PHOTOCOPY
PRESERVATION

(HEALTH - & PRIVACY REGULATION

DRAFT: QUESTIONS ON MEDICAL RECORDS PRIVACY REGULATION

WHAT DOES THE REGULATION DO?

Q: How can you present this regulation as a comprehensive privacy regulation when it allows doctors, hospitals, and health plans to share patients' health information without their consent?

A: This regulation establishes, for the first time ever, establish strong new Federal protections for sensitive health information that is transmitted or maintained electronically. It applies to all health plans, health care clearinghouses such as billing companies, and many health care providers, and will limit the use and release of private health information without consent; restrict the disclosure of protected health information to the minimum amount of information necessary; and establish new administrative and criminal sanctions for the improper use or disclosure of private information.

It's true that the regulation allows plans and providers to use and share health information for health care purposes such as treatment and payment for services in order to ensure smooth functioning of the health care system. However, it requires consent and creates other barriers for use and sharing of such information for purposes not related to health care. We would require the person's consent for uses unrelated to health care, such as marketing, financial underwriting, and employment purposes.

Q: This new regulation doesn't cover many of the entities – like employers – that are responsible for many of the abuses. It also doesn't extend to paper records, which is how most of the medical records in this country are stored. Is this regulation going to have any effect at all?

A: This regulation is a strong first step towards protecting medical records privacy nationwide. Because uncovered entities get the health records they use from plans, providers and clearinghouses, we believe that holding these sources of personal health information to strong privacy standards will greatly enhance patient privacy. In addition, a growing number of paper records are transmitted electronically at some point, and will thus be covered by the regulation.

However, we agree that this regulation is only a first step. Because of limited statutory authority, it does not cover all paper records, which is still how older health records are stored; directly regulate employers, other insurers, public health agencies and other entities accessing information; or create the private right of action that would allow citizens to hold health plans and providers directly accountable for inappropriate and harmful disclosures of information. This is why the President continues to urge the Congress to pass comprehensive legislation without delay.

WOULD YOU VETO A BILL WITH A RIDER?

Q: Some in Congress are already talking about blocking these regulations. What would the President do if Congress added such a provision to either an appropriations bill or a continuing resolution?

A: Comprehensive federal privacy protections are an urgent national priority. Congress recognized this when it gave itself a three-year deadline, and then imposed the regulatory mandate under which we are proposing this regulation. We continue to favor legislation establishing national standards for health records privacy, and are working with the Congress to achieve that result. However, if Congress attempts to impose further delays, the President's senior advisors would likely recommend that he veto such legislation.

EXCESSIVE BURDEN AND COST IMPLICATIONS

Q: Isn't this new rule excessively burdensome for health plans and providers?

A: We do not think so. The regulation is designed to balance the impact of these new requirements on health plans and provider with the pressing need to take action to protect the privacy of health records. Recent studies indicate that two-thirds of Americans do not trust health plans to maintain confidentiality all of the time. Many health plans and providers already use good information practices today, and we believe that all providers should be required to implement these important protections. The cost of not moving ahead in this area is that patients remain unprotected and vulnerable to harmful disclosures of private information.

Q: Won't these new regulations be too costly to implement?

A: We do not believe that there will be an excessive cost that would result from implementing these long overdue protections. The cost of doing nothing is far more problematic. For example, because of the fear that many patients have about the misuse of their medical records, they avoid preventive screenings that could prevent costly hospitalizations. Recognizing this, Congress continues to work on legislation that is even broader in scope than we are authorized to do under current law. We are both working on this issue because they recognize that any cost associated with appropriate interventions in this area are more than offset by the protections they provide.

Q: What is the cost of this new regulation?

A: While full costs are difficult to determine, we have been able to estimate costs for the majority of tasks involved. Our initial calculations show that improving privacy protection through this regulation would be approximately $1.2 billion in the first year and $650 million per year after the first year, a total of $3.7 billion over five years for the tasks we can estimate. This is less than one-tenth of one percent of national health expenditures. We have asked for comments that will help us estimate a more complete set of costs.

ABORTION

Q: Your regulations would allow minors to obtain health care services – including family planning and abortion – without their parents knowledge or consent. Isn't this changing current law?

A: Our proposal would continue to allow states to regulate minors' access to health care services. We are not changing the law in this area.

LAW ENFORCEMENT

Q: You appear to have reversed course on the issue of access to health records by law enforcement authorities. Why? Does the Attorney General support these regulations?

A: Our goal all along has been to strike the proper balance and find ways to guard the privacy of medical records while assuring the protection of public safety. In May, the Justice Department wrote a letter to Senator Jeffords, stating that the Department "recognizes that additional safeguards are necessary to prevent future abuses of medical records privacy, particularly in response to the growing use of computers to store, analyze, and distribute confidential health information." The proposed regulations spell out the safeguards the Administration, including the Department of Justice, believes are appropriate.

Q: Law enforcement officials say that the standards will have a negative impact on their ability to protect public safety. How do you respond?

A: The proposal includes important safeguards to assure that law enforcement officials can get access to essential information. In many circumstances, such as for national-security purposes or to obtain information about a victim's medical condition that is needed immediately, no warrant or similar process would be required. Where officials are seeking to identify a suspect, fugitive, material witness, or missing person, then limited identifying information can be released, which can then form the basis for getting a search warrant or other legal process.

Q: How will the law enforcement provisions work?

A: The proposed rules would allow use and disclosure of health information without the individual's written consent for treatment and payment, and would also allow such use and disclosure for specified priority public policy purposes, including law enforcement. We would allow law enforcement access to medical records due to the importance of protecting public safety, but only when specified requirements are met. In some instances, a warrant or other process would be required. In other instances, the law enforcement official would need only show proof of identification in order to obtain health information.

Q: What are the proposed requirements for law enforcement access?

A: The general rule is that covered entities may disclose records to law enforcement officials only upon a proper, written request. The request may be under an order signed by a judicial officer. It may be under a grand jury subpoena, where the information disclosed will be under grand jury secrecy protections. Or, the request may be by administrative subpoena, subject to a new three-part test. We also provide exceptions, when the law enforcement official would need only show proof of identification in order to obtain health information. These exceptions include when law enforcement is seeking information about a victim's medical condition that is needed immediately, certain national-security purposes, and where officials are seeking to identify a suspect, fugitive, material witness, or missing person.

Q: Are there other law enforcement circumstances where disclosure is allowed?

A: Yes. The proposed rule would allow disclosure without process when law enforcement officials are seeking information about an individual who is or is suspected to be a victim of a crime, abuse, or other harm. In such cases, the law enforcement official could state that the information is needed immediately and is needed to determine whether a violation of law by a person other than the victim has occurred.

Q: Isn't this new rule too lenient on the law enforcement community?

A: The new system must meet two goals at the same time -- protecting patients' privacy and protecting public safety. Consider how often medical information is needed in law enforcement -- to investigate crimes, determine whether a crime was committed, learn the seriousness of a crime, allow prosecutors to determine the proper charge, and set bail, to take but a few examples. Federal enforcement officials and those in each state have differing authorities and procedures for getting this essential information. For instance, about half the states do not have grand juries, and procedures must be available nationwide to get needed medical information. This regulation only has jurisdiction over covered entities such as health care providers and plans, and cannot directly govern courts or law enforcement officials. In light of this limited authority, and to strike the proper balance between the important goals, we have crafted a system that would allow law enforcement access based on administrative requests, where the three-part test is met. We cannot and should not put shackles on the ability of our law enforcement to do their jobs.

Q: Does this proposal undercut the Administration's ability to fight health care fraud?

A: No. There are separate provisions in the proposed regulation for health care oversight. These provisions assure that the necessary information will remain available for civil and criminal enforcement against health care fraud.

Donnals - PRIVACY

Kathleen Rooney Donnals 864 7359

Eddy -

① Org: MPRA by COI — but 22 by federal trustees

- CMS enforcement: what level of privacy would they pursue?
  a. → need subpoenas? what kind - admin or court?
     ⓐ HHS/privacy court letter
  b. → does DOJ need showing on DISCLOSURE HIST?
  c. → what protections when in pursuit of a crime
     - last pursuit: other, no hosp
     - exigent circ: in letter proposal - by p., or "in course of ID or suspect" → DOJ has broad, HHS not
     - non-exigent circ: can you use subp again - (likely handed to Podeker) ↪ HHS will do memo to Eddy +

② MINOR'S RIGHTS / NJ STATUTE: how much access to kids' records? can I use client beneficiary?
- states split → what we do → don't disturb. states guess, but need to say courts affirmatively
- confidentiality org

③ DISCLOSURE WITH
- under HIPAA courts more but weak fines
- could use MCare or OPM — need not wait to pass in other program → HHS worries. wants to see look like a usurpation. wait keep at HIPAA ↪ point to later subsidy

④ Common Rule Prot: sets a standard on human subj research + we need ENHANCE them
- contrast w/ not other HIPAA, point to PREAMBLE

⑧ privacy act – held to fed-held records ⇒ DoD + VA
only to both the + our new reg. ⇒ how handle
overlap? DoD has been lax on this.

⑨ Medicare/SSA/DoD – CIA wants/gets blanket exemption
DoD asking, but HHS says not acceptable – fear of
double standard ~ VA benefits + Treasury says no other
agencies requested

who it relates?
Rodger speaks?

↓

- Kathy Buckley – OMB
- Emily R. W. – NEC
  Handouts by HR(O) + Treasury ~
  by this letter but Brenda who is
  drawing it
- Dan Mendelson
- Gary K. – HHS
  - Jason Horowitz – HHS Leg Aff.
  - Debbie Gary Gambler – DoJ.

THE NEED FOR LEGISLATION

It has been 25 years since former HEW Secretary Elliot Richardson set forth principles that led to the landmark Federal Privacy Act. Those 25 years have brought vast changes in our health care system.

Revolutions in our health care delivery system mean that we must place our trust in entire networks of insurers and health care professionals - both public and private. The computer and telecommunications revolutions mean that information no longer exists in one place - it can travel in real time to many hospitals, physicians, insurers, and across state lines.

In addition, revolutions in biology mean that a whole new world of genetic tests have the potential to either help prevent disease or reveal the most personal health information of a family. Without safeguards to assure citizens that getting tested will not endanger their families' privacy or health insurance, we could endanger one of the most promising areas of research our nation has ever seen.

Health care privacy can be safeguarded. It must be done with national legislation, national education, and an on-going national conversation.

Currently, when we give a physician or health insurance company precious health information, the level of protection will vary widely from state to state. We have no comprehensive federal health information privacy standards. Because the practice of health care is increasingly becoming interstate through mergers, complex contractual relationships and enhanced telecommunications, we can no longer rely on the existing patchwork of state laws. The patchwork does not provide Americans the privacy protections they need or expect. The Congress should seize upon this opportunity to create strong federal standards and reassure the public that they can trust their providers and insurers to keep their health information secure.

In developing our recommendations for federal legislation, we learned a great deal through consultations with a variety of outside groups and from six days of public hearings conducted by the National Committee on Vital and Health Statistics, our statutory federal advisory committee for health data and privacy policy. The hearings involved over 40 witnesses from across the health community, including health care professionals, plans, insurance companies, the privacy community, and the public health and research communities.

We believe our recommendations provide a balanced framework for legislation that can protect the privacy of medical records, guarantee consumers the right to inspect their records, and punish unauthorized disclosures of personal health data by hospitals, insurers, health plans, drug companies or others.

THE PRINCIPLES

The Secretary's recommendations for legislation are grounded in five key principles: Boundaries, Security, Consumer Control, Accountability, and Public Responsibility.

Boundaries

The first is the principle of Boundaries: With very few exceptions, personally identifiable health care information should be disclosed for health purposes and health purposes only. It should be easy to use it for those purposes, and very difficult to use it for other purposes.

For example, employers should be able to use the information furnished by their employers to provide on-site care or to administer a health plan in the best interests of those employees. But those same employers should not be able to use information obtained for health care purposes to discriminate against individuals when making employment decisions - such as hiring, firing, placements and promotions. To enforce these boundaries, we recommend strong penalties for the inappropriate use or disclosure of medical records.

We recommend that the legislation apply specifically to providers and payers, and to anyone who receives health information from a provider or payer, either with the authorization of the patient or as authorized explicitly by legislation.

However, our recommendations acknowledge that these providers and payers do not act alone. In order for a provider or payer to operate efficiently, it may need to enlist a service organization to perform an administrative or operational function. For example, a hospital may hire an organization to encode and process bills, or a managed care organization may contract with a pharmaceutical benefit management company to provide information to pharmacists about what medications are covered and appropriate for their customers.

The numbers and types of service organizations are increasing every day. While most do not have direct relationships with the patients, they do have access to their personal health care information. Therefore, we recommend that they should be bound by the same standards. For example, a health plan's contractor should be allowed to have access to patient lists in order to do mailings to remind patients to schedule appointments for preventive care. But it should not be able to sell the patient lists to a pharmaceutical company for a direct mailing announcing a new product.

Because we recommend a minimum floor of protection for all records, our report does not distinguish among types of health care information based on sensitivity. For example, our recommendations do not include specific provisions related to genetic information in health records.

Genetic information should be covered by the same rules. However, we recognize that the public is especially concerned about the unique properties of genetic information - its predictive nature, and its link to personal identity and kinship and its ability to reveal our family secrets.

Therefore while you are developing privacy legislation, you should also consider how to limit the collection and disclosure of genetic information and prohibit health insurers and employers from discriminating against individuals on the basis of their genetic information. Because of the

speedy development of genetic technologies and its potential for abuse, we recommend that legislation concerning discrimination in underwriting by insurers or other improper use of such information be considered expeditiously. We look forward to continuing our work with you on this issue.

Security

The second principle is Security. Americans need to feel secure that when they give out personal health care information, they are leaving it in good hands. Information should not be used or given out unless either the patient authorizes it or there is a clear legal basis for doing so.

There are many different ways that private information like your blood tests could become public. People who are allowed to see it - such as lab technicians - can misuse it either carelessly or intentionally. And people who should not be seeing it - such as marketers - can find a way to access it, either because the organization holding the information doesn't have proper safeguards or the marketers can find an easy way around the safeguards. To give Americans the security they expect and deserve, Congress should develop legislation that requires those who legally receive health information to take reasonable steps to safeguard it and face consequences for failure to do so.

What do we mean by reasonable steps? The organizations should adopt protective administrative and management techniques, educate their employees, and impose disciplinary sanctions against employees who use information improperly.

We are addressing some of these steps in our Security Standards regulation, implementing the Administrative Simplification mandate under HIPAA. Our NPRM laid out a range of approaches for safeguarding the information to which the HIPAA mandate applies. However, that regulation will only cover the security of specific electronically maintained records. We need comprehensive privacy legislation to cover all health information that needs this kind of protection.

We don't believe a law can specify the details of these protections because each organization must keep pace with the new threats to our privacy and the technology that can either abate or exacerbate them. But a federal law can require everyone who holds health information to have these types of safeguards in place and specify the appropriate sanctions if the information is improperly disclosed.

Consumer Control

The third principle is Consumer Control. The principles of fair information practice (formulated in 1973 by a committee appointed by Secretary Richardson) included as a basic right: "There must be a way for an individual to find out what information about him is in a record and how it is used."

With very narrow exceptions, consumers should have the right to find out what is contained in their records, find out who has looked at them, and to inspect, copy and, if necessary, correct them. Consumers should be given a clear explanation of these rights and they should understand how organizations will use their information. Let me give you an example of why this is important. According to the Privacy Rights Clearinghouse, a California physician in private practice was having trouble getting health, disability, and life insurance. She ordered a copy of her report from the Medical Information Bureau - an information service used by many insurance companies. It included information showing that she had a heart condition and Alzheimer's disease. There was only one problem. None of it was true. Unfortunately, under the current system these types of errors occur all too often. Consumers often do not have access to their own health records and even those who do are not always able to correct some of the most egregious errors.

With that in mind, our recommendations set forth a set of practices and procedures that would require that insurers and health care providers provide consumers with a written explanation detailing who has access to their information and how that information will be used, how they can restrict or limit access to it, and what their rights are if their information is disclosed improperly.

We also recommend procedures for patients to inspect and copy their information, and set out the very limited circumstances under which patient inspection should be properly denied.

Finally, we recommend a process for patients to seek corrections or amendments to their health information to resolve situations in which innocent coding errors cause patients to be charged for procedures they never received, or to be on record as having conditions or medical histories that are inaccurate.

Accountability

The fourth principle is Accountability. If you are using information improperly, you should be punished. This flows directly from the second principle of security - the requirement to safeguard information must be followed by real and severe penalties for violations. Congress should send the message that protecting the confidentiality of health information is vitally important, and that people who violate that confidence will be held accountable.

We recommend that offenders should be subject to criminal felony penalties if they knowingly obtain or use health care information in violation of the standards outlined in our report. The penalties mandated in privacy legislation should be higher when violations are for monetary gain, similar to those Congress mandated in the administrative simplification provisions of HIPAA. In addition, when there is a demonstrated pattern or practice of unauthorized disclosure, those committing it should be subject to civil monetary penalties.

In addition to punishing the perpetrators, we must give redress to the victims. We believe that any individual whose privacy rights have been violated - whether those rights were violated negligently or knowingly - should be permitted to bring a legal action for actual damages and

equitable relief. When the violation is done knowingly, attorney's fees and punitive damages should be available.

These first four principles - Boundaries, Security, Consumer Control and Accountability - must be carefully weighed against the fifth principle, Public Responsibility.

Public Responsibility

Just like our free speech rights, privacy rights can never be absolute. We have other critical - yet often competing - interests and goals. We must balance our protections of privacy with our public responsibility to support national priorities - public health and safety, research, quality care, and our fight against health care fraud and abuse and other unlawful activities.

Our Department is acutely aware of the need to use personal health information for each of these national priorities. For example, HHS auditors use health records to uncover kickbacks, overpayments and other fraudulent activity. Researchers have used health records to help us fight childhood leukemia and uncover the link between DES and reproductive cancers. Public health agencies use health records to warn us of outbreaks of emerging infectious diseases. In addition, our efforts to improve quality in our health care system depend on our ability to review health information to determine how well health institutions and health professionals are caring for patients.

For public health and safety, research, quality evaluations, fraud investigations, and legitimate law enforcement purposes, it's not always possible, or desirable, to ask for each patient's permission for access to the necessary health information. And, in many cases, doing so could create major obstacles in our efforts. While we must be able to use identifiable information when necessary for these purposes, we should use information that is not identifiable as much as possible.

To demonstrate how access must be balanced against public responsibility, let me outline a few of the areas in which we recommend that disclosure of health information should be permitted without patient authorization.

Public Health

Under certain circumstances, we recommend permitting health care professionals, payers, and those receiving information from them to disclose health information without patient authorization to public health authorities for disease reporting, adverse event reporting, public health investigation, or intervention. This is currently how the public health system operates under existing State and federal laws.

For example, consider the outbreak of E. coli in hamburger that resulted in the largest recall of meat products in history. Public health authorities, working with other officials, used personally identifiable information to identify quickly the source of the outbreak and thereby prevent thousands of other Americans from being exposed to a contaminated product.

Research

An important mission for the Department of Health and Human Services is to fund and conduct health research. We understand that research is vitally important to our health care and to progress in medical care. Legislation should not impede this activity.

Today the Federal Policy for Protection of Human Subjects and FDA's Human Subject Regulations protect participants in most research studies that are funded or regulated by the federal government. These rules have worked well to protect the privacy of individuals while not impeding the conduct of research. We recommend that similar privacy protections should be extended to all research in which individually identifiable health information is disclosed, and not just federally funded or regulated research.

All researchers must determine whether their research requires the retention of personal identifiers. There are research studies that can only be conducted if identifiers are retained; for example, outcomes studies for heart attack victims or the recent study which identified a correlation between the incidence of Sudden Infant Death Syndrome and the infant's sleep position. If, and when, personal identifiers are no longer needed, the researcher should be required to remove them and provide assurances that the information will be protected from improper use and unauthorized additional disclosures.

Under the Common Rule, if personal identifiers are necessary, an IRB must review the research proposal and determine whether informed consent is required or may be waived. In order for informed consent to be waived, an IRB must determine that the research involves no more than minimal risk to participants, that the absence of informed consent will not adversely affect the rights or welfare of participants, and that conducting the research would be impracticable if consent were required. This or a similar mechanism of review should be applicable for all research using individually identifiable health information without informed consent regardless of funding source.

This recommendation is consistent with the Federal Policy for the Protection of Human Subjects as well as the Privacy Act - policies that have protected federal research participants and research records for a quarter of a century and that have saved lives and fostered countless improvements in medical treatment.

PREEMPTION

Our recommendations call for national standards. But, we do not recommend outright or overall federal preemption of existing State laws that are more protective of health information.

Some protections that we recommend may be stronger than some existing State laws. Therefore, we recommend that Federal legislation replace State law only when the State law is less protective than the Federal law. Thus, the confidentiality protections provided would be

cumulative and the Federal legislation would provide every American with a basic set of rights with respect to health information.

CONCLUSION

Mr. Chairman, the five principles embodied in our recommendations - Boundaries, Security, Consumer Control, Accountability, and Public Responsibility - should guide a comprehensive law that will create substantive federal standards and provide our citizens with real peace of mind.

The principles represent a practical, comprehensive and balanced strategy to protect health care information that is collected, shared, and used in an increasingly complex world.

In addition to creating new federal standards, we must ensure that every single person who comes in contact with health care information understands why it is important to keep the information safe, how it can be kept safe, and what will be the consequences for failing to keep it safe. Most of all, we must help consumers understand not just their privacy rights, but also their responsibilities to ask questions and demand answers - to become active participants in their health care.

Flawed Provision in HR 10 Threatens Enactment of Strong, Comprehensive Medical Records Privacy Legislation

Despite strong opposition from privacy advocates, the House has included a poorly-drafted medical privacy provision in the financial modernization bill (HR 10). This provision allows sensitive personal medical information to be given out without consent for a wide range of activities, including marketing research and insurance underwriting. Moreover, although this provision gives the false impression of providing broad privacy protections, it threatens the long overdue, strong, comprehensive medical records privacy legislation. In reality, the language fails to provide any meaningful protections, would override some of the basic privacy protections already established at the state level, and is opposed by over 50 consumer and provider advocacy groups, including the AARP, the American Medical Association, and the National Breast Cancer Coalition. Shortcomings of the bill include:

- **Large loopholes allow for inappropriate disclosure of information.** HR 10 allows personal health information to be distributed without consent for a wide range of activities, such as insurance underwriting and marketing research, without providing the necessary safeguards to ensure that information won't be misused. For example, an employer could receive private medical information from a health insurer in order to use it when making decisions about hiring or firing employees.

- **Unlimited disclosure of private medical information**. In addition to allowing disclosure without the consent of the patient, HR 10 does not place common-sense limitations on the scope of the information released. Health insurers requesting documentation that a procedure has been performed should not be given a patient's entire medical record.

- **No restrictions on the use of medical information**. Under HR 10, once an insurer has an individual's private medical information, it can use it for any purpose it wishes. Information received on an insurance application could be used to deny an application for a home mortgage or credit card, all without the patient's consent or knowledge.

- **No real consumer protections.** HR 10 fails to provide crucial consumer protections, including: an individuals' right to access their information; the right to know how information is used; and an assurance that sensitive medical information is safeguarded against inappropriate access.

- **No way to enforce even these insufficient protections.** HR 10 does not provide an avenue for individual's to seek redress if their personal medical information is misused. A right without a remedy is not truly a right. Strong, enforceable privacy legislation includes enforcement mechanisms that make the rights of individuals real.

Finally, the health care industry has been arguing for a single set of rules in order to avoid the significant burdens of complying with multiple regulatory standards. The provisions in HR 10 would conflict with the standards established under Federal regulatory authority by the Health Insurance Portability and Accountability Act (HIPAA). Because this burdensome conflict would dramatically impair the ability of health insurers to conduct business, HIAA and Blue Cross Blue Shield oppose these provisions.

MEMORANDUM

TO: David Beier
Chris Jennings
Sally Katzen
John Spotila

FROM: Peter Swire

DATE: August 10, 1999

RE: Status of Medical Privacy Regulations

Here is an update on the progress of the medical privacy regulation. In summary:

(1) The Working Group is meeting 1:00 to 5:00 every Tuesday and Thursday for about two or three more weeks. They are moving through the issues papers at a faster rate than before. Lisa Rovin says that she is assigning drafting wherever possible, on parallel tracks. I have asked Lisa for a list of who is writing what sections and with what deadlines, but she politely said that HHS has decided to keep that information within HHS.

(2) I have worked with Lisa to identify non-HHS issues. This memorandum explains the progress made in the past week or so with: Justice (including Bureau of Prisons), Veterans, Defense, State, and CIA. I am also briefing the Office of Science and Technology Policy and the Statistical Policy branch on research-related issues.

(3) Attached is the list HHS has provided of "deputies." It is sketchy, and I question whether some of the people are senior enough to speak for their department.

(4) The biggest issue for you is what to do next with Justice. As explained below, we need a political call of what we are trying to achieve and how to achieve it.

Agency-by-Agency Situation.

Justice. HHS (Gary Claxton and Lisa Rovin) and I are confused what EOP wants to do on the issue of law enforcement access. According to Lisa, Ian De Waal of DOJ has already agreed to the parts of the Jennings letter to Jeffords that fit within HIPAA jurisdiction. What more are we looking for? If there is supposed to be a Deputies meeting soon with Justice, what is the agenda and plan for action? HHS and I need more guidance before we can suggest detailed recommended positions, and the political decision of what to ask for seems central.

Also at Justice, I identified people from the Bureau of Prisons to work with the Working Group. The Secretary's recommendation had been to exempt prisoners from the rule, although apparently to continue to allow prisoners to exercise their access rights under the Privacy Act. The Working Group was initially inclined to give prisoners broader rights, and BOP officials

raise the issue to the AG's office. I expressed concerns to Lisa Rovin about over-regulating prisons: (a) our constitutional authority to regulate state and local prisons is doubtful; and (b) the substance and politics of limiting prison authorities' use of medical records is doubtful. Lisa said she would talk privately with BOP to try to head off any problems.

Veterans. The Secretary's recommendation was to allow the two components of VA (Veterans Benefit Administration and Veterans Health Administration) to act for purposes of the reg as if they were a single organization. VA needs to write the reg language to implement this recommendation.

I spoke at length with Jeff Corzatt in the General Counsel's office, and they are now working on this. The Working Group representatives for VA are new to the task, Mechelle Powell and Barbara Millas. In the list from HHS, the deputy named is Thomas Garthwaite, who is the Acting Undersecretary for Health at VHA.

David Beier mentioned his possible interest in working with VA. For now, they seem to be working on their drafting.

Defense. DOD has participated actively and helpfully in the Working Group, represented by Dr. Frances Stewart and Vahan Moushegian. Dr. Stewart has drafted reg language for active duty personnel who are posted overseas, and whose medical records must be available to commanding officers. She has shared that language with HHS and me while it continues in clearance within DOD. She and I have talked at some length to try to identify other areas where DOD may wish to have special language. So far, she has agreed to: (a) contact NSA to learn of special concerns; and (b) work on special language for overseas child protective services, which occur outside of state law.

The DAS above Stewart is Dr. John Mazzuchi. Dr. Stewart has warned that his schedule is extremely tight, and that it often takes a week or more to brief him and get him scheduled. The Assistant Secretary in the health area is Dr. Bailey, who is now in Kosovo and whose schedule is even worse.

State. The State Department has overseas issues comparable to DOD. Until today, they knew nothing about the HHS reg. I am now in touch with Julie Herr in the Legal Advisor's office, and we will make sure that their issues become part of the process.

CIA. Attached is a short memo, requested by you, about how the CIA fits in with the proposed regulation, and including the relevant language from the Jeffords bill.

If I do not hear otherwise in the next couple of days, I will contact the CIA to bring them into the process in the same sort of way as DOD, State, and the other agencies.

Department	Contact	Title	Telephone	Pager
Commerce	Dawn Friedkin	Special Assistant Secretary General Counsel	(202) 482-0074	
Defense	John Mazzuchi	Deputy Asst. Secretary for Clinical and Program Policy	(703) 681-1708	
FTC	Jody Bernstein	Director, Bureau of Consumer Protection		
HHS	Gary Claxton	Deputy Asst. Secretary for Planning and Evaluation	(202) 690-6870	
	Jane Horvath	Deputy Asst. Secretary for Legislation	(202) 690-7450	
	Marcy Wilder	Deputy General Counsel	(202) 690-6318	
Justice	John Bentivoglio	Criminal Division	(202) 514-2707	(888) 415-4725
	Kathy Hawk Sawyer	Director, Federal Bureau of Prisons		
Labor	Leslie Kramerich	Deputy Asst. Secretary, PWBA	(202) 219-8233	
OPM	Janice Lachance	Director, OPM	(202) 606-1100	
SSA	Sue Davis	Director, Disability Redesign	(410) 966-6491	(888) 802-4943
	Susan Daniels	Deputy Commissioner for Disability and Income Security Programs		
VHA	Thomas Garthwaite	Acting Undersecretary for Health, VHA	(202) 273-5878	

Peter Swire
Lauren Steinfeld
August 10, 1999

Briefing Paper on Application of Medical Privacy Regulations to CIA

This briefing paper examines: the CIA's 1997 comments on the Secretary's recommendations; the CIA-related provisions in the Jeffords bill, and the treatment of the CIA under the Privacy Act. The next step is to include the CIA in the Working Group to implement these recommendations.

1. CIA's Prior Comments to Secretary's Recommendations (9/9/97):

   a. The CIA did not request an exemption from legislation, but rather asked for easy access to medical records and freedom to reuse and disclose.

   b. In commenting on the Secretary's Recommendations in 1997, the CIA submitted non-classified proposed changes, which were all accepted. The relevant changes were to add, in the "Law Enforcement" section (p. 60),

      i. an additional category of permissible disclosures without patient authorization:

         "upon the request of an official of the U.S. Intelligence Community, as defined in National Security Act, 50 U.S.C. 401a, who states that the information requested is needed for a lawful purpose."

      ii. that the Intelligence Community and law enforcement have no restrictions on further use or disclosure, except as provided by other law.

2. Jeffords Bill Exempts the CIA from Disclosure Requirements

   * The relevant sections allow the Director to, by regulation, disclose protected health information about officers, employees, and contractors as necessary for lawful intelligence purposes under the National Security Act of 1947. See Attachment.

3. The CIA and the Privacy Act

   * The CIA is permitted to exempt itself from the access provisions (and related provisions) of the Act (Section 552a(j)) and does so on a case-by-case basis.

   * Further, much of the information collected by the CIA may not be covered by the Privacy Act, which covers only citizens and aliens lawfully admitted for

permanent residents.

Attachment

Language from Jeffords Bill Re: CIA Exception

(A) Exceptions.– The Director of the Central Intelligence Agency, may, by regulation, establish exceptions to the disclosure requirements of this Act to the extent that the Director determines that disclosure of the protected health information, relating to officers and employees of the Central Intelligence Agency and contractors of such Agency, is necessary to the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947 (50 U.S.C 401 et seq).

(B) Application to Officers, Employees and Contractors.– The Director of the Central Intelligence Agency may, by regulation, establish for officers, employees and contractors of the Central Intelligence Agency, limitations on the rights of such persons to revoke or amend authorizations for disclosures under section 203 when such authorizations were provided by such officers, employees and contractors as a condition of employment or contract and the disclosure is determined necessary by the Director to the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947 (50 U.S.C 401 et seq).

THE NEED FOR LEGISLATION

It has been 25 years since former HEW Secretary Elliot Richardson set forth principles that led to the landmark Federal Privacy Act. Those 25 years have brought vast changes in our health care system.

Revolutions in our health care delivery system mean that we must place our trust in entire networks of insurers and health care professionals - both public and private. The computer and telecommunications revolutions mean that information no longer exists in one place - it can travel in real time to many hospitals, physicians, insurers, and across state lines.

In addition, revolutions in biology mean that a whole new world of genetic tests have the potential to either help prevent disease or reveal the most personal health information of a family. Without safeguards to assure citizens that getting tested will not endanger their families' privacy or health insurance, we could endanger one of the most promising areas of research our nation has ever seen.

Health care privacy can be safeguarded. It must be done with national legislation, national education, and an on-going national conversation.

Currently, when we give a physician or health insurance company precious health information, the level of protection will vary widely from state to state. We have no comprehensive federal health information privacy standards. Because the practice of health care is increasingly becoming interstate through mergers, complex contractual relationships and enhanced telecommunications, we can no longer rely on the existing patchwork of state laws. The patchwork does not provide Americans the privacy protections they need or expect. The Congress should seize upon this opportunity to create strong federal standards and reassure the public that they can trust their providers and insurers to keep their health information secure.

In developing our recommendations for federal legislation, we learned a great deal through consultations with a variety of outside groups and from six days of public hearings conducted by the National Committee on Vital and Health Statistics, our statutory federal advisory committee for health data and privacy policy. The hearings involved over 40 witnesses from across the health community, including health care professionals, plans, insurance companies, the privacy community, and the public health and research communities.

We believe our recommendations provide a balanced framework for legislation that can protect the privacy of medical records, guarantee consumers the right to inspect their records, and punish unauthorized disclosures of personal health data by hospitals, insurers, health plans, drug companies or others.

THE PRINCIPLES

The Secretary's recommendations for legislation are grounded in five key principles: Boundaries, Security, Consumer Control, Accountability, and Public Responsibility.

Boundaries

The first is the principle of Boundaries: With very few exceptions, personally identifiable health care information should be disclosed for health purposes and health purposes only. It should be easy to use it for those purposes, and very difficult to use it for other purposes.

For example, employers should be able to use the information furnished by their employers to provide on-site care or to administer a health plan in the best interests of those employees. But those same employers should not be able to use information obtained for health care purposes to discriminate against individuals when making employment decisions - such as hiring, firing, placements and promotions. To enforce these boundaries, we recommend strong penalties for the inappropriate use or disclosure of medical records.

We recommend that the legislation apply specifically to providers and payers, and to anyone who receives health information from a provider or payer, either with the authorization of the patient or as authorized explicitly by legislation.

However, our recommendations acknowledge that these providers and payers do not act alone. In order for a provider or payer to operate efficiently, it may need to enlist a service organization to perform an administrative or operational function. For example, a hospital may hire an organization to encode and process bills, or a managed care organization may contract with a pharmaceutical benefit management company to provide information to pharmacists about what medications are covered and appropriate for their customers.

The numbers and types of service organizations are increasing every day. While most do not have direct relationships with the patients, they do have access to their personal health care information. Therefore, we recommend that they should be bound by the same standards. For example, a health plan's contractor should be allowed to have access to patient lists in order to do mailings to remind patients to schedule appointments for preventive care. But it should not be able to sell the patient lists to a pharmaceutical company for a direct mailing announcing a new product.

Because we recommend a minimum floor of protection for all records, our report does not distinguish among types of health care information based on sensitivity. For example, our recommendations do not include specific provisions related to genetic information in health records.

Genetic information should be covered by the same rules. However, we recognize that the public is especially concerned about the unique properties of genetic information - its predictive nature, and its link to personal identity and kinship and its ability to reveal our family secrets.

Therefore while you are developing privacy legislation, you should also consider how to limit the collection and disclosure of genetic information and prohibit health insurers and employers from discriminating against individuals on the basis of their genetic information. Because of the

speedy development of genetic technologies and its potential for abuse, we recommend that legislation concerning discrimination in underwriting by insurers or other improper use of such information be considered expeditiously. We look forward to continuing our work with you on this issue.

Security

The second principle is Security. Americans need to feel secure that when they give out personal health care information, they are leaving it in good hands. Information should not be used or given out unless either the patient authorizes it or there is a clear legal basis for doing so.

There are many different ways that private information like your blood tests could become public. People who are allowed to see it - such as lab technicians - can misuse it either carelessly or intentionally. And people who should not be seeing it - such as marketers - can find a way to access it, either because the organization holding the information doesn't have proper safeguards or the marketers can find an easy way around the safeguards. To give Americans the security they expect and deserve, Congress should develop legislation that requires those who legally receive health information to take reasonable steps to safeguard it and face consequences for failure to do so.

What do we mean by reasonable steps? The organizations should adopt protective administrative and management techniques, educate their employees, and impose disciplinary sanctions against employees who use information improperly.

We are addressing some of these steps in our Security Standards regulation, implementing the Administrative Simplification mandate under HIPAA. Our NPRM laid out a range of approaches for safeguarding the information to which the HIPAA mandate applies. However, that regulation will only cover the security of specific electronically maintained records. We need comprehensive privacy legislation to cover all health information that needs this kind of protection.

We don't believe a law can specify the details of these protections because each organization must keep pace with the new threats to our privacy and the technology that can either abate or exacerbate them. But a federal law can require everyone who holds health information to have these types of safeguards in place and specify the appropriate sanctions if the information is improperly disclosed.

Consumer Control

The third principle is Consumer Control. The principles of fair information practice (formulated in 1973 by a committee appointed by Secretary Richardson) included as a basic right: "There must be a way for an individual to find out what information about him is in a record and how it is used."

With very narrow exceptions, consumers should have the right to find out what is contained in

their records, find out who has looked at them, and to inspect, copy and, if necessary, correct them. Consumers should be given a clear explanation of these rights and they should understand how organizations will use their information. Let me give you an example of why this is important. According to the Privacy Rights Clearinghouse, a California physician in private practice was having trouble getting health, disability, and life insurance. She ordered a copy of her report from the Medical Information Bureau - an information service used by many insurance companies. It included information showing that she had a heart condition and Alzheimer's disease. There was only one problem. None of it was true. Unfortunately, under the current system these types of errors occur all too often. Consumers often do not have access to their own health records and even those who do are not always able to correct some of the most egregious errors.

With that in mind, our recommendations set forth a set of practices and procedures that would require that insurers and health care providers provide consumers with a written explanation detailing who has access to their information and how that information will be used, how they can restrict or limit access to it, and what their rights are if their information is disclosed improperly.

We also recommend procedures for patients to inspect and copy their information, and set out the very limited circumstances under which patient inspection should be properly denied.

Finally, we recommend a process for patients to seek corrections or amendments to their health information to resolve situations in which innocent coding errors cause patients to be charged for procedures they never received, or to be on record as having conditions or medical histories that are inaccurate.

Accountability

The fourth principle is Accountability. If you are using information improperly, you should be punished. This flows directly from the second principle of security - the requirement to safeguard information must be followed by real and severe penalties for violations. Congress should send the message that protecting the confidentiality of health information is vitally important, and that people who violate that confidence will be held accountable.

We recommend that offenders should be subject to criminal felony penalties if they knowingly obtain or use health care information in violation of the standards outlined in our report. The penalties mandated in privacy legislation should be higher when violations are for monetary gain, similar to those Congress mandated in the administrative simplification provisions of HIPAA. In addition, when there is a demonstrated pattern or practice of unauthorized disclosure, those committing it should be subject to civil monetary penalties.

In addition to punishing the perpetrators, we must give redress to the victims. We believe that any individual whose privacy rights have been violated - whether those rights were violated negligently or knowingly - should be permitted to bring a legal action for actual damages and equitable relief. When the violation is done knowingly, attorney's fees and punitive damages

should be available.

These first four principles - Boundaries, Security, Consumer Control and Accountability - must be carefully weighed against the fifth principle, Public Responsibility.

Public Responsibility

Just like our free speech rights, privacy rights can never be absolute. We have other critical - yet often competing - interests and goals. We must balance our protections of privacy with our public responsibility to support national priorities - public health and safety, research, quality care, and our fight against health care fraud and abuse and other unlawful activities.

Our Department is acutely aware of the need to use personal health information for each of these national priorities. For example, HHS auditors use health records to uncover kickbacks, overpayments and other fraudulent activity. Researchers have used health records to help us fight childhood leukemia and uncover the link between DES and reproductive cancers. Public health agencies use health records to warn us of outbreaks of emerging infectious diseases. In addition, our efforts to improve quality in our health care system depend on our ability to review health information to determine how well health institutions and health professionals are caring for patients.

For public health and safety, research, quality evaluations, fraud investigations, and legitimate law enforcement purposes, it's not always possible, or desirable, to ask for each patient's permission for access to the necessary health information. And, in many cases, doing so could create major obstacles in our efforts. While we must be able to use identifiable information when necessary for these purposes, we should use information that is not identifiable as much as possible.

To demonstrate how access must be balanced against public responsibility, let me outline a few of the areas in which we recommend that disclosure of health information should be permitted without patient authorization.

Public Health

Under certain circumstances, we recommend permitting health care professionals, payers, and those receiving information from them to disclose health information without patient authorization to public health authorities for disease reporting, adverse event reporting, public health investigation, or intervention. This is currently how the public health system operates under existing State and federal laws.

For example, consider the outbreak of E. coli in hamburger that resulted in the largest recall of meat products in history. Public health authorities, working with other officials, used personally identifiable information to identify quickly the source of the outbreak and thereby prevent thousands of other Americans from being exposed to a contaminated product.

Research

An important mission for the Department of Health and Human Services is to fund and conduct health research. We understand that research is vitally important to our health care and to progress in medical care. Legislation should not impede this activity.

Today the Federal Policy for Protection of Human Subjects and FDA's Human Subject Regulations protect participants in most research studies that are funded or regulated by the federal government. These rules have worked well to protect the privacy of individuals while not impeding the conduct of research. We recommend that similar privacy protections should be extended to all research in which individually identifiable health information is disclosed, and not just federally funded or regulated research.

All researchers must determine whether their research requires the retention of personal identifiers. There are research studies that can only be conducted if identifiers are retained; for example, outcomes studies for heart attack victims or the recent study which identified a correlation between the incidence of Sudden Infant Death Syndrome and the infant's sleep position. If, and when, personal identifiers are no longer needed, the researcher should be required to remove them and provide assurances that the information will be protected from improper use and unauthorized additional disclosures.

Under the Common Rule, if personal identifiers are necessary, an IRB must review the research proposal and determine whether informed consent is required or may be waived. In order for informed consent to be waived, an IRB must determine that the research involves no more than minimal risk to participants, that the absence of informed consent will not adversely affect the rights or welfare of participants, and that conducting the research would be impracticable if consent were required. This or a similar mechanism of review should be applicable for all research using individually identifiable health information without informed consent regardless of funding source.

This recommendation is consistent with the Federal Policy for the Protection of Human Subjects as well as the Privacy Act - policies that have protected federal research participants and research records for a quarter of a century and that have saved lives and fostered countless improvements in medical treatment.

PREEMPTION

Our recommendations call for national standards. But, we do not recommend outright or overall federal preemption of existing State laws that are more protective of health information.

Some protections that we recommend may be stronger than some existing State laws. Therefore, we recommend that Federal legislation replace State law only when the State law is less protective than the Federal law. Thus, the confidentiality protections provided would be cumulative and the Federal legislation would provide every American with a basic set of rights with respect to health information.

CONCLUSION

Mr. Chairman, the five principles embodied in our recommendations - Boundaries, Security, Consumer Control, Accountability, and Public Responsibility - should guide a comprehensive law that will create substantive federal standards and provide our citizens with real peace of mind.

The principles represent a practical, comprehensive and balanced strategy to protect health care information that is collected, shared, and used in an increasingly complex world.

In addition to creating new federal standards, we must ensure that every single person who comes in contact with health care information understands why it is important to keep the information safe, how it can be kept safe, and what will be the consequences for failing to keep it safe. Most of all, we must help consumers understand not just their privacy rights, but also their responsibilities to ask questions and demand answers - to become active participants in their health care.

MEMORANDUM

TO: David Beier
Chris Jennings
Sally Katzen
John Spotila

FROM: Peter Swire

DATE: August 10, 1999

RE: Status of Medical Privacy Regulations

Here is an update on the progress of the medical privacy regulation. In summary:

(1) The Working Group is meeting 1:00 to 5:00 every Tuesday and Thursday for about two or three more weeks. They are moving through the issues papers at a faster rate than before. Lisa Rovin says that she is assigning drafting wherever possible, on parallel tracks. I have asked Lisa for a list of who is writing what sections and with what deadlines, but she politely said that HHS has decided to keep that information within HHS.

(2) I have worked with Lisa to identify non-HHS issues. This memorandum explains the progress made in the past week or so with: Justice (including Bureau of Prisons), Veterans, Defense, State, and CIA. I am also briefing the Office of Science and Technology Policy and the Statistical Policy branch on research-related issues.

(3) Attached is the list HHS has provided of "deputies." It is sketchy, and I question whether some of the people are senior enough to speak for their department.

(4) The biggest issue for you is what to do next with Justice. As explained below, we need a political call of what we are trying to achieve and how to achieve it.

Agency-by-Agency Situation.

Justice. HHS (Gary Claxton and Lisa Rovin) and I are confused what EOP wants to do on the issue of law enforcement access. According to Lisa, Ian De Waal of DOJ has already agreed to the parts of the Jennings letter to Jeffords that fit within HIPAA jurisdiction. What more are we looking for? If there is supposed to be a Deputies meeting soon with Justice, what is the agenda and plan for action? HHS and I need more guidance before we can suggest detailed recommended positions, and the political decision of what to ask for seems central.

Also at Justice, I identified people from the Bureau of Prisons to work with the Working Group. The Secretary's recommendation had been to exempt prisoners from the rule, although apparently to continue to allow prisoners to exercise their access rights under the Privacy Act. The Working Group was initially inclined to give prisoners broader rights, and BOP officials

raise the issue to the AG's office. I expressed concerns to Lisa Rovin about over-regulating prisons: (a) our constitutional authority to regulate state and local prisons is doubtful; and (b) the substance and politics of limiting prison authorities' use of medical records is doubtful. Lisa said she would talk privately with BOP to try to head off any problems.

Veterans. The Secretary's recommendation was to allow the two components of VA (Veterans Benefit Administration and Veterans Health Administration) to act for purposes of the reg as if they were a single organization. VA needs to write the reg language to implement this recommendation.

I spoke at length with Jeff Corzatt in the General Counsel's office, and they are now working on this. The Working Group representatives for VA are new to the task, Mechelle Powell and Barbara Millas. In the list from HHS, the deputy named is Thomas Garthwaite, who is the Acting Undersecretary for Health at VHA.

David Beier mentioned his possible interest in working with VA. For now, they seem to be working on their drafting.

Defense. DOD has participated actively and helpfully in the Working Group, represented by Dr. Frances Stewart and Vahan Moushegian. Dr. Stewart has drafted reg language for active duty personnel who are posted overseas, and whose medical records must be available to commanding officers. She has shared that language with HHS and me while it continues in clearance within DOD. She and I have talked at some length to try to identify other areas where DOD may wish to have special language. So far, she has agreed to: (a) contact NSA to learn of special concerns; and (b) work on special language for overseas child protective services, which occur outside of state law.

The DAS above Stewart is Dr. John Mazzuchi. Dr. Stewart has warned that his schedule is extremely tight, and that it often takes a week or more to brief him and get him scheduled. The Assistant Secretary in the health area is Dr. Bailey, who is now in Kosovo and whose schedule is even worse.

State. The State Department has overseas issues comparable to DOD. Until today, they knew nothing about the HHS reg. I am now in touch with Julie Herr in the Legal Advisor's office, and we will make sure that their issues become part of the process.

CIA. Attached is a short memo, requested by you, about how the CIA fits in with the proposed regulation, and including the relevant language from the Jeffords bill.

If I do not hear otherwise in the next couple of days, I will contact the CIA to bring them into the process in the same sort of way as DOD, State, and the other agencies.

Department	Contact	Title	Telephone	Pager
Commerce	Dawn Friedkin	Special Assistant Secretary General Counsel	(202) 482-0074	
Defense	John Mazzuchi	Deputy Asst. Secretary for Clinical and Program Policy	(703) 681-1708	
FTC	Jody Bernstein	Director, Bureau of Consumer Protection		
HHS	Gary Claxton	Deputy Asst. Secretary for Planning and Evaluation	(202) 690-6870	
	Jane Horvath	Deputy Asst. Secretary for Legislation	(202) 690-7450	
	Marcy Wilder	Deputy General Counsel	(202) 690-6318	
Justice	John Bentivoglio	Criminal Division	(202) 514-2707	(888) 415-4725
	Kathy Hawk Sawyer	Director, Federal Bureau of Prisons		
Labor	Leslie Kramerich	Deputy Asst. Secretary, PWBA	(202) 219-8233	
OPM	Janice Lachance	Director, OPM	(202) 606-1100	
SSA	Sue Davis	Director, Disability Redesign	(410) 966-6491	(888) 802-4943
	Susan Daniels	Deputy Commissioner for Disability and Income Security Programs		
VHA	Thomas Garthwaite	Acting Undersecretary for Health, VHA	(202) 273-5878	

Peter Swire
Lauren Steinfeld
August 10, 1999

Briefing Paper on Application of Medical Privacy Regulations to CIA

This briefing paper examines: the CIA's 1997 comments on the Secretary's recommendations; the CIA-related provisions in the Jeffords bill, and the treatment of the CIA under the Privacy Act. The next step is to include the CIA in the Working Group to implement these recommendations.

1. CIA's Prior Comments to Secretary's Recommendations (9/9/97):

   a. The CIA did not request an exemption from legislation, but rather asked for easy access to medical records and freedom to reuse and disclose.

   b. In commenting on the Secretary's Recommendations in 1997, the CIA submitted non-classified proposed changes, which were all accepted. The relevant changes were to add, in the "Law Enforcement" section (p. 60),

      i. an additional category of permissible disclosures without patient authorization:

         "upon the request of an official of the U.S. Intelligence Community, as defined in National Security Act, 50 U.S.C. 401a, who states that the information requested is needed for a lawful purpose."

      ii. that the Intelligence Community and law enforcement have no restrictions on further use or disclosure, except as provided by other law.

2. Jeffords Bill Exempts the CIA from Disclosure Requirements

   * The relevant sections allow the Director to, by regulation, disclose protected health information about officers, employees, and contractors as necessary for lawful intelligence purposes under the National Security Act of 1947. See Attachment.

3. The CIA and the Privacy Act

   * The CIA is permitted to exempt itself from the access provisions (and related provisions) of the Act (Section 552a(j)) and does so on a case-by-case basis.

   * Further, much of the information collected by the CIA may not be covered by the Privacy Act, which covers only citizens and aliens lawfully admitted for

permanent residents.

Attachment

Language from Jeffords Bill Re: CIA Exception

(A) Exceptions.– The Director of the Central Intelligence Agency, may, by regulation, establish exceptions to the disclosure requirements of this Act to the extent that the Director determines that disclosure of the protected health information, relating to officers and employees of the Central Intelligence Agency and contractors of such Agency, is necessary to the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947 (50 U.S.C 401 et seq).

(B) Application to Officers, Employees and Contractors.– The Director of the Central Intelligence Agency may, by regulation, establish for officers, employees and contractors of the Central Intelligence Agency, limitations on the rights of such persons to revoke or amend authorizations for disclosures under section 203 when such authorizations were provided by such officers, employees and contractors as a condition of employment or contract and the disclosure is determined necessary by the Director to the conduct of lawful intelligence activities conducted pursuant to the National Security Act of 1947 (50 U.S.C 401 et seq).

Flawed Provision in HR 10 Threatens Enactment of Strong, Comprehensive Medical Records Privacy Legislation

Despite strong opposition from privacy advocates, the House has included a poorly-drafted medical privacy provision in the financial modernization bill (HR 10). This provision allows sensitive personal medical information to be given out without consent for a wide range of activities, including marketing research and insurance underwriting. Moreover, although this provision gives the false impression of providing broad privacy protections, it threatens the long overdue, strong, comprehensive medical records privacy legislation. In reality, the language fails to provide any meaningful protections, would override some of the basic privacy protections already established at the state level, and is opposed by over 50 consumer and provider advocacy groups, including the AARP, the American Medical Association, and the National Breast Cancer Coalition. Shortcomings of the bill include:

- **Large loopholes allow for inappropriate disclosure of information.** HR 10 allows personal health information to be distributed without consent for a wide range of activities, such as insurance underwriting and marketing research, without providing the necessary safeguards to ensure that information won't be misused. For example, an employer could receive private medical information from a health insurer in order to use it when making decisions about hiring or firing employees.

- **Unlimited disclosure of private medical information**. In addition to allowing disclosure without the consent of the patient, HR 10 does not place common-sense limitations on the scope of the information released. Health insurers requesting documentation that a procedure has been performed should not be given a patient's entire medical record.

- **No restrictions on the use of medical information**. Under HR 10, once an insurer has an individual's private medical information, it can use it for any purpose it wishes. Information received on an insurance application could be used to deny an application for a home mortgage or credit card, all without the patient's consent or knowledge.

- **No real consumer protections.** HR 10 fails to provide crucial consumer protections, including: an individuals' right to access their information; the right to know how information is used; and an assurance that sensitive medical information is safeguarded against inappropriate access.

- **No way to enforce even these insufficient protections.** HR 10 does not provide an avenue for individual's to seek redress if their personal medical information is misused. A right without a remedy is not truly a right. Strong, enforceable privacy legislation includes enforcement mechanisms that make the rights of individuals real.

Finally, the health care industry has been arguing for a single set of rules in order to avoid the significant burdens of complying with multiple regulatory standards. The provisions in HR 10 would conflict with the standards established under Federal regulatory authority by the Health Insurance Portability and Accountability Act (HIPAA). Because this burdensome conflict would dramatically impair the ability of health insurers to conduct business, HIAA and Blue Cross Blue Shield oppose these provisions.

PRESIDENT CLINTON TAKES STRONG NEW STEPS TO PROTECT THE PRIVACY OF PERSONAL HEALTH INFORMATION
October 29, 1999

President Clinton today will unveil a landmark set of privacy protections for electronic medical information stored or transmitted electronically. This new regulation, which the President is proposing because of Congress's failure to act, underscores the Administration's commitment to safeguarding the security of personal health information. But the President will note that because his regulatory authority is limited, comprehensive federal legislation is urgently needed, and he will urge Congress to enact broader privacy protections without further delay.

The new regulation that President Clinton and HHS Secretary Shalala are announcing today would apply to all health plans and many health care providers, as well as to health care clearinghouses such as billing companies. It would 1) limit the non-consensual use and release of private health information; 2) inform consumers about their right to access their records and to know who else has accessed them; 3) restrict the disclosure of protected health information to the minimum necessary; 4) establish new disclosure requirements for researchers and others seeking access to health records; and 5) establish new criminal and civil sanctions for the improper use or disclosure of such information.

THE AMERICAN PEOPLE WANT THE PRIVACY OF THEIR HEALTH RECORDS TO BE PROTECTED. Today, even amidst a boom in the collection and dissemination of personal data, patients do not have the right under Federal law to see their own health files or to know who is receiving their health information. Nor do they have basic protections to ensure that sensitive information is not inappropriately used or disclosed. Indeed, under the current loose patchwork of state laws, personal health information can be distributed -- without consent -- for reasons that have nothing to do with a patient's medical treatment. Patient information held by an insurer can in many cases be passed on to a lender who may then deny the patient's application for a home mortgage or a credit card, or to an employer who may use it in personnel decisions. Moreover, patients wishing to access or control the release of such information may be subject to the whim of their insurance company or health care provider.

PRESIDENT CLINTON UNVEILS NEW SAFEGUARDS FOR SENSITIVE HEALTH INFORMATION. The new regulation being unveiled today is designed to give consumers more control over their health information; set boundaries on the use and release of health records and ensure their security; establish accountability for inappropriate use and release; and balance public responsibility with privacy protections. This new regulation would:

GIVE CONSUMERS CONTROL OVER THEIR HEALTH INFORMATION

- **Limit the release of private health information without consent.** This rule would establish a new Federal requirement that doctors, hospitals, health plans, and other covered entities could not -- without a patient's written consent -- release identifiable health information for purposes unrelated to treatment, payment for services, or priorities like public health. Under the current regime, such data is often released to marketing firms, financial institutions, and employers, without knowledge or consent, and is then

used in direct marketing campaigns, in loan eligibility decisions, and for promotion and other purposes. In fact, a recent University of Illinois survey indicated that 35 percent of Fortune 500 companies check health records before they hire or promote.

- **Inform consumers how their health information is being used.** This new regulation will require health plans and providers to publish a notice to patients about how their information is being used and to whom it is being disclosed. It will also give each individual patient a right to a "disclosure history," listing the entities that have received information for purposes unrelated to treatment or payment.

- **Give patients access to their own health file and the right to request amendments or make corrections.** The regulation will give patients the right to see and copy their own records as well as the right to request correction of potentially harmful errors in their health files. These access and amendment rights are a core part of any regime to protect individual privacy. Without them, a person with an improper diagnosis in his or her medical file or payment record could be denied health insurance and left no redress.

SET BOUNDARIES ON MEDICAL RECORD USE AND RELEASE

- **Restrict the amount of information used and disclosed to the "minimum necessary."** Currently, health care providers and plans can often release a patient's entire health record even if an employer or other entity needs only particular information. This new regulation would restrict the information that is used and disclosed to the minimum amount of information necessary.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

- **Require the establishment of privacy-conscious business practices.** Sensitive information is often stored where it can be easily accessed. Earlier this year, for example, a major medical center inadvertently stored several thousand patient records on a public Internet site for two months. The regulation the President will announce today will require health plans and providers to establish internal procedures to protect the privacy of health records. They include: training employees about privacy considerations in the workplace; receiving complaints from patients on privacy issues; designating a "privacy officer" to assist patients with complaints and employees with questions; and ensuring that appropriate safeguards are in place for the protection of health information.

BALANCE PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

- **Require that information be disclosed only for research conducted responsibly.** Since health care research is an important public priority, under this rule researchers may obtain identifiable health information without prior consent if they certify to a provider or plan that an "institutional review board" or "privacy board" has reviewed the research protocol and determined that the research would meet certain privacy protection criteria.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORD USE AND RELEASE

- **Create new criminal and civil penalties for improper use or disclosure of information.** Currently, there is often no legal basis to prosecute individuals who inappropriately disclose private medical information. This rule creates new criminal penalties for intentional disclosure -- up to $50,000 and up to a year in prison. Disclosure with an intent to *sell* the data will be punishable with a fine of up to $250,000 and up to 10 years in prison. The regulation also establishes new civil penalties of $100 per person for unintentional disclosures and other violations (up to $25,000 per person per year).

NOW CONGRESS MUST ENACT COMPREHENSIVE LEGISLATION. The important new protections President Clinton will unveil today are a critical first step -- a step he is taking because Congress has failed to act in the three-year timeframe it gave itself in 1996. But the President's administrative authority is limited by statute and there remains an urgent need for comprehensive Federal privacy protections. Today's regulation, for instance, does not cover all paper records. It does not directly regulate many entities, including employers, other insurers, or public health agencies -- thus allowing for unlimited reuse of information by such entities. Federal legislation is also needed to fortify the penalties and to create a private right of action so that citizens can hold health plans and providers directly accountable for inappropriate and harmful disclosures of information. That is why President Clinton today will call on Congress to finish the job and enact the comprehensive protections that the American people want and need.

PRESIDENT CLINTON TAKES STRONG NEW STEPS TO PROTECT THE PRIVACY OF PERSONAL HEALTH INFORMATION
October 29, 1999

Today, President Clinton, together with HHS Secretary Shalala, will unveil a proposed regulation ~~that will~~ to establish strong new privacy protections for sensitive health information that is transmitted or maintained electronically. The new regulation would apply to all health plans, health care clearinghouses such as billing companies, and many health care providers. This rule would limit the use and release of private health information without consent; restrict the disclosure of protected health information to the minimum amount of information necessary; establish new requirements for disclosure of information to researchers and others seeking access to health records; inform consumers about their right to access their health records and to know who else has accessed them; and establish new administrative and criminal sanctions for the improper use or disclosure of private information. The important new protections established by this regulation are a critical first step, but limits on the Administration's statutory authority prevent us from directly regulating many entities, such as employers, who often receive sensitive information from health plans and providers. In addition, the regulation does not apply to information maintained only in paper, as opposed to electronic, form. For these reasons, the President will continues urge the Congress to pass comprehensive Federal legislation without delay.

THE PRIVACY OF INDIVIDUAL HEALTH RECORDS ARE NOT PROTECTED. Today, there is no comprehensive Federal requirement to provide patients with basic privacy protections such as the right to access their health file or to know to whom their health information is disclosed; nor are there basic protections to ensure that sensitive information is protected from inappropriate use or disclosure. Under the current loose patchwork of state laws, personal health information can often be distributed without consent for reasons that have nothing to do with a patient's treatment. Often, information held by an insurer can be passed on to a lender who can then deny that patient's application for a home mortgage or a credit card, or to an employer who uses it in personnel decisions. Personal health information may be disclosed for insurance underwriting purposes, for market research, or any other reason without any safeguards to protect it against misuse. In addition, patients wishing to access or control the release of such records may be subject to the whim of their insurance company, health care provider, or anyone else who holds their records. Today, the President will:

UNVEIL NEW PROTECTIONS FOR SENSITIVE HEALTH INFORMATION. The new regulation being unveiled today is designed to give consumers more control over their health information; set boundaries on the use and release of health records and ensure their security; establish accountability for inappropriate use and release; and balance public responsibility with protecting privacy. This new regulation would:

GIVE CONSUMERS CONTROL OVER THEIR HEALTH INFORMATION

- **Limit the release of private health information without consent.** This new regulation would establish the first Federal requirement that identifiable health information would generally not be released by doctors, hospitals, health plans, or other covered entities

without the written consent of the patient for purposes unrelated to treatment and payment for services or public priorities such as public health. Currently, private health information is often released to private marketing firms, financial institutions, and employers, without the knowledge or consent of the patient, and is used in direct marketing campaigns, in loan eligibility decisions, and for promotion and other personnel purposes. For example, a recent University of Illinois survey indicated that 35 percent of Fortune 500 companies check health records before they hire or promote.

- **Inform consumers about how their health information is being used.** This new regulation would require health plans and providers to notify patients about how their information is being used and who it is being disclosed to in two important ways. First, it will require the publication of a notice describing how the particular organization uses and discloses information in health records. Second, it will give each individual patient a right to a "disclosure history," listing the entities that received information from their file for purposes unrelated to treatment or payment.

- **Give patients access to their own health file and the right to request amendments or make corrections.** The regulations will give patients the right to see and copy their own records and a right to request that information in their health file be corrected if an error in the file could harm the individual. These access and amendment rights are a core part of any regime to protect individual privacy. Without these rules, a person with an improper diagnosis noted in his or her medical file or payment record could be denied health insurance and there would be no procedures to allow the person to address the inaccuracy.

SET BOUNDARIES ON MEDICAL RECORD USE AND RELEASE

- **Restrict the amount of information used and disclosed to the "minimum necessary."** This new regulation would restrict the information that is used and disclosed to the minimum amount of information necessary. Currently, health care providers and plans often may be able to release a patient's full health record to outside entities without justification. For instance, an employer requesting information to process claims for a work-related injury could be forwarded an employee's entire health record.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

- **Require the establishment of privacy conscious business practices.** The regulation being released today would require health plans and providers to establish internal procedures to protect the privacy of health records, including training employees about privacy considerations and operations in the workplace; receiving complaints from patients on privacy issues; designating a "privacy officer" to assist patients with complaints and employees with questions on how to abide by the entity's privacy procedures; and ensuring that appropriate safeguards are in place for the protection of health information. Currently, sensitive information is often stored where it can be easily accessed. For example, earlier this year, a major medical center inadvertently stored several thousand patient records on a public Internet site for two months.

BALANCE PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

- **Require that information be disclosed only for research that is conducted in a responsible manner.** Because health care research is an important public priority, researchers are allowed to obtain identifiable health information without the prior consent of the patient if they certify to a health care provider or health plan that an "institutional review board" or "privacy board" reviewed the research protocol and determined that the research would meet privacy criteria. For instance, the research must be of sufficient importance to outweigh the privacy intrusion to the individual whose information is being disclosed, and the researcher must have an adequate plan to protected identifiers from improper use and disclosure.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORD USE AND RELEASE

- **Create new criminal and civil penalties for improper use or disclosure of information.** These new regulations will establish new criminal penalties for intentional disclosure of up to $50,000 and up to 1 year imprisonment. Disclosure with an intent to sell the information will be punishable with a fine of up to $250,000 and up to 10 years in prison. The regulation will also establish new civil money penalties of $100 per person for unintentional disclosures and other violations (up to a maximum of $25,000 per person per year). Currently, there may be no legal basis to prosecute individuals who inappropriately disclose private information.

THE NEED FOR COMPREHENSIVE FEDERAL LEGISLATION REMAINS. Today, the President will stress the continuing need for Congress to pass comprehensive Federal legislation because of the statutory limits placed on his administrative authority by the Health Insurance Portability and Accountability Act. The regulation being released today does not: cover all paper records, which is still how older health records are stored; directly regulate employers, other insurers, public health agencies and other entities accessing information, placing an additional regulatory burden on health plans and providers and allowing for the unlimited reuse of information by these entities; inadequate penalties for violations; and it does not create the private right of action that would allow citizens to hold health plans and providers directly accountable for inappropriate and harmful disclosures of information.

Document No. [redacted]

WHITE HOUSE STAFFING MEMORANDUM

Date: 10/28/99 ACTION / CONCURRENCE / COMMENT DUE BY: ASAP

Subject: Departure Statement - Privacy Protections for Medical Records

	ACTION	FYI		ACTION	FYI
VICE PRESIDENT	✓	☐	LOCKHART	☐	✓
PODESTA	✓	☐	MARSHALL	✓	☐
ECHAVESTE	✓	☐	MOORE	☐	☐
RICCHETTI	✓	☐	NASH	☐	☐
LEW	☐	☐	NOLAN	☐	☐
BAILY	☐	☐	REED	✓	☐
BERGER	☐	☐	SOSNIK	✓	☐
BLUMENTHAL	☐	☐	SPERLING	☐	☐
BURSON	☐	☐	STEIN	☐	☐
CAHILL	☐	☐	STREETT	☐	☐
EDMONDS	✓	☐	TRAMONTANO	✓	☐
FRAMPTON	☐	☐	UCELLI	✓	☐
IBARRA	☐	☐	VERVEER	☐	☐
JOHNSON, B.	☐	☐	Eric Liu →	✓	☐
JOHNSON, J.	✓	☐	Chris Jennings	✓	☐
LANE	☐	☐	Peter Swire	✓	☐
LEWIS	✓	☐	Sally Katzen	✓	☐

REMARKS: Comments to Lawell Weiss x62734

RESPONSE:

Office of the Staff Secretary
Ext. 62702

'99 OCT 28 PM5:42

Draft 10/27/99 5:30p.m.
Lowell Weiss

PRESIDENT WILLIAM J. CLINTON
REMARKS UPON DEPARTURE
ON PRIVACY PROTECTIONS FOR MEDICAL RECORDS
THE WHITE HOUSE
October 29, 1999

Good morning. Today, I am pleased to announce new actions to give the American people the privacy protections they need at a time of great change in our medical system.

Every American has a right to know that his or her medical records are treated with the highest degree of privacy, protected at all times from falling into the wrong hands. And yet, as more and more of our medical records are stored electronically, the threats to our privacy have greatly increased.

To be sure, storing and transmitting medical records electronically is a remarkable application of information technology. Electronic records are not only cost-effective. They can save lives -- by helping doctors make much quicker and better-informed decisions, by helping to prevent dangerous drug interactions, by giving patients in rural areas the benefit of specialist care hundreds of miles away.

But, believe it or not, our electronic medical records are not protected in any way under federal law. Today, with the click of a mouse, personal health information can easily -- and legally -- be passed around without patients' consent ... to people who are not doctors ... for reasons that have nothing to do with patient care.

Let me give you just two examples. A recent survey showed that more than a third of all Fortune 500 companies reported that they check medical records before they hire or promote. We also have seen deeply disturbing reports that drug manufacturers have gained access to sensitive patient information for the purposes of marketing their products directly to consumers; patients who have gone to a doctor for a routine test will later receive a letter from a drug company touting treatments for their ailments.

Although legal, these are outrageous invasions of privacy. And today, I will put an end to them. I will honor my State of the Union pledge and use the full authority of this office to create the first comprehensive national standards for protection of medical records. These new standards were developed by Sec. Shalala and the Department of Health and Human Services. I want to thank them for their tireless work.

The new standards would apply to all electronic medical records -- and to all health plans. They would greatly limit the release of private health information without consent. They would require health plans to inform patients about how medical information is used and to whom it is disclosed. They would give patients the right to see their own health files and request corrections. They would require health plans and providers to strengthen internal safeguards. They would create new criminal and civil penalties for improper use or disclosure of information. These standards represent an unprecedented step toward putting Americans back in control of their own medical records.

The reason I am taking this step through executive order is because, quite simply, the leadership in Congress failed to live up to its responsibility to act. On this crucial issue, as in so many others, the leadership of Congress has let the American people down. Congress gave itself three full years in which to pass meaningful privacy protections. And yet, two months ago, that three-year deadline expired, giving me the authority to step in and take action myself.

Even though I have now done so, there are still some protections that we can give our families only with the help of Congress. For example, only through legislation can we cover all paper records and all employers. So today, I say to the Congressional leaders: America's families are still waiting for you to help protect them from new abuses in this Information Age. You owe the American people the peace of mind of comprehensive medical privacy legislation. Let's do this together. Let's make this a season of progress.

# # #