Executive Office of the President of the United States

Peter P. Swire
The Chief Counselor for Privacy
Office of Management and Budget
Old Executive Office Building, Room 349
Washington D.C. 20503
(202) 395-1095
(202) 395-3047 (FAX)

FAX TRANSMITTAL

TO: Chris Jennings

Fax: 695597

From: Peter Swire

Date: 06-08-00

Total Number of Pages:

Comments:

GRAMM Bill

Leach Bill

DETERMINED TO BE AN ADMINISTRATIVE MARKING
INITIALS: 2LR DATE: 06/25/12
2012-0463-S

Possible Gramm language

~~Confidential~~ –close hold

Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. 6802) is amended by inserting at the end thereof the following new subsection:

"(f) CONSUMER CONSENT REQUIRED FOR SHARING OF HEALTH INFORMATION AMONG AFFILIATES AND NONAFFILIATES.--

"(1) In deciding whether, or on what terms, to offer, provide, or continue to provide a loan or credit to a consumer, a financial institution shall not obtain or receive individually identifiable health information about the consumer from an affiliate or nonaffiliated third party, or evaluate or otherwise consider any such information, unless the financial institution–

"(A) has clearly and conspicuously requested in writing that the consumer affirmatively consent to such transfer and use of that information with respect to a particular loan or extension of credit; and

"(B) has obtained from the consumer such affirmative consent and such consent has not been withdrawn.

"(2) The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that is described in section 1171(6)(B) of the Social Security Act.

"(3) For purposes of paragraph (1), the term 'writing' means electronic or other form permitted by regulations implementing this provision.

"(4) Any consent provided by the consumer under paragraph (1)(B) that is not in writing shall be confirmed in writing promptly by the financial institution.".

To: Gary, Swine, Baer (Bera-), Ross, Strauss
Leach Bill as introduced
Fr: Marie L.
Hearing next Wed the 14th in HBC

....
(Original Signature of Member)

Leach Bill as introduced

106TH CONGRESS
2D SESSION

H. R. ____

IN THE HOUSE OF REPRESENTATIVES

Mr. LEACH introduced the following bill; which was referred to the Committee on ____________________

A BILL

To strengthen consumers' control over the use and disclosure of their health information by financial institutions, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Medical Financial Privacy Protection Act".

SEC. 2. USE AND DISCLOSURE OF HEALTH INFORMATION BY FINANCIAL INSTITUTIONS.

(a) IN GENERAL.—Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) is amended by inserting after section 502 the following:

"SEC. 502A. SPECIAL RULES FOR HEALTH INFORMATION.

"(a) RULES FOR DISCLOSURE.—

"(1) GENERAL RULE REQUIRING AFFIRMATIVE CONSENT FOR DISCLOSURE.—

"(A) IN GENERAL.—A financial institution may not disclose any individually identifiable health information pertaining to a consumer to an affiliate or a nonaffiliated third party unless the financial institution—

"(i) has provided to the consumer a clear and conspicuous notice in writing, in electronic form, or in another form permitted by the regulations implementing this subtitle, of the categories of such information that may be disclosed and the categories of affiliates or nonaffiliated third parties to whom the financial institution discloses such information;

"(ii) has clearly and conspicuously requested in writing, in electronic form, or in another form permitted by the regulations

implementing this subtitle, that the consumer affirmatively consent to such disclosure; and

"(iii) has obtained from the consumer such affirmative consent and such consent has not been withdrawn.

"(B) WITHDRAWAL OF CONSENT.—Any withdrawal of consent is subject to the rights of any financial institution that acted in reliance on the consent prior to its withdrawal.

"(2) DISCLOSURE OF INFORMATION ABOUT PERSONAL SPENDING HABITS.—

"(A) IN GENERAL.—If a financial institution provides a service to a consumer through which the consumer makes or receives payments or transfers by check, debit card, credit card, or other similar instrument, the financial institution may not disclose any information described in subparagraph (B) pertaining to the consumer to an affiliate or a nonaffiliated third party unless the financial institution has satisfied the requirements of clauses (i), (ii), and (iii) of paragraph (1)(A) with respect to the disclosure.

"(B) INFORMATION DESCRIBED.—The information described in this paragraph is—

"(i) an individualized list of a consumer's transactions or an individualized description of a consumer's interests, preferences, or other characteristics; or

"(ii) any such list or description constructed in response to an inquiry about a specific, named individual;

if the list or description is derived from individually identifiable health information collected in the course of providing a service described in subparagraph (A) to the consumer.

"(3) DISCLOSURE OF AGGREGATE LISTS.—A financial institution may not disclose any aggregate list of consumers containing or derived from individually identifiable health information to an affiliate or a nonaffiliated third party unless the financial institution has satisfied, for each consumer on the list, the requirements of clauses (i), (ii), and (iii) of paragraph (1)(A) with respect to the disclosure.

"(4) EXCEPTIONS TO DISCLOSURE LIMITATIONS.—This section shall not restrict a financial institution from disclosing individually identifiable health information—

"(A) for a purpose described in paragraph (1), (2), (3), (5), (7), or (8) of section 502(e);

"(B) in order to facilitate customer service, such as maintenance and operation of consolidated customer call centers or the use of consolidated customer account statements; or

"(C) to the institution's attorneys, accountants, and auditors.

"(5) LIMITS ON REDISCLOSURE AND REUSE OF INFORMATION.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), an affiliate or a nonaffiliated third party that receives individually identifiable health information from a financial institution under this section shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the financial institution.

"(B) DISCLOSURE UNDER AN EXCEPTION.—Notwithstanding subparagraph (A), any person that receives individually identifiable health information from a financial institution in accordance with one of the exceptions in paragraph (4) may use or disclose such information only—

"(i) as permitted under that exception; or

"(ii) under another exception in such paragraph to carry out the purpose for which the information was disclosed by the financial institution.

"(6) CONSTRUCTION.—Except as provided in paragraph (4)(A), this section applies in lieu of subsections (b), (c), and (e) of section 502 to a disclosure by a financial institution of individually identifiable health information.

"(b) RULES FOR RECEIPT AND USE.—

"(1) IN GENERAL.—In deciding whether, or on what terms, to offer, provide, or continue to provide a loan or credit to a consumer, a financial institution shall not request to receive individually identifiable health information about the consumer from an affiliate or nonaffiliated third party, or use, evaluate, or otherwise consider any such information, unless the financial institution—

"(A) has clearly and conspicuously requested in writing, in electronic form, or in another form permitted by the regulations implementing this subtitle, that the consumer affirmatively consent to such receipt and use; and

"(B) has obtained from the consumer such affirmative consent and such consent has not been withdrawn.

"(2) RESTRAINT ON INFORMATION REQUESTS.—In deciding whether, or on what terms, to offer, provide, or continue to provide a loan or credit to a consumer, a financial institution shall not request the consent described in paragraph (1)(A) to receive individually identifiable health information available from an affiliate, if the financial institution would not otherwise normally receive the same or substantially similar information from a nonaffiliated third party if that third party were the only person able to provide the information.

"(c) CONSUMER RIGHTS TO ACCESS AND CORRECT INFORMATION.—

"(1) ACCESS.—

"(A) IN GENERAL.—Upon the request of a consumer, a financial institution shall make available to the consumer individually identifiable health information about the consumer that is within the possession of the financial institution.

"(B) EXCEPTIONS.—Notwithstanding subparagraph (A), a financial institution—

"(i) shall not be required to disclose to a consumer any confidential commercial information, such as an algorithm used to derive credit scores or other risk scores or predictors;

"(ii) shall not be required to create new records in order to comply with the consumer's request;

"(iii) shall not be required to disclose to a consumer any information assembled by the financial institution, in a particular matter, as part of the financial institution's efforts to comply with laws preventing fraud, money laundering, or other unlawful conduct; and

"(iv) shall not disclose any information required to be kept confidential by any other Federal law.

"(2) CORRECTION.—

"(A) OPPORTUNITY TO DISPUTE.—A financial institution shall provide a consumer the opportunity to dispute the accuracy of any individually identifiable health information disclosed to the consumer pursuant to paragraph (1), and to present evidence thereon.

"(B) AMENDMENT, CORRECTION, OR DELETION.—A financial institution—

"(i) shall amend, correct, or delete material information identified by a consumer that is materially incomplete or inaccurate; or

"(ii) shall notify the consumer of—

"(I) its refusal to make such amendment, correction, deletion;

"(II) the reasons for the refusal; and

"(III) the identity of the person who created the information and shall refer the consumer to that person for purposes of amending or correcting the information or filing with it a concise statement of what the consumer believes to be the correct information.

"(3) COORDINATION AND CONSULTATION.—In prescribing regulations implementing this subsection, the Federal agencies specified in section 504(a) shall consult with one another to ensure that the regulations—

"(A) impose consistent requirements on the financial institutions under their respective jurisdictions;

"(B) take into account conditions under which financial institutions do business both in the United States and in other countries; and

"(C) are consistent with the principle of technology neutrality.

"(4) CHARGES FOR DISCLOSURES.—A financial institution may impose a reasonable charge for making a disclosure under this subsection, which charge shall be disclosed to the consumer before making the disclosure.

"(d) SPECIAL REQUIREMENT TO PROTECT MENTAL HEALTH INFORMATION.—In any case in which this section requires a person to obtain a consumer's affirmative consent to a receipt, use, or disclosure of individually identifiable health information, the person shall obtain a separate and specific consent with respect to any information pertaining to the mental health or mental condition of an individual.

"(e) RELATIONSHIP TO OTHER LAWS.—Nothing in this section shall be construed as—

"(1) modifying, limiting, or superseding standards promulgated by the Secretary of Health and Human Services under—

"(A) part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.); or

"(B) section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191; 110 Stat. 2033); or

"(2) authorizing the use or disclosure of individually identifiable health information in a manner other than as permitted by other applicable law.".

(b) DEFINITION OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.—Section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809) is amended by adding at the end the following:

"(12) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.—The term 'individually identifiable health information' means any information, including demographic information obtained from or about an individual, that is described in section 1171(6)(B) of the Social Security Act (42 U.S.C. 1320d(6)(B)).".

(c) CLERICAL AMENDMENT.—The table of contents for the Gramm-Leach-Bliley Act is amended by inserting after the item relating to section 502 the following:

"Sec. 502A. Special rules for health information.".

SEC. 3. REGULATIONS; EFFECTIVE DATE.

(a) REGULATIONS.—

(1) REGULATORY AUTHORITY.—Section 504(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6804(a)) shall apply to the issuance of regulations to carry out the amendments made by this Act in the same manner as such section applies to the issuance of other regulations to carry out subtitle A of title V of the Gramm-Leach-Bliley Act, except as provided in paragraph (4).

(2) AUTHORITY TO GRANT EXCEPTIONS.—The regulations issued to carry out the amendments made by this Act may include such additional exceptions to the provisions of section 502A of the Gramm-Leach-Bliley Act, as inserted by section 2, as are deemed consistent with the purposes of subtitle A of title V of such Act, except as provided in paragraph (3)(B).

(3) SPECIAL PROTECTIONS FOR MENTAL HEALTH INFORMATION.—

(A) IN GENERAL.—The regulations issued to carry out the amendments made by this Act shall, where appropriate, include special policies and procedures to protect the confidentiality of individually identifiable health information re-

lating to the mental health or mental condition of an individual.

(B) AUTHORITY TO GRANT EXCEPTIONS.—The regulations issued to carry out the amendments made by this Act may not include any exception to the provisions of section 502A of the Gramm-Leach-Bliley Act, as inserted by section 2, that diminishes the protection afforded by such section to the confidentiality of individually identifiable health information relating to the mental health or mental condition of an individual.

(4) DEADLINE.—Regulations to carry out the amendments made by this Act shall be issued in final form not later than 6 months after the date of the enactment of this Act.

(b) EFFECTIVE DATE.—The amendments made by this Act shall take effect 6 months after the date on which regulations are required to be issued under subsection (a)(4), except to the extent that a later date is specified in such regulations.

TOTAL P.15

DEPARTMENT OF HEALTH AND HUMAN SERVICES
ASSISTANT SECRETARY FOR PLANNING AND EVALUATION
OFFICE OF HEALTH POLICY

PHONE: (202) 690-6870 FAX: (202) 401-7321

Date: 4/18/00

From: Gary Claxton

To: Chris Jennings

Phone: (202) 690-
(202) 690-6870
FAX: (202) 401-7321

Phone:

Fax:

Number of Pages (Including Cover): 2

Comments:

fax to Chris Jennings & Peter Swire

BNA Daily Report for Executives
No. 75
Tuesday April 18, 2000 Page C-1

Analysis & Perspective

Health Care
HHS Rule Protecting Health Care Privacy
Irks Some Employers, Likely to Affect Many

A proposed rule issued by the Department of Health and Human Services on privacy of medical information does not directly impose obligations and requirements on employers, yet benefit specialists interviewed by BNA and comment letters received by HHS suggest the regulations are likely to have a dramatic effect on how many companies operate.

The proposed rule, issued in October of last year, seeks to protect electronically maintained health data from misuse by regulating disclosures of patient health information. It would prohibit disclosure of medical information for purposes other than health care transactions unless authorized by patients, allow patients to know who is using their health information and how it is being used, require individuals who possess information to safeguard it from inappropriate use or disclosure and hold those who use information accountable for handling of this information, and provide legal recourse to persons harmed by the misuse of their information.

As required by the Health Insurance Portability and Accountability Act, the HHS regulation is being drafted because Congress has not passed comprehensive legislation to protect privacy of health data. The rule applies only to electronically transmitted health information, but many comments on the proposal recommended expanding the scope to paper records.

The proposed rule "will affect employers tremendously," Kirk Nahra, a partner with the law firm Wiley, Rein & Fielding, in Washington, D.C., told BNA April 5.

The proposed rule will make it more difficult for employers to gain access to employee medical information, will require the rewriting of health insurance contracts, and could have an effect on health care costs, Nahra said.

Nahra pointed out that the proposed rule does not directly refer to any requirement placed on employers. "That's sort of odd," Nahra commented, adding that HHS likely will focus on the rule's effect on businesses in

its revisions of the proposal.

Clarity Sought on Employer Obligations

Joanne Hustead, director of legal and public policy at the National Partnership for Women and Families, told BNA that HHS failed to address the major issue of employers' access to their employees' medical information. "They missed a really great opportunity in the regs to make it clear what obligations employers have," she said.

Medical information privacy is a major concern of employees, Hustead said. "People are extremely concerned about what employers know and what they do with that information," she said. For example, she said, an employer could use a worker's medical records as the basis for denying him a promotion.

When asked if she thought HHS would revisit the issues surrounding employers in a final rule, Hustead replied, "I certainly hope so."

Julia Bellinger, manager of tax benefits legislation and regulation at the Society for Human Resource Management, expressed regret that the rule is somewhat inconsistent and vague in terms of employer requirements. "If it was more specific at least we'd know where we stand," she said, adding that SHRM members "don't quite know what they're supposed to do."

Effect on Employers

According to attorneys Dorthula H. Powell-Woodson and Serena G. Simons, members with the law firm Miller & Chevalier, in Washington, D.C., employers are covered by the proposed regulations if they sponsor an insured or self-insured health plan that covers at least 50 participants or has a third-party administrator, operate an on-site health clinic, or engage in information processing that includes a health care services component.

"Every company with a health plan or with an on-site health facility will be affected," Simons told BNA.

The regulations impose several fundamental changes, according to the attorneys. They require limited disclosure of protected health information (PHI), so that people within the organization receive only the amount necessary to accomplish their functions. Business partners, such as third-party administrators, HMOs, or PPOs, also are required to use PHI in the same manner, and the company may be liable if the third party fails to

follow the regulations. Finally, the regulations require the development and implementation of policies and procedures that provide notice to individuals regarding the uses and disclosures of PHI and how individuals may exercise their rights.

As for what the regulations will mean to employers, Powell-Woodson and Simons listed the following potential employer requirements:

tracking why, what, and to whom PHI is released;

reconfiguring information systems for health plan or health care personnel to have access only to the information necessary to do their jobs and creating communication barriers between health plan provider and non-health plan provider components;

policing business partners for compliance with regulations;

hiring or designating staff to develop, implement, and enforce the necessary policies and procedures; and

training employees on the appropriate uses and disclosures of PHI.

"It's going to potentially change the dynamic of many employer programs that are in place," Simons said of the rule. She noted that under the rule, an employer's HR department, if it administers the company health plan, would be covered by the requirements while the rest of the organization would not. "They take sort of a component approach," Simons said.

According to information provided by Miller & Chevalier, civil monetary penalties for failure to comply with the regulations are up to $25,000 per year. Criminal liabilities can include $250,000 fines and 10 years in jail.

Fraud Prevention, Wellness Plans

HHS received more than 40,000 paper comment letters and 10,000 e-mail messages on the rule. Employer comments expressed various reservations about the rule, including a concern that the rule potentially could prohibit fraud prevention activities, such as the review of claims charged against group medical plans to ensure they are filed by eligible employees and dependents.

The U.S. Chamber of Commerce, in its comments, wrote that while HHS's efforts to protect the privacy of individuals' medical information are commendable, "we believe there are certain provisions that present serious issues for employers." For one thing, it said, "it is unclear the extent to which employers may be covered by the rule."

The chamber expressed fear that the rule would limit activities of employers that run health improvement and well-being programs for their employees. "[T]he Department's final rule should make clear that an employer's operation of these types of programs does not trigger the authorization requirements of the rule," the chamber wrote.

Another concern of the chamber was the proposal's effect on integrated benefits programs. "Many employers are moving toward integrated systems to provide health care, workers' compensation, and disability coverage to their employees," the chamber wrote. The proposed rule would raise obstacles to this kind of plan, such as forcing an employer to obtain separate consent forms if it wanted to use information from its health plan to administer its disability plan.

Employers seeking to review the quality of their health care plans also could butt up against the HHS rule, the chamber wrote. It noted that certain evaluations could be stymied by the inability to get access to protected medical records.

LPA Inc., an employer advocacy organization, stated in its comments that its "concern centers on the broad definition of 'health information.' " LPA wrote that the definition arguably is broad enough to include data compiled through mandatory drug testing programs, data compiled from fitness for duty tests in accordance with the Americans with Disabilities Act, and medical information provided by an employee as a condition of taking leave under the Family and Medical Leave Act. "LPA believes that the final regulations should clearly exempt these uses from their scope, both for compelling public policy reasons and because they are adequately regulated by existing employment laws," the association said.

Liability for Business Partners

The National Employee Benefits Institute, a foundation serving the employee benefits interests of large employers, argued that "subjecting plans to vicarious liability for the errors of a business partner with respect to the use and disclosure of protected health information ... would unfairly penalize a plan for conduct that is outside of its

control." Furthermore, NEBI said, the proposal provides no guidance "as to whether business partner relationships would be deemed by HHS to exist within different divisions of the same employer, and if so, how such relationships should be addressed with respect to the use and disclosure of protected health information."

The National Association of Manufacturers asserted that it is "particularly concerned" about potential litigation arising out of the regulations. "The further involvement of the trial bar in our beleaguered health care system will inevitably lead to higher costs, reduced benefits and fewer covered individuals," NAM wrote.

Federal Express Corp. wrote that the onerous nature of the rule could have the effect of making some companies discontinue their health care plans. "We are especially concerned that the combined effect of burdensome, expensive privacy regulations and overly protective patient's rights legislation will cause many self-insured employers to throw up their hands over excessive regulation of voluntarily provided benefits and discontinue offering health coverage under the provisions of ERISA," it wrote.

The National Partnership for Women and Families wrote that HHS "needs to clarify the responsibilities of employers that sponsor health plans for their employees ...." The partnership recommended that the rules make clear that while employers "in their entirety are not covered entities, the component of the employer that sponsors an ERISA-covered plan (the 'health care component') is a covered entity."

Comments showed that privacy advocates generally are in favor of the rule and are urging HHS to strengthen the individual rights provisions.

Privacy Rule Timeline, Background

Section 264 of the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), enacted Aug. 21, 1996, required that if legislation establishing privacy rights were not enacted by Aug. 21, 1999, the secretary of health and human services would promulgate final regulations containing standards by Feb. 21, 2000. Congress missed the deadline.

The proposed rules were released Oct. 29, 1999, and published in the Federal Register Nov. 3 (64 Fed. Reg. 59917). The original comment

deadline for the regulations was Jan. 3. HHS later extended that deadline until Feb. 17.

Groups that would be covered under the rule include health care providers who transmit health information electronically, health plans, health care clearinghouses, and their business partners.

By Simon J. Nadel

American Psychiatric Association
1400 K Street, NW
Washington, DC 20005

Division of Government Relations
Telephone: (202) 682-6060
DGR Fax : (202) 682-6287

FAX COVER

TO: Chris Jennings

FAX: 202-456-5557

FROM: Will Bruno

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

Number of pages transmitted including cover 7 **Date:** 12/3/99 **Time:** 9:20

Message

American Psychiatric Association

1400 K Street, N.W.
Washington, D.C. 20005
Telephone 202.682.6000
Fax 202.682.6850
E-mail apa@psych.org
Internet www.psych.org

November 29, 1999

U.S. Department of Health and Human Services
Assistant Secretary for Planning and Evaluation
Attention: Privacy-P
Room G-322A
Hubert H. Humphrey Building
200 Independence Avenue Avenue, SW
Washington, D.C. 20201

Re: APA Preliminary Comments

Dear Assistant Secretary Hamburg:

The American Psychiatric Association on behalf of more than 40,000 psychiatrists nationwide believe President Clinton's privacy proposal is a valuable first step toward protecting patient privacy. Before these recommendations are finalized, additional protections are critically needed to protect patient privacy and to promote high quality health care. As physicians we believe patients and our own families deserve stronger protections.

It is often overlooked that confidentiality is an essential element of high quality health care. Some patients refrain from seeking medical care or drop out of treatment in order to avoid any risk of disclosure of their records. And some patients simply will not provide the full information necessary for successful treatment. Patient privacy is particularly critical in ensuring high quality mental health care.

We urge the Administration to take these additional steps, and we will also be asking Congress to implement more comprehensive legislation.

1) Patients should be able to choose who will see their medical records. Under the Administration's proposal, patient consent is not required for disclosure of medical records for treatment, payment, and broadly defined business "operations" purposes. This represents a significant change not only to the historic patient doctor treatment relationship but also an impediment to physicians' efforts to provide the best possible medical care. In some areas patients may lose some privacy protections currently used by hospitals and physicians. We need to take steps to ensure that doctor-patient confidentiality is preserved and strengthened.

Regrettably, the Administration proposal does not recognize that these regulations will change current practice and provides a de facto federal good housekeeping seal of approval to practices which undermine privacy. Patient consent before use and disclosure of records is almost always required today. We should be strengthening patients' rights rather than missing this key opportunity to achieve meaningful patient privacy.

For example, the Administration's proposal would allow a doctor to examine the records of patients the doctor is not even treating. In this way the privacy of any other patient "with similar conditions" or those "in the same family or living in the same household" could be violated. The doctor could review literally thousands of patient records without patient consent. In addition, no notice to the patient that the record has been reviewed is provided and no particular safeguard to prevent any health care provider from abusing this authority is established.

Another concern is that HMOs and providers who wish to provide a higher level of protections are actually prohibited from doing so under the regulations. "A covered entity would be prohibited from soliciting an authorization from an individual for treatment payment, and health operations unless such an authorization is required by other applicable law."

The proposed regulations set no real limits on the demands of payers for access to patients' medical information, which often amount to requests for entire patient records. These excessive demands routinely include information for which there is no legitimate need for payments purposes. Significantly narrower definitions of the information that may be released for payment purposes is needed to protect patient privacy.

We believe that workable approaches to obtaining patient consent for release of medical record information are available and can be implemented without disruption to the health care system. Thus, the critical principle of patient consent need not be sacrificed for fears of reduced efficiency. APA would be happy to discuss these ideas in greater detail with you.

2) Even if you accept the Clinton Administration's general approach of no informed consent before disclosure of the record for health purposes, patients will lose some existing privacy protections. Patients will lose additional existing privacy protections because of provisions governing disclosure outside the health care system. Hospitals' and doctors' current practice requiring patient consent before disclosure will change as

a result of the regulation. Patients' ability to choose when their medical records information is disclosed *outside* the health system will be reduced.

For example, under current law when hospitals or doctors receive a request for a medical record from an attorney for civil and administrative purposes they will generally not disclose medical records information without the patient's consent. But the new regulation would allow providers to disclose medical records information to attorneys who write a letter "certifying that the ...information requested concerns a litigant to the proceeding and that the health condition of such litigant is at issue." These procedures provide no check on attorneys' behavior in requesting records of marginal or no relevance to a case, for the purpose of embarrassing or intimidating opposing parties. Once the information is disclosed, the damage is done; post hoc remedies cannot restore parties' privacy.

The same loss of patient consent is likely to occur as a result of provisions allowing disclosures to "governmental health data systems." The prospect of huge government data banks filled with confidential, identifiable medical information is justifiably threatening to most citizens. We believe that substantial new privacy protections need to be applied in this area.

3) Additional protections for mental health and other particularly sensitive medical records information are critical. For example, with reference to mental health treatment, the Clinton proposal allows patients' highly personal information about their functioning in a social and professional context discovered in the course of treatment to be disclosed without their consent.

The U.S. Supreme Court recognized the special status of mental health information in its 1996 *Jaffee v. Redmond* decision and ruled that additional protections are essential for effective psychiatric treatment. The Court held that "Effective psychotherapy depends upon an atmosphere of confidence and trust.... For this reason *the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment,"* (emphasis added).

APA believes that for treatment and "operations purposes" the proposed rule allows for the use and disclosure of far too much information without the patient's consent. We also believe that language needs to be added to clarify that the amendment's privacy protections cover treatment modalities broader than psychotherapy and also cover information that is part of the patient's medical record. Finally, we believe a potential loophole needs to be closed in the explanatory text suggesting that *any* information in the "medical record" or that is needed for treatment, payment, and

health care operations can be used and disclosed without patient consent. Certainly, it is not the intention of the Administration to include such an expansive loophole in this provision that is critically important for effective medical care.

4) Additional protections are needed to prevent employer access to workers' medical records. Nobody wants his or her supervisor to be able to peruse their most personal medical information.

Particularly important is adding specific prohibitions on access by supervisory personnel to records, extending the scope of the regulations' protections to all employers, and providing privacy protections for the information contained in workman's compensation records. To the extent that the Administration believes it does not have authority under Health Insurance Portability and Accountability Act (HIPAA) for these purposes we urge you to send separate legislation to Capitol Hill to achieve these purposes.

5) We also want all Americans to be free from unreasonable police access to their most personal medical record information. The Administration's proposal falls short in this area.

We believe that the same constitutional protections (a Fourth Amendment probable cause standard) should apply to a persons' medical history as it would to the possessions in their homes and that additional limits should be placed on access to medical records for "identification" purposes.

6) We are concerned by the ease with which states ostensibly will be able to win approval of their requests that certain state laws less protective of privacy be retained.

If states are allowed to retain their weak privacy laws too easily citizens in these states would not benefit from the higher level of privacy protection in the federal privacy law. We also believe that members of the public and affected parties should be able to comment upon such states' requests for determinations and advisory opinions relating to retaining state laws less protective of privacy. The regulations should require full consideration of privacy considerations including the possibility that the quality of patient care or patient access to care will suffer as a result of the retention of state law.

We are particularly concerned by a provisions which would allow a new basis for states to avoid the higher level of patient protections contained in the federal law in cases where the less privacy protective state law is needed for "the efficiency and

cases where the less privacy protective state law is needed for "the efficiency and effectiveness of the health care system." The other exceptions in the regulations to federal floor preemption are based on the requirements of HIPAA, but this last extremely broad phrase is not required by HIPAA and is so vague that it would allow virtually any state law less protective of privacy to be retained. This contradicts the basic premise of floor preemption contained in HIPAA.

7) We are also very concerned by the gaps in privacy protections for medical records information contained in the recently passed financial services modernization law. Specifically, we believe that that the consent of the patient should be required before medical records information is shared among entities, particularly for purposes such as making loan determinations.

While we are encouraged that these regulations prohibit many harmful uses and disclosures allowable under the new financial services modernization law, we believe strong prohibitions in this area should be implemented as soon as possible. In particular we urge you to issue final regulations limited to prohibiting this type of information sharing which would take effect in the early winter of 2000.

8) We welcome the many very positive provisions contained in the Administration proposal and urge that they be retained including:

- non-preemption of more privacy protective state laws
- the requirement the entire medical record not be used in cases where a portion of the record will suffice, i.e. the "minimum amount necessary" requirement
- the requirement that an entity's notice of confidentiality requirements be provided to patients at least every three years
- the inclusion of some increased limitation on law enforcement access to medical records
- the opportunity for patients to request additional privacy protections
- extension, in many circumstances, of federal "common rule" research protections to privately funded research
- restrictions on the sale of medical record information
- restrictions on use for marketing purposes, fundraising, health plan enrollment decisions and employment decisions

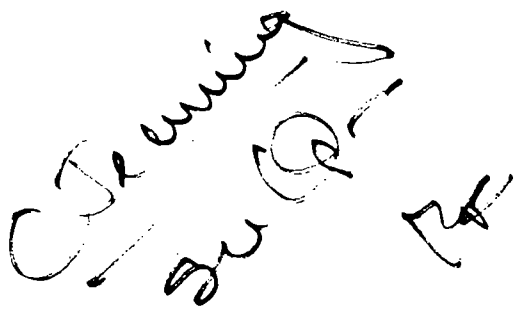
Thank you for considering our views, and we look forward to discussing them with you further. Please feel free to contact me or William Bruno, Associate Director of Government Relations at (202) 682-6060.

Sincerely,

Jay B. Cutler
Special Counsel and Director,
Division of Government Relations
American Psychiatric Association

Cc: Chris Jennings
Peter Swire
Gary Claxton
Lisa Rovin

10-31-99



Copied
Jennings
Podesta

10-31-99

RULES ON PRIVACY OF PATIENT DATA STIR HOT DEBATE

HEALTH GROUPS OBJECT

Clinton's Plan Is Criticized as Costly and Inadequate for Protecting Records

A1

By ROBERT PEAR

WASHINGTON, Oct. 29 — President Clinton kicked off an intense debate today on how to protect the privacy of medical records in an era when doctors can test their patients for genetic defects and send the information around the world with the click of a computer mouse.

In unveiling new rules to safeguard such information, Mr. Clinton said, "These standards represent an unprecedented step toward putting Americans back in control of their own medical records."

But doctors said the rules were inadequate and could actually erode some protections that patients now have. Several physician groups said they had been invited to today's White House ceremony, but stayed away because in many cases the proposal does not require that patients give consent before their records are shared, only that they be notified. Such a rule, they said, does not give patients enough control over the use and disclosure of their medical records.

The Administration estimated that compliance would cost the health-care industry $3.8 billion over five years, but the insurance industry says the costs could be 10 times that amount. With both sides saying they support the goals of the standards, a central point in the debate will be: What is privacy worth in dollars and cents?

Health insurance plans object, in particular, to a provision that would make them responsible for privacy lapses by companies that collaborate in the care of a patient. For example, an H.M.O. that sends a patient to a pharmacy could be liable if the pharmacy improperly uses the patient's records.

Under the proposed rules, patients would gain a new Federal right to inspect, copy and suggest corrections in medical records that have been kept or transmitted electronically.

Federal officials estimated that it would cost doctors, hospitals and health maintenance organizations more than $400 million to issue notices informing patients of their privacy rights, as required by the rules. In addition, the officials predicted, thousands of patients will try to correct their medical records, and it will cost the health-care industry more than $2 billion to deal with these requests over the next five years.

The rules would permit the use and disclosure of medical information without a patient's consent for treatment, payment and a wide range of loosely defined "health-care operations," including many common business practices of H.M.O.'s.

Dr. Donald J. Palmisano, a trustee of the American Medical Association, said, "The A.M.A. believes that mere notice of a health plan's intended use is inadequate."

Many doctors contend that health plans and insurance companies should have to obtain consent from patients before using information from their files to monitor the patients' compliance with recommendations for medical treatment and testing. Too often, the doctors say, H.M.O.'s interfere in the doctor-patient relationship by suggesting a cheaper drug or a different course of treatment.

The Clinton Administration would allow health plans to use personal health information, without a patient's consent, for the following "health-care operations": assessing the quality of care and the performance of doctors and nurses; developing clinical guidelines; setting premiums for the renewal of insurance contracts, and investigating fraud.

Dr. Richard K. Harding, vice president of the American Psychiatric Association, said the proposed rules "give the Federal Good Housekeeping Seal of Approval to practices that could undermine privacy."

Many states allow patients to limit the use of some or all of the information in their medical files. In theory, the Federal rules do not override state laws that provide more protection for privacy.

But William B. Bruno, a lawyer for the psychiatric association, said, "Patients could lose some protections they now have. At present — because of state laws, court decisions and canons of medical ethics — many hospitals will not disclose medical records unless the patient gives consent. The Federal Government is now weighing in, saying that's not required. It's giving a green light for significant changes in current practice."

Administration officials insisted that the rules would create protections in areas where none now exist. Doctors, hospitals and H.M.O.'s would, for example, have to keep logs documenting who got access to patients' records for various purposes.

The rules would greatly expand the role of the Federal Government in regulating the practices of the health-care industry. It would set hundreds of detailed Federal standards, with civil and criminal penalties for violations.

Mary Nell Lehnhard, senior vice president of the Blue Cross and Blue Shield Association, described the rules as costly, complex and confusing.

"We believe that all patients should have the peace of mind that comes from knowing their personal records are secure, and we are outraged when breaches of this trust occur," Ms. Lehnhard said. "But why do we need 600 pages of regulations to protect medical records when the Bill of Rights takes only one page to provide Americans with all their basic rights? Why didn't the Administration just simply spell out what activities are illegal?"

Janlori Goldman, director of the health privacy project at Georgetown University, said, "This is a historic day. These regulations will be the first enforceable Federal rules protecting health privacy."

But, Ms. Goldman said, the proposal falls short because "there is no requirement that a judge or a magistrate approve or deny access to medical records sought by law enforcement agencies."

Under the rules, most health-care providers would have to designate "privacy officials" to develop privacy policies and procedures. This rule would apply even to a small office with three doctors, who could designate the office manager as privacy coordinator. Providers would also have to designate a "contact person" to handle patients' complaints about violations of privacy.

Mr. Clinton and Donna E. Shalala, the Secretary of Health and Human Services, expansively interpreted their authority. The rules make doctors, H.M.O.'s and insurance compa-

Copied
Jennings
Podesta

The New York Times
SATURDAY, OCTOBER 30, 1999

1/2

Associated Press

President Clinton offered rules yesterday that he said would put "Americans back in control of their own medical records." He also met with the health secretary, Donna E. Shalala, at the White House.

nies responsible for any violation of a patient's privacy by their "business partners."

Kristin A. Bass, director of legislative affairs at the American Association of Health Plans, a trade group, said that an H.M.O. would have little power over a drug store that improperly sold information about the patient to a drug manufacturer.

"They would hold us responsible for the pharmacy's misbehavior," Ms. Bass said.

Insurance plans could also be held accountable for the misuse of medical records by their other "business partners," including lawyers, auditors, billing firms and consultants.

Under the rules, health-care providers and health plans would have to get a patient's consent for certain types of disclosures — if, for example, the information was to be used in marketing.

Doctors and insurers could not insist that people surrender their privacy rights as a condition of obtaining treatment or insurance. In other words, they could not coerce patients into giving consent.

The Administration acknowledged that the rules would create substantial costs for health-care providers and health plans. But, it said, the rules are necessary because computer technology makes it possible to "breach the security and privacy of health information on a scale that was previously inconceivable."

In addition, doctors have many new clues to their patients' destiny. Scientists have developed more than 450 genetic tests that may help identify people with an increased risk of developing breast cancer, prostate cancer and other diseases.

In a preface to the rules, the Administration said they would have "major social benefits" that could not be quantified. Privacy concerns now discourage people from being tested for certain types of cancer and for some sexually transmitted diseases, the Administration said. The new rules will allay these concerns, so more people will receive effective treatments, it said.

A person who violated the rules could be required to pay a civil penalty of $25,000. The rules authorize tougher penalties for criminal violations: a $50,000 fine and one year in prison for willful violations; a $250,000 fine and 10 years in prison if the offender tried to use or sell data for "commercial advantage, personal gain or malicious harm."

The public will have two months to comment on the proposals, which are to be published in the Federal Register on Nov. 3. The Secretary of Health and Human Services is supposed to issue final rules, with the force of law, by Feb. 21, 2000.

Mr. Clinton said he was acting because Congress failed to meet its goal of adopting comprehensive privacy standards by Aug. 21.

"I am taking this action today because Congress has failed to act and because, a few years ago, Congress explicitly gave me the authority to step in if they were unable to deal with this issue," he said.

The New York Times

SATURDAY, OCTOBER 30, 1999

2/2

Outline: Proposed Standards for Privacy of Individually Identifiable Health Information

Statutory Requirement

Section 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, enacted August 21, 1996, requires that, if legislation establishing privacy standards is not enacted "by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act."

The statutory deadline for Congress to enact legislation was August 21, 1999. Absent legislation, HHS has developed its proposed rule.

Overview

The proposed rule would:

- allow health information to be used and shared easily for the treatment and for payment of health care;
- allow health information to be disclosed without an individual's authorization for certain national priority purposes (such as research, public health and oversight), but only under defined circumstances;
- require written authorization for use and disclosure of health information for other purposes, and
- create a set of fair information practices to inform people of how their information is used and disclosed, ensure that they have access to information about them, and require health plans and providers to maintain administrative and physical safeguards to protect the confidentiality of health information and protect against unauthorized access.

Scope

a. Entities covered by the proposed rule

- Health care providers who transmit health information electronically
- Health plans
- Health care clearinghouses

b. Health information covered by the proposed rule ("Protected health information")

- Protection would start when information becomes electronic, and would stay with the information as long as the information is in the hands of a covered entity.
  - -- Information becomes electronic either by being sent electronically as one of the specified Administrative Simplification transactions or by being maintained in a computer system.

-- The paper progeny of electronic information is covered; the information would not lose its protections simply because it is printed out of the computer.

HIPAA protects the information itself, not the record in which the information appears.

- The information must be "identifiable." If the information has any components that could be used to identify the subject, it would be covered.

General rules

We propose that covered entities be prohibited from using or disclosing health information except: as authorized by the patient, or as explicitly permitted by the regulation. The regulation would permit use and disclosure of health information without authorization for purposes of health care treatment, payment and operations, and for specified national policy activities under conditions tailored for each type of such permitted use or disclosure.

- The amount of information to be used or disclosed would be restricted to the minimum amount necessary to accomplish the relevant purpose, taking into consideration practical and technological limitations.
  -- There would be exceptions for situations in which assessment of what is minimally necessary is appropriately made by someone other than the covered entity (e.g., such as when an individual authorizes a use or disclosure of information, or when the disclosure is mandatory under another law).
  -- We would allow covered entities to rely on requests by certain public agencies in determining the minimum necessary information for certain disclosures.

  Under the principle of minimum necessary use, if an entity consists of several different components, the entity would be required to create barriers between components so that information is not used or shared inappropriately.

- To encourage covered entities to strip identifiers from health information when it is possible to do so, we would permitted a covered entity to use and disclose such de-identified information in any way, provided that:
  – it does not disclose the key or other mechanism that would enable the information to be re-identified, and
  -- it has no reason to believe that such use or disclosure will result in the use or disclosure of protected health information (e.g., because the recipient has the means to re-identify the information).

  We would treat the key to coded identifiers the same as the information to which it pertains. A covered entity could use or disclose a key only as it could use or disclose the underlying information.

- We would permit covered entities to disclose protected health information to persons they hire to perform functions on their behalf, where such information is needed for that function. These 'business partners" would include contractors such as lawyers, auditors, consultants, health care clearinghouses, and billing firms, but not members of the covered entity's workforce.

- Except where the business partner is providing a treatment consultation or referral, we would require covered entities to enter into contracts with their business partners and would require the contracts to include terms to ensure that the protected health information disclosed to a business partner remains confidential. Business partners would not be permitted to use or disclose protected health information in ways that would not be permitted of the covered entity itself. We use the contract as a tool for protecting information, because the HIPAA does not provide legislative authority for the rule to reach many such business partners directly.

- The uses and disclosures permitted by this rule would be exactly that -- permitted, not required. For disclosures not compelled by other law, providers and payers would be free to disclose or not, according to their own policies and principles. At the same time, nothing in this rule would provide authority for a covered entity to refuse to make a disclosure mandated by other law.

- Only two disclosures would be required by this proposed rule: disclosure to the subject individual pursuant to the individual's request to inspect and copy health information about him or her, and certain disclosures for the purposes of enforcing the rule.

- Health information covered by the proposed rule generally would remain protected for two years after the death of the subject of the information, subject to certain exceptions.

Disclosures without authorization for health care treatment, payment, and operations

- Covered entities could use and disclose protected health information without authorization for treatment, payment and health care operations. This would include purposes such as quality assurance, utilization review, credentialing, and other activities that are part of ensuring appropriate treatment and payment.

- Individuals generally could ask a covered entity to restrict further use and disclosure of protected health information for treatment, payment, or health care operations, with the exception of uses or disclosures required by law. The covered entity would not be required to agree to such a request, but if the covered entity and the individual agree to a restriction, the covered entity would be bound by the agreement.

Uses and disclosures with individual authorization

- Covered entities could use or disclose protected health information with the individual's authorization for almost any lawful purpose.

- We would prohibit covered entities from conditioning treatment or payment on the

individual agreeing to disclose information for other purposes, and require the authorization form to state this prohibition.

- While the provisions of this proposed rule are intended to make authorizations for treatment and payment purposes unnecessary, some States may continue to require them. Generally, this rule would not supersede such State requirements. However:
  - -- the rule would impose a new requirement that such State-mandated authorizations must be physically separate from an authorization for other purposes described in this rule.
  - -- the authorization would have to meet the rule's requirements for the content of such authorizations (although a state law could require that an authorization contain additional provisions).

- We would require authorizations to specify the information to be disclosed, who would get the information, and when the authorization would expire. If an authorization is sought so that a covered entity may sell or barter the information, the covered entity would have to disclose this fact on the authorization form.

- Use or disclosure of information by the covered entity inconsistent with the authorization would be unlawful.

- Individuals could revoke an authorization.

Permissible uses and disclosures for purposes other than treatment, payment and operations

- Covered entities could use and disclose protected health information without individual authorization for the following national priority activities:

  - -- Oversight of the health care system, including quality assurance activities;
  - -- Public health, and in emergencies affecting life or safety;
  - -- Research;
  - -- Judicial and administrative proceedings;
  - -- Law enforcement;
  - -- To provide information to next-of-kin;
  - -- For identification of the body of a deceased person, or the cause of death;
  - -- For government health data systems;
  - -- For facilities' (hospitals, etc.) directories;
  - -- To financial institutions, for processing payments for health care; and
  - -- In other situations where the use of disclosure is mandated by other, consistent with the requirements of the other law.

- Specific conditions would have to be met in order for the use or disclosure of protected health information to be permitted. These conditions are tailored to the need for each specific category listed above and to the types of organizations involved in such activities.

Individual rights

The proposed rule would provide several basic rights for individuals with respect to protected health information about them. Individuals would have:

- The right to receive a written notice of information practices from health plans and providers. The notice must describe the types of uses and disclosures that the plan or provider would make with health information (not just those uses and disclosures that could lawfully be made). When plans and providers change their information practices, they would also have to update the notice. Plans and providers would be required to follow the information practices specified in their most current notice.

- The right to obtain access to protected health information about them, including a right to inspect and obtain a copy of the information.

- The right to request amendment or correction of protected health information that is inaccurate or incomplete.

- The right to receive an accounting of the instances where protected health information about them has been disclosed by a covered entity for purposes other than treatment, payment, or health care operations (subject to certain time-limited exceptions for disclosures to law enforcement and oversight agencies).

Administrative requirements and policy development and documentation

This proposed rule would require providers and payers to develop and implement basic administrative procedures to protect health information and the rights of individuals with respect to that information.

- Covered entities would be required to maintain documentation of their policies and procedures for complying with the requirements of the proposed rule. The documentation must include a statement of the entity's practices regarding who would have access to protected health information, how that information would be used within the entity, and when that information would or would not be disclosed to other entities.

- Covered entities would be required to have in place administrative systems, appropriate to the nature and scope of their business, that enable them to protect health information in

accordance with this rule. Specifically, covered entities would be required to:

-- designate a privacy official;
-- provide privacy training to members of its workforce;
-- implement safeguards to protect health information from intentional or accidental misuse;
-- provide a means for individuals to lodge complaints about the entity's information practices, and maintain a record of any complaints; and
-- develop a system of sanctions for members of the workforce and business partners who violate the entity's policies.

Scalability

We propose privacy standards that covered entities must meet, but leave the detailed policies and procedures for meeting these standards to the discretion of each covered entity.

- We intend that implementation of these standards be flexible and scalable, to account for nature of each covered entity's business, and the covered entity's size and resources. We would require that each covered entity assess its own needs and implement privacy policies appropriate to its information practices and business requirements.
- The preamble to the proposed rule will include examples of how implementation of these standards are scalable.

Preemption

Pursuant to HIPAA, this rule will preempt state laws that are in conflict with the regulatory requirements and that provide less stringent privacy protections, with specified exceptions for certain public health functions and related activities.

Enforcement

- Under HIPAA, the Secretary is granted the authority to impose civil monetary penalties against those covered entities which fail to comply with the requirements of this regulation.

- HIPAA also established criminal penalties for certain wrongful disclosures of protected health information. These penalties are graduated, increasing if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain.

- Civil monetary penalties are capped at $25,000 for each calendar year for each standard that is violated.

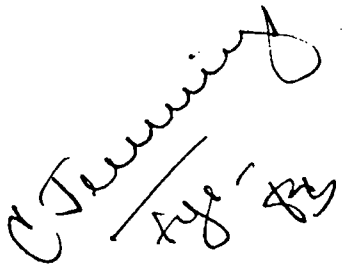
What this proposed rule does not do

- The HIPAA limits the application of our proposed rule to the covered entities. It does not provide the authority for the rule to reach many entities that receive health information from these covered entities, so the rule cannot put in place appropriate restrictions on how such recipients of protected health information may use and re-disclose such information.

- Any provider who maintains a solely paper information system cannot be subject to these privacy standards.

- There is no statutory authority for a private right of action for individuals to enforce their privacy rights.

THE PRESIDENT HAS SEEN
10-28-99



copies
Jennings
Podesta

CLINTON TO UNVEIL RULES TO PROTECT MEDICAL PRIVACY

FAULTS CAPITOL IMPASSE

Sharing of Records in Age of Managed Care Is Issue — Insurers See High Cost

By ROBERT PEAR

WASHINGTON, Oct. 26 — President Clinton will soon announce sweeping new Federal rules to protect the privacy of billions of medical records and will assail Congress for failing to enact any safeguards, Administration officials said today.

The proposed regulations would be the first comprehensive Federal standards specifically intended to protect the confidentiality of medical records. The move comes at a time when doctors, hospitals, pharmacists and health maintenance organizations are sharing more and more data, often without the knowledge of patients, and insurance companies are demanding more information to justify the payment of claims.

Consumer advocates support most of the Administration's proposals. But the proposed rules have generated criticism from insurance companies and hospitals, which say the rules would be costly to carry out. Law-enforcement officials have also expressed concerns because they believe the rules could require them to obtain search warrants in cases where warrants are not now required. And psychiatrists have criticized the rules, saying they may unintentionally weaken a patient's control over medical records.

The proposed rules would cover any medical records that are kept or transmitted electronically, as well as paper printouts of electronic transactions. Patients would generally have a right to review and copy their medical records, and to supplement the records or correct mistakes, Administration officials said. Doctors, hospitals and insurers could not disclose personal health information except for certain specified purposes like medical treatment and the payment of claims.

Most medical records are still kept on paper, but a growing number of health plans require doctors to submit claims electronically. In practice, health care experts said, the proposed rules would set standards for all medical records because it is not practical for doctors and insurers to follow different policies for the use of personal medical information kept in different forms.

Congress has been trying to write such protections into law, but the effort has stalled because of profound disagreements between privacy advocates and the health care industry. In 1996, Congress imposed a deadline on itself, requiring the Secretary of Health and Human Services to issue privacy rules if lawmakers failed to pass health privacy legislation by Aug. 21, 1999. The Administration's new proposals carry out that requirement.

The public will have an opportunity to comment on the proposed rules. Under the 1996 law, the Secretary of Health and Human Services must issue final rules by Feb. 21 next year.

In offering the proposed rules, White House officials said, Mr. Clinton will try to achieve three political purposes. He will put pressure on Congress to pass legislation, to provide a solid statutory framework for the new standards. He will present himself as a champion of privacy rights, a politically popular cause. And, by making aggressive use of his power, he will try to counter the perception of himself as a lame duck.

The President expressed impatience on Monday, when he criticized Republicans for blocking his proposal to provide prescription drug benefits under Medicare. In a fleeting reference to his next initiative, Mr. Clinton said: "Because they have not taken action to protect the privacy of medical records, I will use the power of my office to do that in the coming days."

Chris Jennings, the health policy coordinator at the White House, said: "We would have preferred that Congress pass bipartisan legislation. They gave themselves three years to do it. But in the absence of action on Capitol Hill, the President will act."

Federal officials are still analyzing the cost of their proposals. A recent study by the Blue Cross and Blue Shield Association said that compliance with such standards could cost tens of billions of dollars because health care providers, health plans and insurance companies would have to retrain employees, hire privacy experts, rewrite contracts and reprogram computers.

Administration officials are compiling data to try to undercut those cost estimates.

The rules appear stricter than the comparable provisions of a landmark bill hammered out last week to overhaul the nation's financial system. Under that bill, divisions of a big financial conglomerate — for example, an insurance company and a consumer bank — could share information about a customer under many circumstances, and they would have to inform customers at least once a year of their policies on privacy and disclosure.

Under the medical privacy rules, an insurer would also have to inform the subscriber of its privacy practices, but it would be more difficult for the insurer to share health information with an affiliated company. In most cases, the insurer would have to get the consumer's permission before allowing use of the data for purposes unrelated to medical treatment or the payment of claims.

The proposed rules will probably not go far enough to satisfy psychiatrists, but may go too far for some law-enforcement officials.

Dr. Paul S. Appelbaum, vice president of the American Psychiatric Association, said: "The Administration's proposal would protect notes taken by a therapist in the course of psychotherapy, and that's good. But it would take away some of the power that patients have traditionally had to decide when and if their records are released to third parties. Under these rules, much information could be disclosed without the patients' consent to anybody involved in their care."

In general, law-enforcement agencies would need a search warrant, a subpoena or some other legal authorization to get confidential medical records. Federal, state and local law-enforcement officials said they wanted to preserve their ability to get immediate access to medical information without a warrant in emergencies — when they are investigating a bomb threat or trying to rescue hostages, for example.

John R. Justice, chairman of the National District Attorneys Associa-

Clinton attacks Congress as stalling on privacy.

tion, said investigators often did not have enough time or specific information to get a warrant for medical records in "exigent circumstances." For example, he said, the police may want to know about the health problems of a person who is holding hostages or being held hostage.

Experts on health privacy in and out of the Government said the rules also included these provisions:

¶Health care providers and H.M.O.'s would not have to get a patient's consent before disclosing information needed for medical treatment or the payment of claims. But they would have to get the patient's consent if the information was to be used for marketing and certain types of research.

¶The Federal rules would establish minimum protections for patients' privacy and would not override any contrary provisions of state law that were "more stringent" than the Federal requirements.

¶Before disclosing data, doctors would have to take reasonable steps to make sure they did not disclose more information than was needed to accomplish the purpose of the request. The rules would forbid the wholesale release of entire records when a small part would suffice.

¶Doctors, hospitals and health plans could charge a reasonable fee to cover the cost of copying records.

Under Federal law, doctors and hospitals can be fined up to $50,000 for the improper disclosure of confidential medical information, and they are subject to larger fines if they sell such data for "commercial advantage" or "malicious harm." Under the proposed rules, patients would not gain any new Federal right to sue a doctor or an H.M.O. for divulging medical records. Federal officials said only Congress could create a new right to sue.

The proposed rules would provide additional protection for some sensitive personal information in mental health records, but not as much protection as many psychiatrists want.

Under the proposal, a psychotherapist would not need a patient's consent to disclose information about the diagnosis of a condition, the patient's level of functioning or medications when such information was necessary for treatment or for the payment of claims. But the therapist would have to get the patient's consent before disclosing more detailed information about a patient's feelings or sexual relationships.

The New York Times

WEDNESDAY, OCTOBER 27, 1999

Executive Office of the President of the United States

Peter P. Swire
The Chief Counselor for Privacy
Office of Management and Budget
Washington D.C. 20503
(202) 395-1095
(202) 395-6974 (FAX)

FAX TRANSMITTAL

TO: Devorah Adler

Fax: 456 - 5557

From: Peter Swire

Date: Oct 18

Total Number of Pages: 6

Comments:

HEALTH PRIVACY POLLING DATA

January 1999 poll by Princeton Survey Research Associates for the California HealthCare Foundation:

- **One in five** American adults believe that a health care provider, insurance plan, government agency, or employer has improperly disclosed personal medical information. Half of these people say it resulted in personal embarrassment or harm.
- **One in six** American adults say they have done something out of the ordinary to keep personal medical information confidential. Among the actions reported: going to another doctor; paying out-of-pocket for services; not seeking care; giving inaccurate or incomplete information on a medical history; and asking a doctor not to write down the health problem or record a less serious or embarrassing condition.
- **Only a third** of U.S. adults say they trust health plans and government programs like Medicare to maintain confidentiality all or most of the time.

1992 poll by Louis Harris & Associates for Equifax:

- 27% of the public believe they have been the victims of an improper disclosure of personal health information.
- In order to protect their privacy, 11% said that they or an immediate family member paid out-of -pocket for health care, rather than submit a claim.
- Seven percent chose not to seek care because they didn't want to harm their "job prospects or other life opportunities."

1993 poll by Louis Harris & Associates for Equifax:

- 67% believe there are *already* strong laws protecting the confidentiality of medical records.
- Majority of the public (56%) favored the enactment of strong comprehensive federal legislation to protect the privacy of health care information.
- Of that majority, eighty-five percent (85%) responded that protecting the confidentiality of medical records was absolutely essential or very important to

them.

- An overwhelming percentage wanted penalties imposed for unauthorized disclosure of medical records (96%), guaranteed access to their own records (96%), and rules regulating third-party access to personal health information.

1995 poll by Louis Harris & Associates for Equifax:

- 82% of people were concerned about their privacy, up from 64% in 1978.

1996 poll by Louis Harris & Associates for Equifax:

- Only eighteen percent (18%) of the public consider the use of patient records for medical research without prior permission to be very acceptable. Thirty-nine percent (39%) found the use somewhat acceptable. The public's comfort level increased if the information released did not identify individual patients, but one-third found it not at all acceptable for researchers to use non-identifiable health information without patient consent.

MEDICAL PRIVACY STORIES

- Medical Marketing Service advertises a database available to pharmaceutical marketers which includes the names of 4.3 million people with allergies; 923,000 with bladder control problems; and 380,000 who suffer from clinical depression. (See www.mmslists.com)

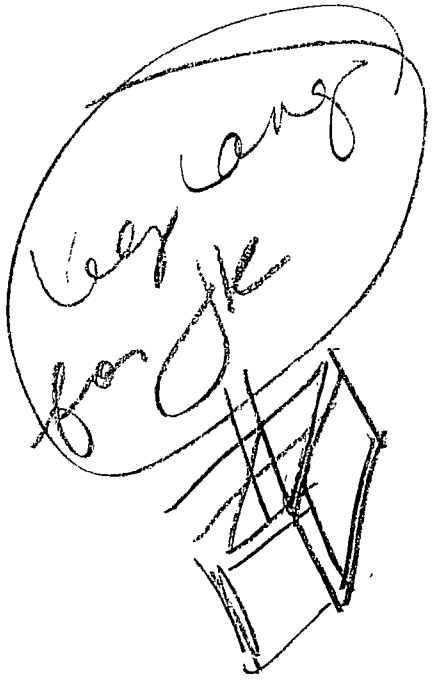
- The chain drug stores CVS and Giant Food admitted to making patient prescription records available for use by a direct mail and pharmaceutical company. Their stated intent was to track customers who don't refill prescriptions, and send them letters encouraging them to refill, and consider alterative treatments. However, in response to the outrage and worry expressed by their customers, both companies subsequently advertised their plans to abandon their marketing and direct mail campaigns. ("Prescription Fear, Privacy Sales," *The Washington Post*, p. A1, 2/15/98)

- An Orlando woman recently had her doctor perform some routine tests, and received a letter weeks later from a drug company touting a treatment for her high cholesterol. ("Many Can Hear What You Tell Your Doctors: Records of Patients Are Not Kept Private," *Orlando Sentinel*, 11/30/97, A1)

- After suffering a work-related injury to her wrist, Roni Breite authorized her insurance company to release information pertaining to her wrist ailment to her employer. When she had the opportunity to review her medical record, the file contained her *entire* medical history, including records on recent fertility treatment and pregnancy loss. (E. McCarthy, "Patients voice growing concerns about privacy," *Sacramento Business Journal*, April 5, 1999)

- Several thousand patient records at the University of Michigan Medical Center inadvertently lingered on public internet sites for two months. The problem was discovered when a student searching for information about a doctor was linked to files containing private patient records with names, addresses, phone and Social Security numbers, job status, treatments for medical conditions and other data. ("Black Eye at the Med Center," *Washington Business*, February 22, 1999)

- Recently, Aetna health insurance claim forms blew out of a truck on the way to a recycling center and scattered on I-84 in East Hartford during the evening rush hour. Aetna, the nation's largest health insurer, quickly dispatched employees — some of them on the way home from work — to scoop up forms containing names and personal health information. Both times, the papers should have been shredded under company policy, but weren't. ("Careless Disposal of Records Imperils Privacy," *The Hartford Courant*, May 14, 1999)


Very long
for Jake

- Intermountain HealthCare, a Utah-based health plan, recently took steps to recover patient medical files that were misplaced. IHC said that its Salt Lake Clinic had donated a file cabinet to Deseret Industries, and did not know that some records and laboratory reports had accidently slipped behind the drawers.
(J. Costanzo, "IHC Sues over Misplaced Records," *The Deseret News*, December 2, 1998)

- In a 1993 poll, 27% of those polled believed that their medical information had been improperly disclosed. Almost a third of health care leaders could describe confidentiality violations in their organizations in detail. (*Louis Harris Privacy Surveys*)

- The 13-year-old daughter of a hospital employee took a list of patient's names and phone numbers from the hospital when visiting her mother at work. As a joke, she contacted patients and told them that they were diagnosed with HIV. (*The Washington Post*, March 1, 1995)

- The Harvard Community Health Plan, a Boston-based HMO, admitted to maintaining detailed notes of psychotherapy sessions in computer records that were accessible by all clinical employees. Following a series of press reports describing the system, the HMO revamped its computer security practices. (*Boston Globe*, March 7, 1995)

- In *Doe v. Septa*, Rite-Aid drug store in Pennsylvania provided to the state's transportation authority (SEPTA) information about the prescription drugs being taken by SEPTA's employees. In disclosing to SEPTA authorities that one of its employees was receiving AZT, Rite-Aid in effect disclosed the employee's HIV status. Prior to the disclosure, Doe's employers had assured him that although they were self-insured, no information regarding his prescription drugs or HIV status would be disclosed outside of the Medical Department. The court found no privacy violation stemming from this disclosure since Doe could not prove actual damages and the employer was deemed to have a legitimate interest in knowing the details of how its employees used the health plan.
(*Doe v. Septa*, WL 76, 2891. (3d Cir. 1995))

- After news of actress Nicole Kidman's recent surgery was leaked to the press, photos of her leaving the UCLA Medical Center appeared in papers with commentary about her health status. (*Parade Magazine*, May 10, 1998)

- In Tampa, a public health worker walked away with a computer disk containing the names of 4,000 people who tested positive for HIV. The disks were sent to two newspapers. (*USA Today*, October 10, 1996)

- A banker who also served on his county's health board cross referenced customer accounts with patient information. He called due the mortgages of anyone suffering from cancer. (*The National Law Journal*, May 30, 1994)

- New York Congresswoman Nydia Velasquez' confidential medical records — including details of a bout with depression and a suicide attempt — were faxed from a New York

hospital to a local newspaper and television station on the eve of her 1992 primary. After overcoming the fallout from this disclosure and winning the election, Rep. Velasquez testified eloquently about her experiences before the Senate Judiciary Committee as it was considering a health privacy proposal.

- In Maryland, eight Medicaid clerks were prosecuted for selling computerized record printouts of recipients' and dependents' financial resources to sales representatives of managed care companies. (*Forbes*, May 20, 1996, p. 252)

- The late tennis star Arthur Ashe's positive HIV status was disclosed by a health care worker and published by a newspaper without his permission.

Medical Record Privacy Regulations
Talking Points

- For the first time in our nation's history, the Federal government is proposing a set of strong, enforceable national standards protecting the privacy of Americans' medical records. This is truly an historic step.

- Federal privacy laws protect consumers' bank records, their credit reports, and even their video rental records. Yet, until now, there have not been federal standards protecting the privacy of medical records – the most sensitive information a person has. While many states have worked hard to protect patients in this area, these laws are quite uneven and contain many significant gaps.

- These proposed standards will protect the privacy of patients' medical records created by doctors, hospitals, health plans, and health care clearinghouses that are either transmitted or maintained electronically.

- Americans are worried that the privacy of their medical information will be violated. A recent national survey showed that one in five Americans believe that their health information is not secure. In fact, 1 in 6 Americans are already taking action on their own to avoid creating a medical record, including withholding information from their doctors, changing doctors, or even avoiding care altogether. The absence of privacy protections is compromising the quality of care in our country.

- The standards being proposed by HHS today follows the five principles that I put forward to Congress two years ago and will provide Americans with greater peace of mind as they seek care. They will also make the delivery of health care more efficient by allowing health care providers, health plans, and health care clearinghouses to operate under a consistent set of rules.

- The standards being proposed today – while important – do not provide Americans with complete protection. HIPAA limits our authority to those medical records that are either transmitted or maintained by electronic means. We do not have authority to protect records that are maintained in paper form only. We also are unable to provide Americans with a critical consumer protection – the right to take action in the courts when their medical information is used inappropriately. Congress must act to fill these significant gaps in patient protection.

- The Clinton Administration continues to believe that the best solution to these problems is the enactment of a bipartisan law that establishes a strong national floor of privacy protections for all Americans. We are committed to working with the

Congress to pass such a law. In the meantime, we will move ahead with implementing the standards we propose today.

- Earlier this month, the House of Representatives put aside partisan bickering and passed a comprehensive Patients' Bill of Rights. Congress should continue this bipartisan approach and enact a comprehensive medical privacy bill that President Clinton can sign.