

As the Administration moves forward to meet its responsibilities under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 to enact regulations governing the confidentiality of individually-identifiable health information, it is of critical importance to American working families that health information and medical records related to occupational conditions be accorded the same respect and protection that will apply to health information and medical records derived from non-occupational conditions.

It is a fundamental issue of fairness and equity that all medical records be treated the same. Workers, simply by virtue of the origin of their medical condition, should never be treated as second-class citizens. We do not believe that Congress intended or expected American workers to surrender the right of privacy over their medical records as a condition of employment.

While we recognize that the statutory definition of health plan under HIPAA does not reach workers' compensation, automobile and other liability insurance, we see no statutory bar to applying HIPAA privacy regulations to providers of workers' compensation benefits who handle and prepare medical records in connection with delivery of these medical services. Thus, these regulations can and should require health care providers to limit the information they release to insurers and employers to only that information that they determine is both appropriate and necessary. Providers should be restricted from divulging any information about an individual's health records to employers and workers' compensation insurers except for information that is directly related to whether the claim is work-related, meaning for the limited purposes of determining eligibility for coverage and for payment of the claim, and for information that they

need to know in order to make work-related accommodations or to comply with work-restrictions. Special rules should apply to employers who provide "onsite" or "in plant" or company-controlled medical care. In this way, health care providers who are employed or controlled by such employers will be subject to the same rules that apply to all other health care providers. Health care providers should be subject to sanctions and criminal penalties for any violation of these safeguards.

Sincerely,

Gerald Shea
Assistant to the President
for Public Policy

cc: Karen Tramontano

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.

HEALTH PRIVACY PROJECT
INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

The State of Health Privacy: An Uneven Terrain

Executive Summary

There is no comprehensive federal law that protects the privacy of people's health information. The U.S. Congress is moving ahead to meet a self-imposed deadline to enact a broad health privacy statute by August 1999. If the deadline is not met, the Secretary of Health and Human Services must issue regulations by February 2000. At this time, people must rely on whatever health privacy protections are built into their state's statutes.

As the congressional debate over health privacy heats up, there is a question that is always asked but— until now— has been impossible to answer. "What state laws exist in this area? How have states responded to the health privacy needs of their citizens?"

This report is the first-ever comprehensive 50-state survey of health privacy statutes. In our experience, the hallmarks of researching state health privacy laws have been that: 1) nothing is simple; and 2) nothing is predictable. In the process of researching, analyzing, and summarizing the statutes, we reached a number of conclusions and made a few surprising discoveries. But in many more ways, the states defy categorization.

State laws relating to health privacy have been enacted at different points in time, over many years, and to address a wide variety of uses and public health concerns. One must approach each state on its own terms and attempt to understand the protections as a unique whole within the state. In striving for precision and nuance, our labels of state laws are accompanied by qualifiers and explanations.

Laws relating to health privacy can be found in nearly every nook and cranny of a state's statutes – in obvious and obscure sections of a state's code, buried in regulations, developed in case law, and detailed in licensing rules. Florida, for example, has more than 60 statutes that address health privacy, and the state is not unique.

A number of initial observations emerge from the state summaries:

States legislate and regulate health privacy by entity.

There is little mystery about why state health privacy laws are so extensive, vast, and detailed: the statutes reflect the diverse users of health information. Consider the following four types of users: physicians, schools, insurers, and state agencies. Each has a specific function in the state and a legal and regulatory structure specific to its roles. Thus, the statutory requirements for how they handle medical information are different.

To understand what confidentiality protections do exist at the state level, one must first begin by

examining the laws applying to the different entities that collect, use, maintain, and distribute health information. Even states that attempt to handle health privacy in a comprehensive fashion ultimately establish unique rules for different entities. In looking at a state's laws and determining what kind of privacy protections exist, one must always ask, "Who's holding the data?" and "What is the medical condition at issue?"

The end result of this legislating by entity is that state laws – with a few notable exceptions – do not extend *comprehensive* protections to people's medical records. Thus, a state statute may impose privacy rules on hospitals but not dentists. The state may restrict the use and disclosure of information derived from a genetic test but not information obtained in a routine physical. Or just the opposite may be true in a neighboring state.

The cumulative effect of these various statutes might appear erratic, but so many of the laws that do exist provide meaningful protections for consumers and speak to the specific needs of the organizations and citizens of the state. For instance, a nursing home may have different information needs than a public hospital, and state laws attempt to accommodate these differences.

The vast majority of state statutes were never intended to be comprehensive.

Virtually every state has some law aimed at the confidentiality of patient information, but very few states have anything approaching a comprehensive health privacy law. Three notable exceptions are Hawaii, Rhode Island and Wisconsin, each of which has comprehensive health privacy laws. Many states have health privacy laws governing certain health care entities, such as hospitals or clinics, but no privacy protections regulating health plans and HMOs.

State confidentiality requirements are part and parcel of larger statutes that provide consumer protections or regulate persons or entities. Many of the statutes, for example, are imbedded within licensing requirements. In this context, the provider is required to maintain health information in confidence in order to obtain and maintain a license to practice from the state. One must read *all* of the statutes together in order to glean an understanding of how health information is protected as it moves between persons and entities.

An ethical duty to maintain confidentiality is often assumed.

Most states appear to presume an ethical duty on the part of health care providers to keep information confidential. Many statutes, for instance, do not explicitly impose a duty of confidentiality, but they do stipulate a penalty for breaching patient confidentiality. It seems that in these instances, the states did not see a need to *legislate* the ethical duty. Unfortunately, the users of health information have extended well beyond those who may be bound by professional codes of ethics.

State laws have not kept pace with changes in health care delivery and technology.

Most state laws do not reflect the dramatic changes in the health care environment or the dramatic changes in information technology. Today, for instance, the majority of health care is not delivered by physicians. Integrated delivery systems (such as HMOs and provider networks) and the establishment of statewide health information databases have created new demands for data that push well beyond the limits originally anticipated by the states. The variety of people and entities collecting, receiving and using health information has also extended far beyond the health care environment. A physician, for example, may be obligated to report a person with epilepsy to the Department of Motor Vehicles, which in turn may revoke a driver's license.

Therefore, in many ways, the state laws defy summarization – they are detailed, specific, and intricate. Nevertheless, we have attempted to bring some coherence to this report. The summaries are arranged in four broad categories: Patient Right of Access, Restrictions on Disclosure, Privileges, and Condition-specific Requirements. Our major findings in each category are listed below.

Key Findings

Patient Access
States vary widely in the rights they grant to patients to receive and copy their own medical records. Some states have no statutory right of access, such as Kansas and North Dakota. Three states – Alabama, Idaho, and New Mexico – and the District of Columbia, only have a statutory right for patients to access their own mental health records.

On the opposite end of the continuum, a few states – such as Connecticut and Minnesota – grant access to records maintained by nearly all of the potential sources of patient data, i.e. government agencies and entities, hospitals, physicians, insurers, schools, and even non-traditional health care providers such as natureopaths. Maine and South Dakota, for example, have cast a particularly wide net with respect to providing access to records maintained by health care providers by using broad definitions that anticipate future users and holders of medical information, such as those performing *in vitro fertilization* and blood banks.

Most states fall somewhere in the middle of these two extremes. Forty-four states provide *some* right of access, but this figure is a bit misleading. The right of access quickly breaks down:

33 states provide a right of access to hospital records;

13 states provide a right of access to HMO records; and

16 states provide a right of access to insurance records.

Many additional statutes cover specific providers – such as physicians, psychiatrists, and pharmacists. However limited the right, the impact of providing the right should not be underestimated. For example, in response to the public's desire to utilize alternative sources for contact lenses, Colorado and a few other states require optometrists to disclose prescriptions to their patients.

All state statutes that grant people a right to see and copy their own medical records limit that right with a set of exceptions. The most common exception is that a patient can be refused access to his or her own medical record if the record holder believes that the release of the information could endanger the life and safety of the subject of the information or another person.

Many states have also granted patients the right to amend or correct their medical information, particularly when the records are held by insurance companies. In Illinois, New Jersey and Ohio, for example, the statute includes a detailed procedure for resolving a patient's challenge to the accuracy or completeness of the record. Where the provider and the patient disagree, for example, the patient may be able to insert a statement of his or her position in the record.

Most states allow a person or entity to charge patients for copies of their medical record. Some states specify a cost in the statute – in Kentucky, for example, a health care provider or hospital must provide a patient with a *free* copy of their medical record. A patient may be charged for additional copies, but not more than $1 per page. Other states require that the fee be waived if the patient is contesting an adverse underwriting decision. The most common approach is to stipulate that an entity may charge a "reasonable" fee.

Restrictions on Disclosure
States vary widely in terms of the restrictions or prohibitions they impose on disclosures of medical records and medical information. The restrictions tend to be triggered in two instances: by the entity holding the data, and the kind of information being held.

For the most part, the state statutes prohibit *a person or entity* from disclosing information unless certain conditions are met. The most notable impact of this approach is that it may limit the actual protections afforded the data. Once the information is disclosed, it may or may not be afforded the same protections by the receiving entity. For instance, the state laws may not place limits on the re-disclosure patient data, or the receiving entity may not be under any legal obligation to adhere to the privacy rules imposed on

the disclosing entity.

In comparison, a few states – such as Wisconsin and Rhode Island – have statutes that prohibit *medical information* from being disclosed, regardless of the entity holding the record.

Overall, *the most common restriction found in state statute is that patient authorization must be secured prior to health information being disclosed.* Some states specify the format and content of the authorization form in statute. Many states allow patients to revoke authorizations.

At the same time, these statutes all specify numerous exceptions to this general rule in which a person or entity may disclose information without patient authorization. The most common instances include: for purposes of treatment; to secure payment for healthcare; for auditing; and for quality assurance activities. Most statutes allow access to patient data for research purposes, without any patient notification or authorization. (See later discussion on research.)

Also of note is that some states do prohibit the re-disclosure of medical information. In such instances, an entity that *receives* medical information is prohibited from re-disclosing the information unless a separate authorization is secured, or the disclosure is in keeping with the statutory requirements imposed on the original disclosure. Other states do not statutorily restrict the re-disclosure of medical information. In Montana, for instance, the state has adopted a public policy that recognizes that a patient's interest in the proper use of health care information survives its initial release by a health care provider. The state, however, has decided not to statutorily regulate subsequent disclosures because a person's expectation of privacy changes when the information is held by a non-health care provider.

Privileges

We have included a survey of states' statutory privileges for two reasons: 1) to date, all of the proposed federal health privacy legislation leave state privilege law intact; and 2) many states' statutes governing the confidentiality of health care information maintained by HMOs provide that an HMO is entitled to claim any statutory privilege against disclosure that the provider of the information is entitled to claim. Thus, in order to understand what privilege an HMO might be able to exercise, it is necessary to know what statutory privileges exist.

A common misconception about the physician-patient privilege is that it is a general prohibition against a health care provider sharing information about his or her patients. However, it is important to recognize that in *legal* terms, there is a distinction between "privilege" and "confidential." The law of privilege is generally seen as a rule of evidence which is limited in scope. It allows a patient in a legal or quasi legal proceeding to refuse to disclose, and to prevent others from disclosing, certain confidential information (usually communications) obtained during the course of diagnosis and treatment. In contrast, a health care provider's duty of confidentiality to her patients, arising from a code of ethics, by regulation, or otherwise, is a broader duty not to disclose to the public information obtained in a professional capacity.

That being said, it must be noted that even legal professionals often use the terms interchangeably. We have attempted to note where a state has worded its statutory privilege in such a way as to extend it beyond a legal or quasi legal proceeding.

It must be emphasized that this is a summary of statutory rules of privilege. Many more providers and entities may be covered by a state's common law privilege. The summaries do not include a discussion of when privilege may be waived. State law is detailed and voluminous on this subject, and we chose simply to indicate to whom the statutory privilege applies.

Condition-specific Requirements

Nearly all states have laws that impose condition-specific privacy requirements, most often to shield people with mental illness, communicable diseases, cancer, and other sensitive, stigmatized illnesses from broad disclosures. Many of these laws were passed to respond to public fear that certain health information would be widely disclosed and used to deny patients benefits or result in other harm. Where

this fear acted as a barrier to seeking health care, treatment, or counseling, states have moved to bolster public trust and confidence in the health care system by enacting heightened privacy rules in these specific areas. The protections tend to attach to the information at the point of collection, before the information is disclosed. These requirements may, for example, direct a provider, hospital, or laboratory to obtain a particular kind of authorization from the patient.

In some circumstances, the condition-specific requirements allow for *greater* disclosure of the information. Some mental health statutes, for example, explicitly allow family members to access the mental health records of a family member who has been committed. Other statutes allow employers to share medical information about an employee if it affects her performance on the job.

Most of the condition-specific requirements that exist at the state level, however, were enacted hand-in-hand with *mandatory* reporting laws. For instance, essentially all states require that health care providers report to governmental health authorities the identity of persons suspected or diagnosed as having specified contagious diseases, such as tuberculosis. Many states require providers to report the identity of children born with birth defects to a central registry. The statutes then limit how the health authorities or registry can use or disclose the information which has been collected. In most cases, however, the protections do not apply to any other entity holding the same information -- such as the provider, hospital, or insurance company. While the summaries note the protections afforded the data, it is important not to lose sight of the fact that these privacy laws were enacted on the backend of laws requiring doctors and other health care providers to report to state officials identifiable patient data related to certain illnesses and conditions. Clearly, state lawmakers viewed such privacy protections as a necessary balm to quiet public fears of the government developing health information databases on vulnerable citizens. Our inclusion of the public health reporting requirements and related privacy protections are not comprehensive, but we point out that many states' reporting requirements are aimed beyond communicable or infectious diseases. Many states collect health information to study costs, outcomes, and quality – all of which rely on extensive patient data. In turn, there is a great demand – often answered in the affirmative – for access to this data.

Remedies and Penalties
Most state health privacy statutes contain some form of remedies and penalties that are triggered by violations of the law. Commonly found are private right of action provisions granting people the ability to bring lawsuits when the statute has been violated, without first having to meet any additional standard of proof, i.e. that the violation was willful or intentional. It is enough that the law was violated. A full range of damages, remedies, and attorney's fees and costs are usually available, however the monetary damages are often set quite low. In some cases, these statutory remedies may be construed as exclusive, thereby barring people from raising other claims, such as privacy torts or other common law claims.

Government-maintained Records
Across the board, records held by government agencies and officials are treated differently – and are usually more protected – than the medical information collected and held by the private sector. In some instances, the medical records held by the government are the only records protected in statute. In effect, a state statute may impose confidentiality requirements only on public hospitals, leaving people who are treated in private hospitals without the same legal safeguards. In Oregon, for example, the statutory prohibitions on disclosure, including authorizations, apply only to *public* providers of health care. Private health care providers are simply "encouraged, but not required, to adopt voluntary guidelines limiting the disclosure of medical records..."

Although this legal distinction – between public and private holders of medical information – is rooted in the constitutional principle that there must be limits on government action vis-a-vis the individual, it may not be particularly meaningful to health care consumers. Therefore, privacy protections for other personal information have been extended in a number of federal and state privacy statutes to restrict the private sector's collection and use of personal information.

Research
Again, there is little uniformity in how state statutes regulate researcher access to people's medical information. The vast majority of laws, however, do allow researchers broad access to patient records.

As the laws apply to private entities, researcher access is almost always built in as an exception to a statute's patient authorization requirements. What limits do exist usually speak only to specific information – such as genetic information or HIV/AIDS information.

On the other hand, researcher access to patient data held by government entities, i.e., agencies or registries, is in some instances more detailed. Some registries, for example, have strict conditions that must be met before researchers can access data and may require that personal identifiers be removed before a researcher can access information.

Conclusion

Again, there is no comprehensive federal law protecting the privacy of people's medical records. Congress has acknowledged that such a law *should* be passed and imposed a deadline on itself to do so by August 1999. If Congress fails to meet the deadline, the Secretary of Health and Human Services is required to issue regulations by February 2000.

Health privacy is not a new issue to the U.S. Congress. Each year over the past decade, as debate has resumed over how to best craft a health privacy law, the question is inevitably raised, "What have the states done? What are the state health privacy laws? What will be the impact on the states of any federal preemption of state law? What negative and positive models exist for us to learn from?" For the most part, these questions have gone unanswered. Until now, no comprehensive compilation of state health privacy laws existed.

As this report documents, there is little probability that any federal law could match the breadth and scope of the existing state laws. As such, any federal law that *fully* preempted state law would eliminate some of the rights and protections consumers currently enjoy and disrupt current state legal and regulatory structures. Here's why –

States have been the first to respond to concerns about health privacy and they have enacted many strong protections.

State health privacy statutes cover a broad range of entities and, not surprisingly, are both weak and strong. In terms of broad consumer protections, one can identify many significant gaps and weaknesses in most state statutes: such as a limited right for a patient to access his or her own medical record; little ability for patients to limit disclosure of their medical records; and little recourse when the laws are violated.

On the other hand, state laws enacted in response to a particular public concern, or a public health threat– such as in the areas of mental illness, communicable disease, cancer, and genetic testing – are often strong, detailed, and aimed at the states' unique experiences with their citizens.

State laws address a level of detail not considered in any of the federal proposals.

The importance of the detail in state health privacy law should not be underestimated. Because the states legislate by entity, they are often able to craft laws that speak to the unique needs of the patient population and the information needs of particular entities. An HMO, for example, has very different needs than a family planning clinic.

State law is extensive – it is impossible to predict the full impact of full federal preemption.

Most importantly, it is almost impossible to predict the full impact of federal preemption on state laws relating to health privacy. Remember that these summaries are only the tip of the iceberg in terms of relevant state statutes. Many more laws govern areas such as adoption, workers compensation, public health reporting, civil, judicial and administrative procedures, fraud and abuse, and law enforcement access.

There is widespread consensus that a federal law could help to provide significant new protections and to establish some basic rules about the use and disclosure of health information. However, until this point, the policy debate about preemption tended to be based on rhetoric, not fact. There is a large body of law before us now. While many of the facts are reassuring, it does not lend itself to easy answers.

A significant challenge is before us. There is no doubt that such a comprehensive federal health privacy law could be beneficial in many ways. But while a federal law could substantially benefit people by establishing a baseline of consumer protections, a federal law that ignored the significant role states have played in protecting health information could disrupt the legal and regulatory structures at the state level and, in turn, some of the protections currently afforded to consumers.

Our hope is that this report will serve as the factual basis upon which to proceed, providing us with a true opportunity to move beyond the rhetoric that has so far defined this debate.

c. Disclosures for law enforcement purposes

[Please label comments about this section with the subject: "Law Enforcement Purposes"]

In § 164.xxx, we propose to permit covered entities to disclose protected health information to a law enforcement official conducting a law enforcement inquiry if the request for protected health information is made pursuant to a judicial or administrative process, as described below. Similarly, we would propose to permit disclosure of protected health information to law enforcement for the conduct of lawful intelligence activities. We would further permit such disclosure for the purpose of identifying a suspect, fugitive, material witness, or missing person, if the covered entity discloses only limited identifying information. As with all disclosures authorized under this subsection, the disclosure of protected health information must be authorized under other federal or state law.

i. Importance of law enforcement and the need for protected health information.

Protected health information may be needed as part of a law enforcement investigation. Health information about a victim of a crime may be needed to investigate the crime, or to allow prosecutors to determine the proper charge. For some crimes, the severity of the victim's injuries will determine what charge should be brought against a suspect. The medical condition of a defendant may also be relevant to whether a crime was committed, or to the seriousness of a crime. The medical condition of a witness may be relevant to the reliability of that witness. Medical, billing, accounting or other documentary records in the possession of a covered entity can be important evidence relevant to criminal fraud or conspiracy investigations.

In many cases, the law enforcement official will obtain such evidence through lawful process, such as judicially executed warrant, an administrative subpoena, or a grand jury subpoena. In other circumstances, time constraints preclude use of such process. For example, health information may be needed when a law enforcement official is attempting to apprehend an armed suspect who is rapidly fleeing. Health information may be needed from emergency rooms to locate a fleeing prison escapee or suspected rapist who was injured and is believed to have stopped to seek medical care.

Protected health information may be sought as part of a law enforcement investigation, to determine whether and who committed a crime, or it may be sought in conjunction with the trial to be presented as evidence. These uses of medical information are clearly in the public interest. Requiring the authorization of the subject prior to disclosure could impede important law enforcement activities by making apprehension and conviction of some criminals difficult or impossible.

ii. Proposed requirements.

In § 164.xxx, we propose to permit covered entities to disclose protected health information to law enforcement officials conducting or supervising a law enforcement inquiry or proceeding if the request for protected health information is:

(1) pursuant to a warrant, subpoena, or order issued by a court, or a subpoena issued by a grand jury subpoena; or

(2) pursuant to an administrative subpoena or summons, civil investigative demand, or similar certification or written order issued pursuant to federal or state law; or

(3) for the conduct of lawful intelligence activities conducted pursuant to the national Security Act of 1947 (50 U.S.C. 401 et seq) or is made in connection with providing

protective services to the President or other individuals pursuant to section 3056 of title 18, United States Code , and the disclosure is otherwise authorized under Federal or state law.

In § 164.xxx, we also propose to permit covered entities to disclose protected health information to law enforcement officials conducting or supervising a law enforcement inquiry or proceeding for the purpose of identifying a suspect, fugitive, material witness, or missing person, if the covered entity discloses only "limited identifying information" and the disclosure is otherwise authorized under Federal or state law.

Under the first part of this proposal, we would authorize disclosure of protected health information pursuant to a request that has been reviewed by a court or grand jury. For these requests, other law requires some showing that the requested information is relevant to an ongoing judicial or grand jury process, and we would not interfere with that process. These disclosures are permitted because they are mandatory under other law, and thus would be permitted by section xxx of this rule, above. We discuss them here in order to address all law enforcement issues together.

Also under this proposal, protected health information could be disclosed pursuant to any type of administrative subpoena or summons, civil investigative demand, or similar process authorized under federal or state law that includes formal review of the request for information and written evidence of that review. If the request is issued pursuant to an administrative process that is evidenced by the production of a subpoena, summons, or similar document, a covered entity may disclose protected health information in accordance with the terms of the document. The provisions of this section are intended to permit disclosure pursuant to the broad spectrum of administrative procedures by which law enforcement officials obtain approval of requests for information. The preceding list of legally authorized process is intended to provide examples of types of legal process which to which a covered entity may respond; it may not be exhaustive of the types of process available in different federal, state or local jurisdictions. A covered entity that complies with lawful process from a law enforcement official will not be subject to sanctions under this rule. We do not intend to disrupt legitimate law enforcement activities, and request comment on whether or not these provisions recognize the types of administrative approval procedures that currently exits.

This rule should not interfere with the conduct of lawful security functions in protection of the public interest, as defined by the Congress. Therefore, under this proposal, we would allow disclosure of protected health information for the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947. Similarly, we would allow disclosure of protected health information for providing protective services to the President or other individuals pursuant to section 3056 of title 18, United States Code. Where such disclosures are authorized by Federal or state law, we would not interfere with these important national security activities.

We anticipate that disclosure of health information by covered entities pursuant to this section will principally be made pursuant to lawful process. In some cases, however, law enforcement may be seeking limited but focused information needed to obtain a warrant. For example, a witness to a shooting may know the time of the incident and the fact that the perpetrator was shot in the left arm, but not the identity of the perpetrator. Law enforcement has a legitimate need to ask local emergency rooms whether anyone presented with a bullet wound to

the left arm near the time of the incident. Law enforcement does not have sufficient information to obtain a warrant, but rather is seeking such information. In such cases, when only limited identifying information is disclosed and the purpose is solely to ascertain the identity of a person, the invasion of privacy is outweighed by the public interest. Because only this limited identifying information could be disclosed, and thus the actual medical record could not be provided, the infringement on privacy is reduced. Therefore, we would permit covered entities to disclose limited identifying information in response to an oral or written request from law enforcement for the purpose of identifying a suspect, fugitive, material witness, or missing person.

We would define "limited identifying information" as the name, address, social security number, date of birth, place of birth, type of injury, and date and time of treatment. Disclosure of any additional information would cause the covered entity to be out of compliance with this provision, and subject to sanction. The request for such information may be made orally or in writing. Requiring the request to be in writing could defeat the purposes of this provision.

This section would not permit disclosure of protected health information absent a request, on the covered entity's own initiative. The circumstances under which such disclosure are permitted are described in section xxx, "Emergency Circumstances."

Under this section, covered entities would have an obligation to verify the legal authority behind the request. Covered entities would not be required to conduct any independent investigation of the legality of the process under which the protected health information is being sought, but would need to review the request to determine that the disclosure would meet the requirements of this provision. We would permit covered entities to rely on a badge or similar identification to confirm that the request for protected health information is being made by a law enforcement official. If the request is not made in person, we would permit the covered entity to rely on official letter head or similar proof.

Where the covered entity must verify that lawful process has been obtained, the document evidencing the order would be required. Such process may generally indicate the nature of the protected health information relevant to the law enforcement matter, or it may identify specifically what protected health information is sought. The covered entity could rely on either type of statement, but it could not disclose more information than was authorized in the document.

For requests for the conduct of intelligence activities or for protective services, covered entities would be required to verify the identity of the person or entity requesting the information, through a badge or other identification, or official letter head, as just described. If such verification of identify is obtained, covered entities would be permitted to reasonably rely on the representations of such persons that the request is for lawful national security or protective service activities and is authorized by law. Similarly, to disclose limited identifying information, covered entities would be required to obtain verification that the request comes from a law enforcement official, and would be permitted to reasonably rely on such official's representation that the information is needed for the purpose of identifying a suspect, fugitive, material witness, or missing person and is authorized by law.

We considered further specifying the type of documentation or proof that would be acceptable, but decided that the burden of such specific regulatory requirements on covered entities would be unnecessary. As a practical matter, covered entities will not be in a position to evaluate the purpose and scope of the requests made by law enforcement officials, or intelligence

agencies. Therefore, we propose only a general requirement for verification of identify, and permit reasonable reliance on law enforcement's representations regarding the legal authority for the request.

This section is not intended to limit or preclude a covered entity from asserting any lawful defense of otherwise contesting the nature or scope of the process when the procedural rules governing the proceeding so allow. Each covered entity will continue to have available legal procedures applicable in the appropriate jurisdiction to contest such requests where warranted. This rule does not create any new affirmative requirement for disclosure of protected health information.

In obtaining protected health information, law enforcement officials would have to comply with whatever other law was applicable. In certain circumstances, while this subsection may authorize a covered entity to disclose protected health information to law enforcement officials, there may be additional applicable statutes further govern the specific disclosure. If the preemption provisions of this regulation do not apply (section xxx), the covered entity must comply with the requirements or limitations established by such other law, regulation or judicial precedent. For example if State law permitted disclosure only after compulsory process with court review, a provider or payer would not be allowed to disclose information unless the law enforcement authorities had complied with that requirement. Similarly, disclosure of substance abuse patient records subject to Section 290dd-2, Title 42 United States Code, and the implementing regulations, Part 2, Title 42 Code of Federal Regulations, will continue to be governed by those provisions.

This section is only intended to provide authorization to covered entities to disclose health information to law enforcement agencies. It is not intended to compel any disclosures. Some disclosure of protected health information to law enforcement officials, however, will be compelled by law, for example, by compulsory judicial process or compulsory reporting laws (such as law requiring reporting of wounds from violent crimes, suspected child abuse, or suspected theft of prescription controlled substances). Such disclosure of protected health information are not addressed in this section, but would be permitted by this rule under section xxx, which addresses mandatory disclosure of protected health information generally.

We also have clarified that protected health information that could be disclosed under another provision of this rule would not be subject to any review requirement in this section. For example, if emergency circumstances described in section xxx exist, a covered entity may disclose protected health information upon the request of a law enforcement official under that section without the review that might otherwise be required under this section.

In developing our proposal, we considered permitting covered entities to disclose protected health information pursuant to any request made by a law enforcement official, rather than requiring some form of legal process. We rejected this option because we believe that in most instances some form of review should be required. Individuals' expectation of privacy with respect to their health information is sufficiently strong to require some form of process prior to disclosure to the government. At same time we recognize that the public interest is not served by requiring such formal process in every instance. Under our proposal, therefore, law enforcement may obtain certain identifying information in order to identify suspects and witnesses, and may obtain information for national security or protective services activities.

**In this notice, we are not proposing any new legal standards which the reviewing authority must meet in order to issue legal process for disclosure of protected health information

even in cases where there is no judicial or grand jury oversight. Instead, we rely on standards that may be stated in current relevant law. We have concerns about not specifying such a standard, due to the elevated expectations of privacy that people have with respect to their health information and the absence of such third party oversight. We are not specifying a standard here, for three reasons. First, we are not familiar with every standard for disclosure of protected health information applied today under every state or local law, and thus could inadvertently disrupt necessary local law enforcement activities. Second, we are not certain that imposing such a standard is practical under the administrative processes used today for state and local law enforcement activities. Third, in this regulation we do not have direct authority to impose such a standard on law enforcement officials or the courts. We would have to impose such a requirements through covered entities, by requiring them to ensure that the law enforcement official had met the relevant standards (e.g., through a documentation requirement). We are concerned that the privacy enhancement gained through such a requirements would not be outweighed by the administrative burdens imposed on covered entities. And impracticality....

We are, however, concerned about permitting disclosure of protected health information pursuant to process without imposing a minimum floor of protection that must be met before such process can issue. We seek comment on whether and how it might be practical to impose such a standard under the legal authority granted in this statute, and on what such a standard might be. Similarly, while we recognize the need to permit some disclosure of protected health information without prior process, we are concerned about such releases, and seek comment on whether the exceptions proposed here are appropriately defined.

[**Note to reviewers: In other places in this preamble where we do not have legislative authority to include in the regulation an Administration policy (typically involving reuse or disclosure of PHI by an entity that is not covered by the regulation), we have noted so in the preamble, to make clear to the Congress what we would like to see in legislation. In particular, we have done this where the Jeffords bill states a policy we support, to ensure that our intentions with respect to that bill are not misconstrued. The Jeffords bill includes some provisions regarding reuse/disclosure of PHI by law enforcement, that we do not have authority to include in the regulation. We seek your input on whether to discuss the following requirements from the Jeffords bill in this section of the preamble: destruction of evidence when its no longer needed, restricting derivative use/disclosure to legitimate law enforcement, and maximum redaction of identifiers when the information will be used in a public forum.]

New definitions:

Law Enforcement Inquiry or Proceeding. The term "law enforcement inquiry or proceeding" means --

(A) an investigation or official proceeding inquiring into a violation of, or failure to comply with, any statute, regulation, rule or order; or

(B) a criminal, civil or administrative proceeding, arising from a violation of, or failure to comply with, any statute, regulation rule or order.

Law Enforcement Official. The term "law enforcement official" means any officer of the United States of or a State or political subdivision thereof, who is empowered by law to conduct--

(A) an investigation or official proceeding inquiring into a violation of, or failure to comply with, any statute, regulation, rule or order; or

(B) a criminal, civil or administrative proceeding, arising from a violation of, or failure to comply with, any statute, regulation, rule or order.

Draft 9/28/99 3:30p

Dear [House / Senate Conferee]:

I am writing to express my deep concerns about the medical privacy language included in H.R. 10, the Financial Services Act of 1999 as passed by the House. We have worked closely with Members of Congress on a bipartisan basis to craft meaningful, comprehensive medical privacy legislation that can help us achieve the goal of so many Americans – the right to privacy for their medical and genetic information. We believe that the language incorporated in H.R. 10 would significantly undermine these efforts and, perhaps more importantly, erode protections that currently exist by codifying an extremely broad array of disclosures that would not require patient consent and limiting recourse of individuals whose privacy has been violated.

The President has indicated his strong desire to see a comprehensive medical privacy bill enacted before August of this year. As he said in his State of the Union Address:

> "As more of our medical records are stored electronically, the threats to all our privacy increase. Because Congress has given me the authority to act if it does not do so by August, one way or another, we can all say to the American people, we will protect the privacy of medical records and we will do it this year."

The medical privacy language incorporated in HR 10 fails to include the most basic protections -- advising consumers in writing of how their information will be used, providing access and amendment rights, limiting the recipient's use of information to only specified purposes, and similarly limiting redisclosure of the information and provide for recourse for consumers whose privacy has been violated.

Passage by the Congress of a hollow medical privacy provision is worse than no law at all. It would lead the American people to think we took steps to strengthen protection of their health information when quite the opposite would be true. Therefore, I strongly urge you follow the motion to instruct conferees and work to strike this language from H.R. 10 in conference.

We are committed to working with members of the House and Senate to enact comprehensive, free-standing medical privacy legislation. Such a bill must inform consumers about the uses of their private medical information and require patient consent to disclose this sensitive information when it is to be used for something other than treatment of that patient or activities related to payment for such services. Legislation also must place strict boundaries around who may receive and use identifiable health information without the subject's consent, it must ensure that patients' consent for use of their information is truly informed and voluntary, and must include strong penalties for violating patients' privacy.

Comprehensive medical privacy legislation incorporating these principals can be enacted this year. We look forward to working with this Congress to reach that goal.

Sincerely,

Donna E. Shalala

Add treasury sentence here.

- Summers sig?
- conf call

Peter P. Swire
09/29/99 09:02:31 AM

Record Type: Record

To: David W. Beier/OVP@OVP
cc: See the distribution list at the bottom of this message
bcc:
Subject: Re: LRM LJM29 - - HEALTH & HUMAN SERVICES Report on S900 Financial Services Modernization Act of 1999

My reaction to the letter was more positive than David's.

(1) The letter shows HHS' clear opposition to the provision, and explains why.

(2) The best response on this issue will be to get the reg out. As long as we keep our reg authority, there will be a major health privacy set of rules pending and the need to handle it in the banking bill will be much diminished.

(3) Suggestion -- add a sentence saying that "I have been working closely on this issue with Secretary Summers and the Treasury Department, and he has asked me to say that he fully supports the views expressed here." Gary Gensler or Greg Baer would be the Treasury contacts for this.

Peter

David W. Beier@OVP

David W. Beier@OVP
09/28/99 06:51:32 PM

Record Type: Record

To: Lisa J. Macecevic/OMB/EOP@EOP
cc: See the distribution list at the bottom of this message
Subject: Re: LRM LJM29 - - HEALTH & HUMAN SERVICES Report on S900 Financial Services Modernization Act of 1999

Does this mean that we should be meeting to discuss once again our posture on this bill relevative privacy? I worry that this weak letter does not present a strong enough unified front between the different Cabinet agencies.

Message Copied To:

Sarah Rosen Wartell
09/29/99 09:07:22 AM

Record Type: Record

To: Peter P. Swire/OMB/EOP@EOP

cc: See the distribution list at the bottom of this message
Subject: Re: LRM LJM29 - - HEALTH & HUMAN SERVICES Report on S900 Financial Services Modernization Act of 1999

I like peter's approach -- might even go one better and ask Secretary Summer to sign the letter. Not sure that he will want to do so. He still doesn't think he can explain what will happen (post HHS regs but before comprehensive legislation) when institutions not covered by HHS regs (e.g. certain life insurers) share medical info with financial institutions. He feels vulnerable when pressed on this issue.

How do we want to proceed? Jennings or OMB -- Do you want to talk to HHS about this approach? If they like it, we can then talk with Treasury. I am happy to set up a conference call for all of us to work this through.

Message Copied To:

david w. beier/ovp@ovp
lisa j. macecevic/omb/eop@eop
christopher c. jennings/opd/eop@eop
devorah r. adler/opd/eop@eop
peter p. swire/omb/eop@eop
lauren b. steinfeld/omb/eop@eop
gaylee l. morgan/omb/eop@eop
diana espinosa/omb/eop@eop
sarah a. bianchi/ovp@ovp
daniel n. mendelson/omb/eop@eop
sally katzen/omb/eop@eop
john e. thompson/omb/eop@eop
david j. haun/omb/eop@eop
derek a. chapin/omb/eop@eop
alice veenstra/omb/eop@eop
michael f. crowley/omb/eop@eop
broderick johnson/who/eop@eop
joel k. wiginton/who/eop@eop
sarah rosen wartell/opd/eop@eop
paul j. weinstein jr./opd/eop@eop
wendy a. taylor/omb/eop@eop
alexander t. hunt/omb/eop@eop
michael deich/omb/eop@eop
robert j. pellicci/omb/eop@eop
douglas pitkin/omb/eop@eop
justice.lrm@usdoj.gov @ inet
llr@do.treas.gov @ inet