PRESIDENT CLINTON TAKES STRONG NEW STEPS TO PROTECT THE PRIVACY OF PERSONAL HEALTH INFORMATION
October 29, 1999
DRAFT – EMBARGOED UNTIL 10 PM

Today, President Clinton, together with HHS Secretary Shalala, will unveil a proposed regulation that will 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.

DRAFT – EMBARGOED UNTIL 10 PM

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.

DRAFT – EMBARGOED UNTIL 10 PM

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. Although the regulation allows plans and providers to use and share health information for health care purposes such as treatment and payment for services, it requires consent and creates barriers to prevent the use and sharing of information for purposes not related to health care. We would require the patient's consent for uses unrelated to health care, such as marketing, 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. However, we agree that it 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. It is extremely disappointing that Congress could not produce a bill within the three year deadline it imposed upon itself. We can no longer wait for action in this area. If Congress attempts to impose further delays, the President's senior advisors would recommend that he veto such legislation.

EXCESSIVE BURDEN AND COST IMPLICATIONS

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 the implementation of 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.

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.

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: 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.

UNDERMININING CURRENT PROTECTIONS

Q: When you announced these new privacy protections, you said that these new protections were an "unprecedented step toward putting Americans back in control of their own medical records". What is your response to the recent criticism by provider groups, advocates, and health insurance plans that this regulation has too many loopholes to be effective?

A: Under the proposed regulation, the use of medical records without consent is constrained to treatment, payment, and other health care priorities. In many cases, this strengthens current practice in that the consent form used today can often authorize a broad use of information without consent, and is designed to protect providers and plans much more than patients. In addition, the consent form represents one more regulatory burden that we thought was unnecessary. Having said this, if providers and other interested parties can make a compelling case that requiring an written authorization for treatment and payment provides additional protections for patients, we will modify the proposed regulation accordingly.

Outline: Proposed Standards for Privacy of Individually Identifiable Health Information

Statutory Requirement

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

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

Overview

The proposed rule would:

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

Scope

a. Entities covered by the proposed rule

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

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

- Protection would start when information becomes electronic, and would stay with the information as long as the information is in the hands of a covered entity.
  - -- Information becomes electronic either by being sent electronically as one of the specified Administrative Simplification transactions or by being maintained in a computer system.
  - -- The paper progeny of electronic information is covered; the information would not lose its protections simply because it is printed out of the computer.

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

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

General rules

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

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

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

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

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

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

* Except where the business partner is providing a treatment consultation or referral, we would require covered entities to enter into contracts with their business partners and

would require the contracts to include terms to ensure that the protected health information disclosed to a business partner remains confidential. Business partners would not be permitted to use or disclose protected health information in ways that would not be permitted of the covered entity itself. We use the contract as a tool for protecting information, because the HIPAA does not provide legislative authority for the rule to reach many such business partners directly.

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

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

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

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

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

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

Uses and disclosures with individual authorization

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

* We would prohibit covered entities from conditioning treatment or payment on the individual agreeing to disclose information for other purposes, and require the authorization form to state this prohibition.

* While the provisions of this proposed rule are intended to make authorizations for treatment and payment purposes unnecessary, some States may continue to require them. Generally, this rule would not supersede such State requirements. However:

-- the rule would impose a new requirement that such State-mandated authorizations must be physically separate from an authorization for other purposes described in this rule.
-- the authorization would have to meet the rule's requirements for the content of such authorizations (although a state law could require that an authorization contain additional provisions).

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

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

* Individuals could revoke an authorization.

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

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

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

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

Individual rights

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

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

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

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

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

Administrative requirements and policy development and documentation

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

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

* Covered entities would be required to have in place administrative systems, appropriate to the nature and scope of their business, that enable them to protect health information in accordance with this rule. Specifically, covered entities would be required to:
  -- designate a privacy official;
  -- provide privacy training to members of its workforce;
  -- implement safeguards to protect health information from intentional or accidental misuse;
  -- provide a means for individuals to lodge complaints about the entity's information practices, and maintain a record of any complaints; and
  -- develop a system of sanctions for members of the workforce and business partners who violate the entity's policies.

Scalability

We propose privacy standards that covered entities must meet, but leave the detailed policies and

procedures for meeting these standards to the discretion of each covered entity.

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

Preemption

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

Enforcement

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

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

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

What this proposed rule does not do

* The HIPAA limits the application of our proposed rule to the covered entities. It does not provide the authority for the rule to reach many entities that receive health information from these covered entities, so the rule cannot put in place appropriate restrictions on how such recipients of protected health information may use and re-disclose such information.
* Any provider who maintains a solely paper information system cannot be subject to these privacy standards.

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