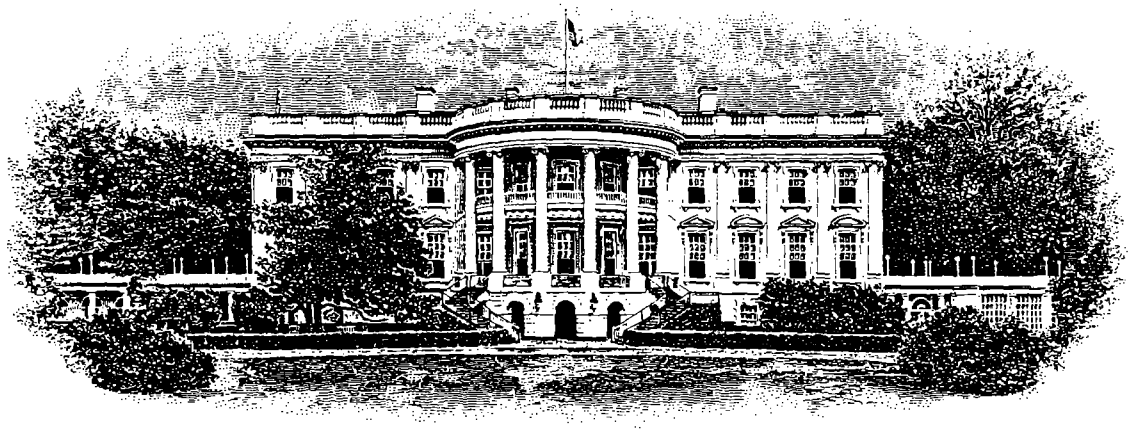
PRIVACY

pete.williams
@nbc.com

The White House



PHOTOCOPY
PRESERVATION

PRESIDENT CLINTON ISSUES STRONG NEW CONSUMER PROTECTIONS TO ENSURE THE PRIVACY OF MEDICAL RECORDS

December 20, 2000

Today, President Clinton will release a final regulation establishing the first-ever Federal privacy protections for the personal health information of all Americans. This rule, which applies to health insurers, virtually all health care providers and clearinghouses, will give consumers more control over and access to their health information; set boundaries on the use and release of health records; safeguard that information; establish accountability for inappropriate use and release; and balance privacy protections with public safety. The final regulation improves on the proposed rule by strengthening several key protections, including: extending protections to personal medical records in all forms – including paper records and oral communications; providing for written consent for routine use and disclosure of health records; protecting against unauthorized use of medical records for employment purposes; and ensuring that health care providers have all the information necessary to appropriately treat their patients.

THE PRIVACY OF INDIVIDUAL MEDICAL RECORDS ARE NOT CURRENTLY PROTECTED. Today, despite the increase in the collection and dissemination of personal data, there is no comprehensive Federal requirement to provide patients with basic privacy protections.

- **Americans are increasingly concerned about losing their privacy.** Recent studies show demonstrate a rising level of public concern about privacy; in 1999, over 80 percent of people surveyed agreed with the statement that they had "lost all control over their personal information."

- **Personal health information can be distributed without consent for reasons that are unrelated to treatment.** Under the current loose patchwork of state laws, 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.

- **Patients are often unable to access their own medical records.** In addition, patients wishing to access or control the release of such records may be unable to do so because of overwhelming barriers established by their insurance company, health care provider, or anyone else who holds their records.

PRESIDENT CLINTON TAKES FINAL ACTION NECESSARY TO IMPLEMENT NEW NATIONAL SAFEGUARDS FOR SENSITIVE HEALTH INFORMATION. The final regulation, which will be fully implemented within two years, is being issued under the authority of the bipartisan Health Insurance Portability and Accountability Act (HIPAA). This regulation, which underscores the Administration's commitment to safeguarding the security of personal health information, will:

GIVE CONSUMERS CONTROL OVER THEIR HEALTH INFORMATION

- **Inform consumers how their health information is being used.** This new regulation requires health plans and providers to inform patients about how their information is being used and to whom it is disclosed. It also gives each individual patient a right to a "disclosure history," listing the entities that received information unrelated to treatment or payment, that must be provided within 60 days.

- **Limit the release of private health information without consent.** This rule establishes a new Federal requirement for doctors treating patients and hospitals to obtain patients' written consent to use their health information even for routine purposes, such as treatment and payment. Other, non-routine disclosures would require separate, specific patient authorization.

- **Give patients access to their own health file and the right to request amendments or corrections.** The regulation gives 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 efforts to protect individual privacy. Without them, a person with an improper diagnosis in his or her medical file 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 often release a patient's entire health record even if an employer or other entity only needs specific information, such as the information necessary to process a worker's compensation claim. This new regulation restricts the information that is used and disclosed to the minimum amount necessary.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

- **Require the establishment of privacy-conscious business practices.** The regulation requires the establishment of 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 ensuring that appropriate safeguards are in place for the protection of health information. Many responsible doctors, hospitals and health plans already provide these common-sense services for their patients, and were instrumental in advocating for a national standard.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORD USE AND RELEASE

- **Create new criminal and civil penalties for improper use or disclosure of information.** In the past, there often has not been any legal basis to prosecute individuals who inappropriately disclose private medical information. This rule applies the standards included in HIPAA to create new criminal penalties for intentional disclosure – up to $50,000 and up to a year in prison. Disclosure with intent to sell the data is 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). Although these enforcement provisions will be helpful, they are no substitute for a private right of action, which makes it possible for patients to be compensated for harmful plan actions.

BALANCE PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

- **Require that information be disclosed only for public health priorities and other responsible research.** The regulation balances the need to protect the public health and support carefully monitored medical research against the need to protect personal medical records from misuse and abuse. The regulation recognizes that threats to public health, such as life-threatening and easily transmitted infectious diseases, will require appropriate monitoring by public health authorities. The regulation encourages health professionals to use de-identified records whenever possible.

- **Limit the disclosure of information without sacrificing public safety.** The rule strikes the proper balance between protecting privacy and meeting the needs of law enforcement. Medical records are often important to the investigation and prosecution of serious criminal activity. At the same time, Americans must not be discouraged from seeking health care because of concerns about having their information inappropriately given to others.

FINAL REGULATION INCLUDES KEY CHANGES TO STRENGTHEN PRIVACY PROTECTIONS. In response to over 50,000 comments submitted by the public, the final regulation being released today strengthens patient protection and control over their health information by:

- **Extending coverage to personal medical records in all forms – including paper records and oral communications.** The proposed regulation released last year was limited to electronic records and any paper records that previously existed in electronic form. The final regulation provides protection for paper and oral in addition to electronic information, creating a privacy system that covers all personal health information created or held by covered entities. Comments received on the proposed regulation affirmed that the Administration had the authority to extend coverage to paper records and overwhelmingly supported broadening the regulation to these records because it would be impractical to have two separate sets of privacy standards for different sets of records.

- **Requiring consent for routine use and disclosure of health records.** The proposed regulation released last year allowed routine disclosure of health information without advance consent for purposes of treatment, payment, and health care operations. The final regulation ensures that written consent for disclosures by front line providers– even routine ones – be obtained in advance. This new requirement was strongly supported by physician and patient advocacy groups.

- **Protecting against unauthorized use of medical records for employment purposes.** The proposed regulation did not clearly explain the regulation's limits on large self-insured employers' access to personal health information for employment or other purposes unrelated to health care without consent. The final regulation clarifies that these employers cannot access medical information for purposes unrelated to health care.

- **Ensuring that health care providers have all the information necessary to appropriately treat their patients.** For most disclosures of health information, such as health information submitted with bills, providers may send only the minimum information needed for the purpose of the disclosure. However, when treating patients, health care providers often need to be able to share more complete information with other providers. The final rule gives providers full discretion in determining what personal health information to include when sending patient records to other providers for treatment purposes.

FINANCIAL IMPACT OF IMPLEMENTATION OF PRIVACY REGULATION. Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress required that the overall financial impact of the HIPAA regulations reduce costs. As such, the financial assessment of the privacy regulation includes the ten-year $29.9 billion savings HHS projects for the recently released electronic claims regulation and the projected $17.6 billion in costs over 10 years projected for the privacy regulation. This produces a net savings of approximately $12.3 billion over 10 years for the health care delivery system while improving the efficiency as well as privacy protections.

PRESIDENT CLINTON CALLS ON THE CONGRESS TO ENACT PRIVACY LEGISLATION TO FINISH THE JOB. Today, President Clinton will once again call on Congress to finish the job on privacy. The regulation being finalized today represents a critical step towards protecting patient privacy that became necessary after Congress failed to act in the three-year timeframe it gave itself in 1996. However, the President's administrative authority is limited by statute and there remains an urgent need for Federal privacy protections to: strengthen penalties and to create a private right of action so citizens can hold health plans and providers accountable for inappropriate and harmful disclosures of information; extend privacy protections to cover other entities that routinely handle sensitive medical information, such as life insurers and worker's compensation programs; and to place appropriate limits on the re-use of medical information by other entities. Today the President is doing what he can in this area. He is issuing an Executive Order to limit the re-use and re-disclosure of certain medical records within the Federal government, but new legislation would be needed to extend these protections more broadly.

PRESIDENT CLINTON ISSUES STRONG NEW CONSUMER PROTECTIONS TO ENSURE THE PRIVACY OF MEDICAL RECORDS

December 20, 2000

Today, President Clinton will release a final regulation establishing the first-ever Federal privacy protections for the personal health information of all Americans. This rule, which applies to health insurers, virtually all health care providers and clearinghouses, will give consumers more control over and access to their health information; set boundaries on the use and release of health records; safeguard that information; establish accountability for inappropriate use and release; and balance privacy protections with public safety. The final regulation improves on the proposed rule by strengthening several key protections, including: extending protections to personal medical records in all forms – including paper records and oral communications; providing for written consent for routine use and disclosure of health records; protecting against unauthorized use of medical records for employment purposes; and ensuring that health care providers have all the information necessary to appropriately treat their patients.

THE PRIVACY OF INDIVIDUAL MEDICAL RECORDS ARE NOT CURRENTLY PROTECTED. Today, despite the increase in the collection and dissemination of personal data, there is no comprehensive Federal requirement to provide patients with basic privacy protections.

- **Americans are increasingly concerned about losing their privacy.** Recent studies show demonstrate a rising level of public concern about privacy; in 1999, over 80 percent of people surveyed agreed with the statement that they had "lost all control over their personal information."

- **Personal health information can be distributed without consent for reasons that are unrelated to treatment.** Under the current loose patchwork of state laws, 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.

- **Patients are often unable to access their own medical records.** In addition, patients wishing to access or control the release of such records may be unable to do so because of overwhelming barriers established by their insurance company, health care provider, or anyone else who holds their records.

PRESIDENT CLINTON TAKES FINAL ACTION NECESSARY TO IMPLEMENT NEW NATIONAL SAFEGUARDS FOR SENSITIVE HEALTH INFORMATION. The final regulation, which will be fully implemented within two years, is being issued under the authority of the bipartisan Health Insurance Portability and Accountability Act (HIPAA). This regulation, which underscores the Administration's commitment to safeguarding the security of personal health information, will:

GIVE CONSUMERS CONTROL OVER THEIR HEALTH INFORMATION

- **Inform consumers how their health information is being used.** This new regulation requires health plans and providers to inform patients about how their information is being used and to whom it is disclosed. It also gives each individual patient a right to a "disclosure history," listing the entities that received information unrelated to treatment or payment, that must be provided within 60 days.

- **Limit the release of private health information without consent.** This rule establishes a new Federal requirement for doctors treating patients and hospitals to obtain patients' written consent to use their health information even for routine purposes, such as treatment and payment. Other, non-routine disclosures would require separate, specific patient authorization.

- **Give patients access to their own health file and the right to request amendments or corrections.** The regulation gives 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 efforts to protect individual privacy. Without them, a person with an improper diagnosis in his or her medical file 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 often release a patient's entire health record even if an employer or other entity only needs specific information, such as the information necessary to process a worker's compensation claim. This new regulation restricts the information that is used and disclosed to the minimum amount necessary.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

- **Require the establishment of privacy-conscious business practices.** The regulation requires the establishment of 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 ensuring that appropriate safeguards are in place for the protection of health information. Many responsible doctors, hospitals and health plans already provide these common-sense services for their patients, and were instrumental in advocating for a national standard.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORD USE AND RELEASE

- **Create new criminal and civil penalties for improper use or disclosure of information.** In the past, there often has not been any legal basis to prosecute individuals who inappropriately disclose private medical information. This rule applies the standards included in HIPAA to create new criminal penalties for intentional disclosure – up to $50,000 and up to a year in prison. Disclosure with intent to sell the data is 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). Although these enforcement provisions will be helpful, they are no substitute for a private right of action, which makes it possible for patients to be compensated for harmful plan actions.

BALANCE PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

- **Require that information be disclosed only for public health priorities and other responsible research.** The regulation balances the need to protect the public health and support carefully monitored medical research against the need to protect personal medical records from misuse and abuse. The regulation recognizes that threats to public health, such as life-threatening and easily transmitted infectious diseases, will require appropriate monitoring by public health authorities. The regulation encourages health professionals to use de-identified records whenever possible.

- **Limit the disclosure of information without sacrificing public safety.** The rule strikes the proper balance between protecting privacy and meeting the needs of law enforcement. Medical records are often important to the investigation and prosecution of serious criminal activity. At the same time, Americans must not be discouraged from seeking health care because of concerns about having their information inappropriately given to others.

FINAL REGULATION INCLUDES KEY CHANGES TO STRENGTHEN PRIVACY PROTECTIONS. In response to over 50,000 comments submitted by the public, the final regulation being released today strengthens patient protection and control over their health information by:

- **Extending coverage to personal medical records in all forms – including paper records and oral communications.** The proposed regulation released last year was limited to electronic records and any paper records that previously existed in electronic form. The final regulation provides protection for paper and oral in addition to electronic information, creating a privacy system that covers all personal health information created or held by covered entities. Comments received on the proposed regulation affirmed that the Administration had the authority to extend coverage to paper records and overwhelmingly supported broadening the regulation to these records because it would be impractical to have two separate sets of privacy standards for different sets of records.

- **Requiring consent for routine use and disclosure of health records.** The proposed regulation released last year allowed routine disclosure of health information without advance consent for purposes of treatment, payment, and health care operations. The final regulation ensures that written consent for disclosures by front line providers– even routine ones – be obtained in advance. This new requirement was strongly supported by physician and patient advocacy groups.

- **Protecting against unauthorized use of medical records for employment purposes.** The proposed regulation did not clearly explain the regulation's limits on large self-insured employers' access to personal health information for employment or other purposes unrelated to health care without consent. The final regulation clarifies that these employers cannot access medical information for purposes unrelated to health care.

- **Ensuring that health care providers have all the information necessary to appropriately treat their patients.** For most disclosures of health information, such as health information submitted with bills, providers may send only the minimum information needed for the purpose of the disclosure. However, when treating patients, health care providers often need to be able to share more complete information with other providers. The final rule gives providers full discretion in determining what personal health information to include when sending patient records to other providers for treatment purposes.

FINANCIAL IMPACT OF IMPLEMENTATION OF PRIVACY REGULATION. Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress required that the overall financial impact of the HIPAA regulations reduce costs. As such, the financial assessment of the privacy regulation includes the ten-year $29.9 billion savings HHS projects for the recently released electronic claims regulation and the projected $17.6 billion in costs over 10 years projected for the privacy regulation. This produces a net savings of approximately $12.3 billion over 10 years for the health care delivery system while improving the efficiency as well as privacy protections.

PRESIDENT CLINTON CALLS ON THE CONGRESS TO ENACT PRIVACY LEGISLATION TO FINISH THE JOB. Today, President Clinton will once again call on Congress to finish the job on privacy. The regulation being finalized today represents a critical step towards protecting patient privacy that became necessary after Congress failed to act in the three-year timeframe it gave itself in 1996. However, the President's administrative authority is limited by statute and there remains an urgent need for Federal privacy protections to: strengthen penalties and to create a private right of action so citizens can hold health plans and providers accountable for inappropriate and harmful disclosures of information; extend privacy protections to cover other entities that routinely handle sensitive medical information, such as life insurers and worker's compensation programs; and to place appropriate limits on the re-use of medical information by other entities. Today the President is doing what he can in this area. He is issuing an Executive Order to limit the re-use and re-disclosure of certain medical records within the Federal government, but new legislation would be needed to extend these protections more broadly.

PRESIDENT CLINTON ISSUES STRONG NEW CONSUMER PROTECTIONS TO ENSURE THE PRIVACY OF MEDICAL RECORDS

December 20, 2000

Today, President Clinton will release a final regulation establishing the first-ever Federal privacy protections for the personal health information of all Americans. This rule, which applies to health insurers, virtually all health care providers and clearinghouses, will give consumers more control over and access to their health information; set boundaries on the use and release of health records; safeguard that information; establish accountability for inappropriate use and release; and balance privacy protections with public safety. The final regulation improves on the proposed rule by strengthening several key protections, including: extending protections to personal medical records in all forms – including paper records and oral communications; providing for written consent for routine use and disclosure of health records; protecting against unauthorized use of medical records for employment purposes; and ensuring that health care providers have all the information necessary to appropriately treat their patients.

THE PRIVACY OF INDIVIDUAL MEDICAL RECORDS ARE NOT CURRENTLY PROTECTED. Today, despite the increase in the collection and dissemination of personal data, there is no comprehensive Federal requirement to provide patients with basic privacy protections.

- **Americans are increasingly concerned about losing their privacy.** Recent studies show demonstrate a rising level of public concern about privacy; in 1999, over 80 percent of people surveyed agreed with the statement that they had "lost all control over their personal information."

- **Personal health information can be distributed without consent for reasons that are unrelated to treatment.** Under the current loose patchwork of state laws, 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.

- **Patients are often unable to access their own medical records.** In addition, patients wishing to access or control the release of such records may be unable to do so because of overwhelming barriers established by their insurance company, health care provider, or anyone else who holds their records.

PRESIDENT CLINTON TAKES FINAL ACTION NECESSARY TO IMPLEMENT NEW NATIONAL SAFEGUARDS FOR SENSITIVE HEALTH INFORMATION. The final regulation, which will be fully implemented within two years, is being issued under the authority of the bipartisan Health Insurance Portability and Accountability Act (HIPAA). This regulation, which underscores the Administration's commitment to safeguarding the security of personal health information, will:

GIVE CONSUMERS CONTROL OVER THEIR HEALTH INFORMATION

- **Inform consumers how their health information is being used.** This new regulation requires health plans and providers to inform patients about how their information is being used and to whom it is disclosed. It also gives each individual patient a right to a "disclosure history," listing the entities that received information unrelated to treatment or payment, that must be provided within 60 days.

- **Limit the release of private health information without consent.** This rule establishes a new Federal requirement for doctors treating patients and hospitals to obtain patients' written consent to use their health information even for routine purposes, such as treatment and payment. Other, non-routine disclosures would require separate, specific patient authorization.

- **Give patients access to their own health file and the right to request amendments or corrections.** The regulation gives 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 efforts to protect individual privacy. Without them, a person with an improper diagnosis in his or her medical file 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 often release a patient's entire health record even if an employer or other entity only needs specific information, such as the information necessary to process a worker's compensation claim. This new regulation restricts the information that is used and disclosed to the minimum amount necessary.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

- **Require the establishment of privacy-conscious business practices.** The regulation requires the establishment of 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 ensuring that appropriate safeguards are in place for the protection of health information. Many responsible doctors, hospitals and health plans already provide these common-sense services for their patients, and were instrumental in advocating for a national standard.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORD USE AND RELEASE

- **Create new criminal and civil penalties for improper use or disclosure of information.** In the past, there often has not been any legal basis to prosecute individuals who inappropriately disclose private medical information. This rule applies the standards included in HIPAA to create new criminal penalties for intentional disclosure – up to $50,000 and up to a year in prison. Disclosure with intent to sell the data is 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). Although these enforcement provisions will be helpful, they are no substitute for a private right of action, which makes it possible for patients to be compensated for harmful plan actions.

BALANCE PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

- **Require that information be disclosed only for public health priorities and other responsible research.** The regulation balances the need to protect the public health and support carefully monitored medical research against the need to protect personal medical records from misuse and abuse. The regulation recognizes that threats to public health, such as life-threatening and easily transmitted infectious diseases, will require appropriate monitoring by public health authorities. The regulation encourages health professionals to use de-identified records whenever possible.

- **Limit the disclosure of information without sacrificing public safety.** The rule strikes the proper balance between protecting privacy and meeting the needs of law enforcement. Medical records are often important to the investigation and prosecution of serious criminal activity. At the same time, Americans must not be discouraged from seeking health care because of concerns about having their information inappropriately given to others.

FINAL REGULATION INCLUDES KEY CHANGES TO STRENGTHEN PRIVACY PROTECTIONS. In response to over 50,000 comments submitted by the public, the final regulation being released today strengthens patient protection and control over their health information by:

- **Extending coverage to personal medical records in all forms – including paper records and oral communications.** The proposed regulation released last year was limited to electronic records and any paper records that previously existed in electronic form. The final regulation provides protection for paper and oral in addition to electronic information, creating a privacy system that covers all personal health information created or held by covered entities. Comments received on the proposed regulation affirmed that the Administration had the authority to extend coverage to paper records and overwhelmingly supported broadening the regulation to these records because it would be impractical to have two separate sets of privacy standards for different sets of records.

- **Requiring consent for routine use and disclosure of health records.** The proposed regulation released last year allowed routine disclosure of health information without advance consent for purposes of treatment, payment, and health care operations. The final regulation ensures that written consent for disclosures by front line providers– even routine ones – be obtained in advance. This new requirement was strongly supported by physician and patient advocacy groups.

- **Protecting against unauthorized use of medical records for employment purposes.** The proposed regulation did not clearly explain the regulation's limits on large self-insured employers' access to personal health information for employment or other purposes unrelated to health care without consent. The final regulation clarifies that these employers cannot access medical information for purposes unrelated to health care.

- **Ensuring that health care providers have all the information necessary to appropriately treat their patients.** For most disclosures of health information, such as health information submitted with bills, providers may send only the minimum information needed for the purpose of the disclosure. However, when treating patients, health care providers often need to be able to share more complete information with other providers. The final rule gives providers full discretion in determining what personal health information to include when sending patient records to other providers for treatment purposes.

FINANCIAL IMPACT OF IMPLEMENTATION OF PRIVACY REGULATION. Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress required that the overall financial impact of the HIPAA regulations reduce costs. As such, the financial assessment of the privacy regulation includes the ten-year $29.9 billion savings HHS projects for the recently released electronic claims regulation and the projected $17.6 billion in costs over 10 years projected for the privacy regulation. This produces a net savings of approximately $12.3 billion over 10 years for the health care delivery system while improving the efficiency as well as privacy protections.

PRESIDENT CLINTON CALLS ON THE CONGRESS TO ENACT PRIVACY LEGISLATION TO FINISH THE JOB. Today, President Clinton will once again call on Congress to finish the job on privacy. The regulation being finalized today represents a critical step towards protecting patient privacy that became necessary after Congress failed to act in the three-year timeframe it gave itself in 1996. However, the President's administrative authority is limited by statute and there remains an urgent need for Federal privacy protections to: strengthen penalties and to create a private right of action so citizens can hold health plans and providers accountable for inappropriate and harmful disclosures of information; extend privacy protections to cover other entities that routinely handle sensitive medical information, such as life insurers and worker's compensation programs; and to place appropriate limits on the re-use of medical information by other entities. Today the President is doing what he can in this area. He is issuing an Executive Order to limit the re-use and re-disclosure of certain medical records within the Federal government, but new legislation would be needed to extend these protections more broadly.

FINAL REGULATION TO PROTECT MEDICAL RECORDS PRIVACY SUMMARY OF CHANGES		
PROVISION	**PROPOSED RULE**	**FINAL RULE**
Expanding the Scope of Protections	The proposed rule limited covered information to information that was or at one point was in electronic form.	The final rule covers all medical record information – including paper records and oral communications.
Strengthening Consent Provisions	The proposed rule did not require health care providers to obtain consent for the disclosure of protected health information for routine uses such as treatment, payment, or health care operations. The proposed rule was silent on providers providing protected health information to appropriate government agencies concerning individuals who are suspected of being victims of abuse, neglect or domestic violence.	The final rule requires health care providers to obtain written consent when disclosing information for any purpose. The final rule requires that health plans and providers attempt to determine patient preferences before disclosing information to someone involved in their care, a family member, or a disaster relief agency of the patient's location or condition. The final rule ensures that individuals who are suspected of being victims of abuse, neglect, or domestic violence are consulted before protected health information is released.
Ensuring that Providers Have the Information Necessary to Treat Their Patients	The proposed rule inadvertently limited the amount of information providers could send to other health care personnel treating a patient.	The final regulation does not apply the "minimum necessary" standard to information shared with other health care professionals for purposes of treatment.
Closing the Loophole for Employer Sponsored Health Plans	The proposed rule did not directly address employer access to protected health information held by employer-sponsored health plans.	The final regulation limits the information that employer-sponsored health plans can share with the employer to information necessary to administer the plan.

FINAL REGULATION TO PROTECT MEDICAL RECORDS PRIVACY SUMMARY OF CHANGES		
PROVISION	**PROPOSED RULE**	**FINAL RULE**
Providing Information to Patients in a Secure Manner	The proposed rule was silent on the manner in which confidential information should be communicated to patients.	The final rule requires that health plans and providers accommodate reasonable requests that information being sent to patients be handled in a manner that protects confidentiality. Health plans must accommodate these requests if the patient certifies that they are in danger if the request is not honored.
Strengthening Public Health Requirements	The proposed rule permits disclosure to individuals working under the direction of a public health authority without consent.	The final regulation narrows this exception to allow disclosure only to those individuals who are undertaking specific activities related to FDA requirements or product recalls.
Reducing the Burden on Business Associates	The proposed rule holds health plans and providers responsible for monitoring their business associates for privacy violations and holding them responsible when violations occur.	The final rule does not require monitoring and holds health plans and providers responsible only for known privacy violations.
Improving Notice of Information Practices	The proposed rule requires covered entities to inform patients of their actual information use practices.	The final rule allows covered entities to use standard language that describes all permitted or requires uses or disclosures.
Protecting the Public Safety	The proposed rule allowed disclosure of limited information to law enforcement officials to identify a suspected fugitive, witness or missing person.	The final rule clarifies the original proposal, stating that health plans and providers can alert law enforcement authorities if a patient admits to participating in a violent crime or escaping lawful custody. The final rule also permits health care providers to notify law enforcement officers of evidence of a crime.

December 20, 2000

Contact: HHS Press Office
(202) 690-6343

PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION
SUMMARY OF THE FINAL REGULATION

Overview: *Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. For many years, the confidentiality of those records was maintained by our family doctors, who kept our records sealed away in file cabinets and refused to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving large gaps in the protection of patients' privacy and confidentiality. There is a pressing need for national standards to control the flow of sensitive patient information and to establish real penalties for the misuse or disclosure of this information.*

President Clinton and Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). That law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. After three years of discussion in Congress without passage of such a law, HIPAA provided HHS with the authority to craft such privacy protections by regulation. Following the principles and policies laid out in the recommendations for national health information privacy legislation the Administration submitted to Congress in 1997, the Administration drafted regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records and the President and Secretary Donna E. Shalala released them in October of last year. During an extended comment period, HHS received, electronically or on paper, more than 52,000 communications from the public.

This final rule provides the first comprehensive federal protection for the privacy of health information. However, because of the limitations of the HIPAA statute, these protections do not fully achieve the Administration's goal of a seamless system of privacy protection for all health information. Members of both parties in Congress will need to pass meaningful, comprehensive privacy protection for American patients that would extend the reach of the standards being finalized today to all entities that hold personal health information.

COVERED ENTITIES

As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

INFORMATION PROTECED

All medical records and other individually identifiable health information held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally, is covered by the final regulation.

COMPONENTS OF THE FINAL RULE

The rule is the result of the Department's careful consideration of every comment and reflects a balance between accommodating practical uses of individually identifiable health information and rendering maximum privacy protection of that information.

CONSUMER CONTROL OVER HEALTH INFORMATION

Under this final rule, patients have significant new rights to understand and control how their health information is used.

- **Patient education on privacy protections.** Providers and health plans are required to give patients a clear written explanation of how they can use, keep, and disclose their health information.

- **Ensuring patient access to their medical records.** Patients must be able to see and get copies of their records, and request amendments. In addition, a history of most disclosures must be made accessible to patients.

- **Receiving patient consent before information is released.** Patient authorization to disclose information must meet specific requirements. Health care providers who see patients are required to obtain patient consent before sharing their information for treatment, payment, and health care operations purposes. In addition, specific patient consent must be sought and granted for non-routine uses and most non-health care purposes, such as releasing information to financial institutions determining mortgages and other loans or selling mailing lists to interested parties such as life insurers. Patients have the right to request restrictions on the uses and disclosures of their information.

- **Ensuring that consent is not coerced.** Providers and health plans generally cannot condition treatment on a patient's agreement to disclose health information for non-routine uses.

- **Providing recourse if privacy protections are violated.** People have the right to complain to a covered provider or health plan, or to the Secretary, about violations of the provisions of this rule or the policies and procedures of the covered entity.

BOUNDARIES ON MEDICAL RECORD USE AND RELEASE

With few exceptions, an individual's health information can be used for health purposes only.

- **Ensuring that health information is not used for non-health purposes.** Patient information can be used or disclosed by a health plan, provider or clearinghouse only for purposes of health care treatment, payment and operations. Health information cannot be used for purposes not related to health care – such as use by employers to make personnel decisions, or use by financial institutions – without explicit authorization from the individual.

- **Providing the minimum amount of information necessary.** Disclosures of information must be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the transfer of medical records for purposes of treatment, since physicians, specialists, and other providers need access to the full record to provide best quality care.

- **Ensuring informed and voluntary consent.** Non-routine disclosures with patient authorization must meet standards that ensure the authorization is truly informed and voluntary.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

The regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity. In this way, implementation of the standards will be flexible and scalable, to account for the nature of each entity's business, and its size and resources. Covered entities must:

- **Adopt written privacy procedures.** These must include who has access to protected information, how it will be used within the entity, and when the information would or would not be disclosed to others. They must also takes steps to ensure that their business associates protect the privacy of health information.

- **Train employees and designate a privacy officer.** Covered entities must provide sufficient training so that their employees understand the new privacy protections procedures, and designate an individual to be responsible for ensuring the procedures are followed.

- **Establish grievance processes.** Covered entities must provide a means for patients to make inquiries or complaints regarding the privacy of their records.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORDS USE AND RELEASE

Penalties for covered entities that misuse personal health information are provided in HIPAA.

- **Civil penalties.** Health plans, providers and clearinghouses that violate these standards would be subject to civil liability. Civil money penalties are $100 per incident, up to $25,000 per person, per year, per standard.

- **Federal criminal penalties.** There would be federal criminal penalties for health plans, providers and clearinghouses that knowingly and improperly disclose information or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

BALANCING PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

After balancing privacy and other social values, HHS is establishing rules that would permit certain existing disclosures of health information without individual authorization for the following national priority activities and for activities that allow the health care system to operate more smoothly. All of these disclosures have been permitted under existing laws and regulations. Within certain guidelines found in the regulation, covered entities may disclose information for:

- Oversight of the health care system, including quality assurance activities
- Public health
- Research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board
- Judicial and administrative proceedings
- Limited law enforcement activities
- Emergency circumstances
- For identification of the body of a deceased person, or the cause of death
- For facility patient directories
- For activities related to national defense and security

The rule permits, but does not require these types of disclosures. If there is no other law requiring that information be disclosed, physicians and hospitals will still have to make judgments about whether to disclose information, in light of their own policies and ethical principles.

SPECIAL PROTECTION FOR PSYCHOTHERAPY NOTES

Psychotherapy notes (used only by a psychotherapist) are held to a higher standard of protection because they are not part of the medical record and never intended to be shared with anyone else. All other health information is considered to be sensitive and treated consistently under this rule.

EQUIVALENT TREATMENT OF PUBLIC AND PRIVATE SECTOR HEALTH PLANS AND PROVIDERS. The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and government agency medical units must comply with the full range of requirements, such as providing notice, access rights, requiring consent before disclosure for routine uses, establishing contracts with business associates, among others.

CHANGES FROM THE PROPOSED REGULATION

- **Providing coverage to personal medical records in all forms.** The proposed regulation had applied only to electronic records and to any paper records that had at some point existed in electronic form. The final regulation extends protection to all types of personal health information created or held by covered entities, including oral communications and paper records that have not existed in electronic form. This creates a privacy system that covers virtually all health information held by hospitals, providers, health plans and health insurers.

- **Requiring consent for routine disclosures.** The final rule requires most providers to obtain patient consent for routine disclosure of health records, in addition to requiring special patient authorization for non-routine disclosures. The earlier version had proposed allowing these routine disclosures without advance consent for purposes of treatment, payment and health care operations (such as internal data gathering by a provider or health care plan). However, most individuals commenting on this provision, including many physicians, believed consent for these purposes should be obtained in advance, as is typically done today. The final rule retains the new requirement that patients must also be provided detailed written information on privacy rights and how their information will be used.

- **Allowing disclosure of the full medical record to providers for purposes of treatment.** For most disclosures, such as information submitted with bills, covered entities are required to send only the minimum information needed for the purpose of the disclosure. However, for purposes of treatment, providers need to be able to transmit fuller information. The final rule gives providers full discretion in determining what personal health information to include when sending patients' medical records to other providers for treatment purposes.

- **Protecting against unauthorized use of medical records for employment purposes.** Companies that sponsor health plans will not be able to access the personal health information held by the plan for employment-related purposes, without authorization from the patient.

COST OF IMPLEMENTATION

Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress provided in HIPAA 1996 that the overall financial impact of the HIPAA regulations reduce costs. As such, the financial assessment of the privacy regulation includes the ten-year $29.9 billion savings HHS projects for the recently released electronic claims regulation and the projected $17.6 billion in costs projected for the privacy regulation. This produces a net savings of approximately $12.3 billion for the health care delivery system while improving the efficiency of health care as well as privacy protection.

PRESERVING EXISTING, STRONG STATE CONFIDENTIALITY LAWS

Stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule sets a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information for civic purposes, we do not preempt these mandates. The result is to give individuals the benefit of all laws providing confidentiality protection as well as to honor state priorities.

THE NEED FOR FURTHER CONGRESSIONAL ACTION

HIPAA limits the application of our rule to the covered entities. It does not provide authority for the rule to reach many persons and businesses that work for covered entities or otherwise receive health information from them. So the rule cannot put in place appropriate restrictions on how such recipients of protected health information may use and re-disclose such information. There is no statutory authority for a private right of action for individuals to enforce their privacy rights. We need Congressional action to fill these gaps in patient privacy protections.

IMPLEMENTATION OF THE FINAL REGULATION

The final regulation will come into full effect in two years. The regulation will be enforced by HHS' Office for Civil Rights, which will provide assistance to providers, plans and health clearinghouses in meeting the requirements of the regulation – including a toll free line to help answer questions: 1-866-OCR-PRIV (1-866-627-7748). The TTY number is 1-866-788-4989. A Web site on the new regulation will also be available at *http://www.hhs.gov/ocr*.

# # #

Note: For other HHS Press Releases and Fact Sheets pertaining to the subject of this announcement, please visit our Press Release and Fact Sheet search engine at: *http://www.hhs.gov/search/press.html/*.

December 20, 2000

Contact: HHS Press Office
(202) 690-6343

PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION
SUMMARY OF THE FINAL REGULATION

***Overview**: Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. For many years, the confidentiality of those records was maintained by our family doctors, who kept our records sealed away in file cabinets and refused to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving large gaps in the protection of patients' privacy and confidentiality. There is a pressing need for national standards to control the flow of sensitive patient information and to establish real penalties for the misuse or disclosure of this information.*

President Clinton and Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). That law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. After three years of discussion in Congress without passage of such a law, HIPAA provided HHS with the authority to craft such privacy protections by regulation. Following the principles and policies laid out in the recommendations for national health information privacy legislation the Administration submitted to Congress in 1997, the Administration drafted regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records and the President and Secretary Donna E. Shalala released them in October of last year. During an extended comment period, HHS received, electronically or on paper, more than 52,000 communications from the public.

This final rule provides the first comprehensive federal protection for the privacy of health information. However, because of the limitations of the HIPAA statute, these protections do not fully achieve the Administration's goal of a seamless system of privacy protection for all health information. Members of both parties in Congress will need to pass meaningful, comprehensive privacy protection for American patients that would extend the reach of the standards being finalized today to all entities that hold personal health information.

COVERED ENTITIES

As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

INFORMATION PROTECED

All medical records and other individually identifiable health information held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally, is covered by the final regulation.

COMPONENTS OF THE FINAL RULE

The rule is the result of the Department's careful consideration of every comment and reflects a balance between accommodating practical uses of individually identifiable health information and rendering maximum privacy protection of that information.

CONSUMER CONTROL OVER HEALTH INFORMATION

Under this final rule, patients have significant new rights to understand and control how their health information is used.

- **Patient education on privacy protections.** Providers and health plans are required to give patients a clear written explanation of how they can use, keep, and disclose their health information.

- **Ensuring patient access to their medical records.** Patients must be able to see and get copies of their records, and request amendments. In addition, a history of most disclosures must be made accessible to patients.

- **Receiving patient consent before information is released.** Patient authorization to disclose information must meet specific requirements. Health care providers who see patients are required to obtain patient consent before sharing their information for treatment, payment, and health care operations purposes. In addition, specific patient consent must be sought and granted for non-routine uses and most non-health care purposes, such as releasing information to financial institutions determining mortgages and other loans or selling mailing lists to interested parties such as life insurers. Patients have the right to request restrictions on the uses and disclosures of their information.

- **Ensuring that consent is not coerced.** Providers and health plans generally cannot condition treatment on a patient's agreement to disclose health information for non-routine uses.

- **Providing recourse if privacy protections are violated.** People have the right to complain to a covered provider or health plan, or to the Secretary, about violations of the provisions of this rule or the policies and procedures of the covered entity.

BOUNDARIES ON MEDICAL RECORD USE AND RELEASE

With few exceptions, an individual's health information can be used for health purposes only.

- **Ensuring that health information is not used for non-health purposes.** Patient information can be used or disclosed by a health plan, provider or clearinghouse only for purposes of health care treatment, payment and operations. Health information cannot be used for purposes not related to health care – such as use by employers to make personnel decisions, or use by financial institutions – without explicit authorization from the individual.

- **Providing the minimum amount of information necessary.** Disclosures of information must be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the transfer of medical records for purposes of treatment, since physicians, specialists, and other providers need access to the full record to provide best quality care.

- **Ensuring informed and voluntary consent.** Non-routine disclosures with patient authorization must meet standards that ensure the authorization is truly informed and voluntary.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

The regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity. In this way, implementation of the standards will be flexible and scalable, to account for the nature of each entity's business, and its size and resources. Covered entities must:

- **Adopt written privacy procedures.** These must include who has access to protected information, how it will be used within the entity, and when the information would or would not be disclosed to others. They must also takes steps to ensure that their business associates protect the privacy of health information.

- **Train employees and designate a privacy officer.** Covered entities must provide sufficient training so that their employees understand the new privacy protections procedures, and designate an individual to be responsible for ensuring the procedures are followed.

- **Establish grievance processes.** Covered entities must provide a means for patients to make inquiries or complaints regarding the privacy of their records.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORDS USE AND RELEASE

Penalties for covered entities that misuse personal health information are provided in HIPAA.

- **Civil penalties.** Health plans, providers and clearinghouses that violate these standards would be subject to civil liability. Civil money penalties are $100 per incident, up to $25,000 per person, per year, per standard.

- **Federal criminal penalties.** There would be federal criminal penalties for health plans, providers and clearinghouses that knowingly and improperly disclose information or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

BALANCING PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

After balancing privacy and other social values, HHS is establishing rules that would permit certain existing disclosures of health information without individual authorization for the following national priority activities and for activities that allow the health care system to operate more smoothly. All of these disclosures have been permitted under existing laws and regulations. Within certain guidelines found in the regulation, covered entities may disclose information for:

- Oversight of the health care system, including quality assurance activities
- Public health
- Research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board
- Judicial and administrative proceedings
- Limited law enforcement activities
- Emergency circumstances
- For identification of the body of a deceased person, or the cause of death
- For facility patient directories
- For activities related to national defense and security

The rule permits, but does not require these types of disclosures. If there is no other law requiring that information be disclosed, physicians and hospitals will still have to make judgments about whether to disclose information, in light of their own policies and ethical principles.

SPECIAL PROTECTION FOR PSYCHOTHERAPY NOTES

Psychotherapy notes (used only by a psychotherapist) are held to a higher standard of protection because they are not part of the medical record and never intended to be shared with anyone else. All other health information is considered to be sensitive and treated consistently under this rule.

EQUIVALENT TREATMENT OF PUBLIC AND PRIVATE SECTOR HEALTH PLANS AND PROVIDERS. The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and government agency medical units must comply with the full range of requirements, such as providing notice, access rights, requiring consent before disclosure for routine uses, establishing contracts with business associates, among others.

CHANGES FROM THE PROPOSED REGULATION

- **Providing coverage to personal medical records in all forms.** The proposed regulation had applied only to electronic records and to any paper records that had at some point existed in electronic form. The final regulation extends protection to all types of personal health information created or held by covered entities, including oral communications and paper records that have not existed in electronic form. This creates a privacy system that covers virtually all health information held by hospitals, providers, health plans and health insurers.

- **Requiring consent for routine disclosures.** The final rule requires most providers to obtain patient consent for routine disclosure of health records, in addition to requiring special patient authorization for non-routine disclosures. The earlier version had proposed allowing these routine disclosures without advance consent for purposes of treatment, payment and health care operations (such as internal data gathering by a provider or health care plan). However, most individuals commenting on this provision, including many physicians, believed consent for these purposes should be obtained in advance, as is typically done today. The final rule retains the new requirement that patients must also be provided detailed written information on privacy rights and how their information will be used.

- **Allowing disclosure of the full medical record to providers for purposes of treatment.** For most disclosures, such as information submitted with bills, covered entities are required to send only the minimum information needed for the purpose of the disclosure. However, for purposes of treatment, providers need to be able to transmit fuller information. The final rule gives providers full discretion in determining what personal health information to include when sending patients' medical records to other providers for treatment purposes.

- **Protecting against unauthorized use of medical records for employment purposes.** Companies that sponsor health plans will not be able to access the personal health information held by the plan for employment-related purposes, without authorization from the patient.

COST OF IMPLEMENTATION

Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress provided in HIPAA 1996 that the overall financial impact of the HIPAA regulations reduce costs. As such, the financial assessment of the privacy regulation includes the ten-year $29.9 billion savings HHS projects for the recently released electronic claims regulation and the projected $17.6 billion in costs projected for the privacy regulation. This produces a net savings of approximately $12.3 billion for the health care delivery system while improving the efficiency of health care as well as privacy protection.

PRESERVING EXISTING, STRONG STATE CONFIDENTIALITY LAWS

Stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule sets a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information for civic purposes, we do not preempt these mandates. The result is to give individuals the benefit of all laws providing confidentiality protection as well as to honor state priorities.

THE NEED FOR FURTHER CONGRESSIONAL ACTION

HIPAA limits the application of our rule to the covered entities. It does not provide authority for the rule to reach many persons and businesses that work for covered entities or otherwise receive health information from them. So the rule cannot put in place appropriate restrictions on how such recipients of protected health information may use and re-disclose such information. There is no statutory authority for a private right of action for individuals to enforce their privacy rights. We need Congressional action to fill these gaps in patient privacy protections.

IMPLEMENTATION OF THE FINAL REGULATION

The final regulation will come into full effect in two years. The regulation will be enforced by HHS' Office for Civil Rights, which will provide assistance to providers, plans and health clearinghouses in meeting the requirements of the regulation – including a toll free line to help answer questions: 1-866-OCR-PRIV (1-866-627-7748). The TTY number is 1-866-788-4989. A Web site on the new regulation will also be available at *http://www.hhs.gov/ocr*.

# # #

Note: For other HHS Press Releases and Fact Sheets pertaining to the subject of this announcement, please visit our Press Release and Fact Sheet search engine at: *http://www.hhs.gov/search/press.html/*.

December 20, 2000

Contact: HHS Press Office
(202) 690-6343

PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION
SUMMARY OF THE FINAL REGULATION

Overview: *Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information. For many years, the confidentiality of those records was maintained by our family doctors, who kept our records sealed away in file cabinets and refused to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving large gaps in the protection of patients' privacy and confidentiality. There is a pressing need for national standards to control the flow of sensitive patient information and to establish real penalties for the misuse or disclosure of this information.*

President Clinton and Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). That law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. After three years of discussion in Congress without passage of such a law, HIPAA provided HHS with the authority to craft such privacy protections by regulation. Following the principles and policies laid out in the recommendations for national health information privacy legislation the Administration submitted to Congress in 1997, the Administration drafted regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records and the President and Secretary Donna E. Shalala released them in October of last year. During an extended comment period, HHS received, electronically or on paper, more than 52,000 communications from the public.

This final rule provides the first comprehensive federal protection for the privacy of health information. However, because of the limitations of the HIPAA statute, these protections do not fully achieve the Administration's goal of a seamless system of privacy protection for all health information. Members of both parties in Congress will need to pass meaningful, comprehensive privacy protection for American patients that would extend the reach of the standards being finalized today to all entities that hold personal health information.

COVERED ENTITIES

As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

INFORMATION PROTECED

All medical records and other individually identifiable health information held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally, is covered by the final regulation.

COMPONENTS OF THE FINAL RULE

The rule is the result of the Department's careful consideration of every comment and reflects a balance between accommodating practical uses of individually identifiable health information and rendering maximum privacy protection of that information.

CONSUMER CONTROL OVER HEALTH INFORMATION

Under this final rule, patients have significant new rights to understand and control how their health information is used.

- **Patient education on privacy protections.** Providers and health plans are required to give patients a clear written explanation of how they can use, keep, and disclose their health information.

- **Ensuring patient access to their medical records.** Patients must be able to see and get copies of their records, and request amendments. In addition, a history of most disclosures must be made accessible to patients.

- **Receiving patient consent before information is released.** Patient authorization to disclose information must meet specific requirements. Health care providers who see patients are required to obtain patient consent before sharing their information for treatment, payment, and health care operations purposes. In addition, specific patient consent must be sought and granted for non-routine uses and most non-health care purposes, such as releasing information to financial institutions determining mortgages and other loans or selling mailing lists to interested parties such as life insurers. Patients have the right to request restrictions on the uses and disclosures of their information.

- **Ensuring that consent is not coerced.** Providers and health plans generally cannot condition treatment on a patient's agreement to disclose health information for non-routine uses.

- **Providing recourse if privacy protections are violated.** People have the right to complain to a covered provider or health plan, or to the Secretary, about violations of the provisions of this rule or the policies and procedures of the covered entity.

BOUNDARIES ON MEDICAL RECORD USE AND RELEASE

With few exceptions, an individual's health information can be used for health purposes only.

- **Ensuring that health information is not used for non-health purposes.** Patient information can be used or disclosed by a health plan, provider or clearinghouse only for purposes of health care treatment, payment and operations. Health information cannot be used for purposes not related to health care – such as use by employers to make personnel decisions, or use by financial institutions – without explicit authorization from the individual.

- **Providing the minimum amount of information necessary.** Disclosures of information must be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the transfer of medical records for purposes of treatment, since physicians, specialists, and other providers need access to the full record to provide best quality care.

- **Ensuring informed and voluntary consent.** Non-routine disclosures with patient authorization must meet standards that ensure the authorization is truly informed and voluntary.

ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

The regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity. In this way, implementation of the standards will be flexible and scalable, to account for the nature of each entity's business, and its size and resources. Covered entities must:

- **Adopt written privacy procedures.** These must include who has access to protected information, how it will be used within the entity, and when the information would or would not be disclosed to others. They must also takes steps to ensure that their business associates protect the privacy of health information.

- **Train employees and designate a privacy officer.** Covered entities must provide sufficient training so that their employees understand the new privacy protections procedures, and designate an individual to be responsible for ensuring the procedures are followed.

- **Establish grievance processes.** Covered entities must provide a means for patients to make inquiries or complaints regarding the privacy of their records.

ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORDS USE AND RELEASE

Penalties for covered entities that misuse personal health information are provided in HIPAA.

- **Civil penalties.** Health plans, providers and clearinghouses that violate these standards would be subject to civil liability. Civil money penalties are $100 per incident, up to $25,000 per person, per year, per standard.

- **Federal criminal penalties.** There would be federal criminal penalties for health plans, providers and clearinghouses that knowingly and improperly disclose information or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

BALANCING PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

After balancing privacy and other social values, HHS is establishing rules that would permit certain existing disclosures of health information without individual authorization for the following national priority activities and for activities that allow the health care system to operate more smoothly. All of these disclosures have been permitted under existing laws and regulations. Within certain guidelines found in the regulation, covered entities may disclose information for:

- Oversight of the health care system, including quality assurance activities
- Public health
- Research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board
- Judicial and administrative proceedings
- Limited law enforcement activities
- Emergency circumstances
- For identification of the body of a deceased person, or the cause of death
- For facility patient directories
- For activities related to national defense and security

The rule permits, but does not require these types of disclosures. If there is no other law requiring that information be disclosed, physicians and hospitals will still have to make judgments about whether to disclose information, in light of their own policies and ethical principles.

SPECIAL PROTECTION FOR PSYCHOTHERAPY NOTES

Psychotherapy notes (used only by a psychotherapist) are held to a higher standard of protection because they are not part of the medical record and never intended to be shared with anyone else. All other health information is considered to be sensitive and treated consistently under this rule.

EQUIVALENT TREATMENT OF PUBLIC AND PRIVATE SECTOR HEALTH PLANS AND PROVIDERS. The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and government agency medical units must comply with the full range of requirements, such as providing notice, access rights, requiring consent before disclosure for routine uses, establishing contracts with business associates, among others.

CHANGES FROM THE PROPOSED REGULATION

- **Providing coverage to personal medical records in all forms.** The proposed regulation had applied only to electronic records and to any paper records that had at some point existed in electronic form. The final regulation extends protection to all types of personal health information created or held by covered entities, including oral communications and paper records that have not existed in electronic form. This creates a privacy system that covers virtually all health information held by hospitals, providers, health plans and health insurers.

- **Requiring consent for routine disclosures.** The final rule requires most providers to obtain patient consent for routine disclosure of health records, in addition to requiring special patient authorization for non-routine disclosures. The earlier version had proposed allowing these routine disclosures without advance consent for purposes of treatment, payment and health care operations (such as internal data gathering by a provider or health care plan). However, most individuals commenting on this provision, including many physicians, believed consent for these purposes should be obtained in advance, as is typically done today. The final rule retains the new requirement that patients must also be provided detailed written information on privacy rights and how their information will be used.

- **Allowing disclosure of the full medical record to providers for purposes of treatment.** For most disclosures, such as information submitted with bills, covered entities are required to send only the minimum information needed for the purpose of the disclosure. However, for purposes of treatment, providers need to be able to transmit fuller information. The final rule gives providers full discretion in determining what personal health information to include when sending patients' medical records to other providers for treatment purposes.

- **Protecting against unauthorized use of medical records for employment purposes.** Companies that sponsor health plans will not be able to access the personal health information held by the plan for employment-related purposes, without authorization from the patient.

COST OF IMPLEMENTATION

Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress provided in HIPAA 1996 that the overall financial impact of the HIPAA regulations reduce costs. As such, the financial assessment of the privacy regulation includes the ten-year $29.9 billion savings HHS projects for the recently released electronic claims regulation and the projected $17.6 billion in costs projected for the privacy regulation. This produces a net savings of approximately $12.3 billion for the health care delivery system while improving the efficiency of health care as well as privacy protection.

PRESERVING EXISTING, STRONG STATE CONFIDENTIALITY LAWS

Stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule sets a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information for civic purposes, we do not preempt these mandates. The result is to give individuals the benefit of all laws providing confidentiality protection as well as to honor state priorities.

THE NEED FOR FURTHER CONGRESSIONAL ACTION

HIPAA limits the application of our rule to the covered entities. It does not provide authority for the rule to reach many persons and businesses that work for covered entities or otherwise receive health information from them. So the rule cannot put in place appropriate restrictions on how such recipients of protected health information may use and re-disclose such information. There is no statutory authority for a private right of action for individuals to enforce their privacy rights. We need Congressional action to fill these gaps in patient privacy protections.

IMPLEMENTATION OF THE FINAL REGULATION

The final regulation will come into full effect in two years. The regulation will be enforced by HHS' Office for Civil Rights, which will provide assistance to providers, plans and health clearinghouses in meeting the requirements of the regulation – including a toll free line to help answer questions: 1-866-OCR-PRIV (1-866-627-7748). The TTY number is 1-866-788-4989. A Web site on the new regulation will also be available at *http://www.hhs.gov/ocr*.

# # #

Note: For other HHS Press Releases and Fact Sheets pertaining to the subject of this announcement, please visit our Press Release and Fact Sheet search engine at: *http://www.hhs.gov/search/press.html/*.

THE WHITE HOUSE

WASHINGTON

December 19, 2000

MEDICAL PRIVACY EVENT

DATE:	December 20, 2000
LOCATION:	Great Hall
	Department of Health and Human Services
BRIEFING TIME:	12:15 pm – 12:20 pm
EVENT TIME:	12:25pm – 1:05pm
FROM:	Bruce Reed, Chris Jennings, Mary Beth Cahill

I. PURPOSE

To release a final regulation establishing the first-ever Federal privacy protections for the personal health information of all Americans and call on Congress to finish the job and enact further protections that the American people want and need.

II. BACKGROUND

Today you will release a final rule, which applies to health insurers, most health care providers, and clearinghouses, to: 1) give consumers more control over and access to their health information; 2) set boundaries on the use and release of health records; 3) safeguard health information; 4) establish accountability for inappropriate use and release of health information; and 5) balance public responsibilities with privacy protections. This final regulation strengthens several key provisions of the proposed rule by:

- Extending protections to personal medical records in all forms, including paper records and oral communications.
- Providing for written consent for routine use and disclosure of health records.
- Protecting against unauthorized use of medical records for employment purposes.
- Ensuring that health care providers have all the information necessary to appropriately treat their patients.

The Privacy Of Individual Medical Records Is Not Currently Protected. Currently, 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. In 1999, more than 80 percent of people surveyed agreed with the statement that they had "lost all control over their personal information." 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 unable to do so because of overwhelming barriers established by their insurance company, health care provider, or anyone else who holds their records.

New National Safeguards For Sensitive Health Information. The final regulation you are releasing today will be fully implemented within two years, and is being issued under the authority of the bipartisan Health Insurance Portability and Accountability Act (HIPAA). This regulation will:

1) **Give consumers control over their health information by:**
   - Requiring health plans and providers to inform consumers how their health information is being used and to whom it is disclosed.
   - Limiting the release of private health information without consent.
   - Giving patients access to their own health file and the right to request amendments or corrections to potentially harmful errors in their health files.
2) **Set boundaries on medical record use and release by:**
   - Restricting the amount of information used and disclosed to the "minimum necessary", as opposed to the patient's entire health record.
3) **Ensure the security of personal health information by:**
   - Requiring the establishment of privacy-conscious business practices.
4) **Establish accountability for medical record use and release by:**
   - Creating new criminal and civil penalties for intentional disclosure (fine up to $50,000 and a year in prison), disclosure with the intent to sell data (fine up to $250,000 and 10 years in prison), unintentional disclosure (fine of $100 per person), and other violations (fine up to $25,000 per person per year).
5) **Balance public responsibility with privacy protections by:**
   - Requiring that information be disclosed only for public health priorities and other responsible research.

Financial Impact Of Implementation Of Privacy Regulation. Recognizing the savings and cost potential of standardizing electronic claims processing and protecting privacy and security, the Congress provided in 1996 that the overall financial impact of the HIPAA regulations reduce costs. As such, the financial assessment of the privacy regulation includes the ten-year $29.9 billion savings HHS projects for the recently released electronic claims regulation and the projected $17.6 billion in costs projected for the privacy regulation. This produces a net savings of approximately $12.3 billion for the health care delivery system while improving the efficiency of health care as well as privacy protection.

Call On Congress To Enact Privacy Legislation To Finish The Job. Despite the importance of today's actions, additional Federal legislation is still needed, and you will call on Congress to enact legislation to: 1) extend these privacy protections to life insurers and worker's compensation programs; and 2) create a private right of action so

citizens can hold health plans and providers accountable for inappropriate and harmful disclosures of information.

III. PARTICIPANTS

Meet & Greet Participants:
Secretary Donna Shalala (curbside)

Deputy Secretary Kevin Thurm, HHS
Mary Beth Donahue, Chief of Staff, HHS
Gary Claxton, HHS
Lisa Rovin, HHS
HHS Staff TBD

Briefing Participants:
Secretary Donna Shalala
Chris Jennings
Sally Katzen
Paul Glastris

Event Participants:
YOU
Secretary Donna Shalala
Janlori Goldman, Director, Health Privacy Project of Georgetown University

IV. PRESS PLAN

Open Press.

V. SEQUENCE OF EVENTS

- **YOU** will arrive at the Department of Health and Human Services, and will greet a small group of HHS staff.
- **YOU** will proceed to the hold for a briefing.
- **YOU** will be announced onto the stage accompanied by Secretary Shalala and Janlori Goldman.
- Secretary Shalala will make brief remarks and introduce Janlori Goldman.
- Janlori Goldman will make brief remarks and introduce **YOU**.
- **YOU** will make remarks, work a ropeline, and depart.

VI. REMARKS

To be provided by speechwriting.

Paul D. Glastris
12/19/2000 08:19:23 PM

Record Type: Record

To: See the distribution list at the bottom of this message

cc:
Subject: final med privacy remarks

Final 12/19/00 8:00 pm
Paul Glastris

PRESIDENT WILLIAM J. CLINTON
REMARKS ON MEDICAL PRIVACY
DEPARTMENT OF HEALTH AND HUMAN SERVICES
WASHINGTON, DC
December 20, 2000

Acknowledgments: Sec. Shalala; my CoS John Podesta, who has worked hard on this issue; Georgetown University Health Privacy Project Director Jan Lori Goldman; representatives of nurses, doctors, consumers and the privacy community.

In 1928, Justice Brandies famously wrote that privacy is "the right most valued by civilized men...the right to be left alone." Nothing is more private than what goes on inside your own body, or in the case of psychiatric records, your own mind. If we are to defend the freedom of individuals in the information age, we must protect the privacy of individual medical records.

Today, I am pleased to release new federal rules protecting the medical records of virtually every American. These rules represent the most sweeping privacy protections ever written, and they are built on the foundation of bipartisan Kennedy-Kassebaum legislation I signed four years ago.

This action is required by the great tides of technological and economic change that have swept through the medical profession in recent years. In the past, medical records were kept on paper, by doctors you knew, and stored in file cabinets by nurses you knew. Seldom were these records shared with anyone outside the doctor's office.

Today, physicians are increasingly storing medical records electronically. And they are now obliged to share records, in paper or electronic form, with insurance companies and other reviewers. 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 to make quicker and better-informed

decisions.

The problem is that with the click of a mouse, your personal health information can be accessed without your consent by people you don't know, who aren't physicians, for reasons that have nothing to do with health care. It doesn't take a doctor to understand that that's a prescription for abuse.

So the rules I am releasing today have been carefully crafted for the 21st Century—to make your medical records easier to see for those who should see them, and much harder to see for people who shouldn't.

Employers, for instance, shouldn't see your medical records except for limited reasons, such as to process insurance claims. Yet too often they do. A recent survey showed that more than a third of all Fortune 500 companies check medical records before they hire or promote. One large employer in Pennsylvania had no trouble obtaining detailed information on the prescription drugs taken by its workers, easily discovering that one employee was HIV positive. That's wrong. And under the rules I am releasing today, it will be illegal.

Private companies shouldn't be able to get a hold of your most intimate medical information for marketing purposes, yet too often they do. Recently, expectant mothers who haven't even told their friends the good news, are finding sales letters for baby products in their mailboxes. That's wrong, and under these new rules, it will be illegal.

Health insurance companies shouldn't be able to share your medical records with mortgage companies, who might use them to deny you a loan. Yet too often that's what happens. Under these rules, it will be illegal.

Health insurance companies also shouldn't be able to keep you from seeing your own medical records. Up till now, they could. Under these rules, they won't be able to.

Under the rules we are issuing today, health plans and providers will have to tell you up front who will and won't be allowed to see your records.

And under an executive order I am issuing today, the federal government will no longer have free rein to launch criminal prosecutions based on information gleaned from routine audits of medical records.

With these actions today, I have done everything I can to protect the sanctity of individual medical records. But there are further protections our families need that only Congress can provide. For example, only new legislation from Congress can we make these new protections fully enforceable and cover every entity that holds your medical records. I urge the new Congress to act quickly to provide those additional protections.

For eight years now, I have worked to fulfill a new vision of government and politics, marrying our enduring values to the demands of the information age. In many ways, these

new medical privacy rules exemplify that vision. They are one more example of how, at the dawn of a new century, America is prepared to meet the future.

Thank you.

Message Sent To:

Remarks of Janlori Goldman, Director, Health Privacy Project

December 20, 2000

I am deeply honored to be here for this historic occasion. Today, President Clinton and Secretary Shalala are releasing landmark rules that create a federal privacy right in personal health information. These regulations you are signing today are urgently needed, and on behalf of the disability rights and consumer groups in our coalition who have fought long and hard for strong, enforceable medical privacy rules, we applaud you Mr. President, and Madame Secretary, and all those who worked so hard in the Administration to bring these regulations into the light of day. I especially want to single out for praise John Podesta whose leadership and commitment made this possible.

Until today, we had no federal privacy law protecting peoples' medical records. And people have suffered as a consequence.

Terri Seargent, who is here with us today, was fired from her job after her employer learned that she had been diagnosed with a genetic

disorder that would require expensive treatment. Terri was a valued employee who had received a positive review and a raise just before her company fired her. In fact, the EEOC determined Terri was fired Terri because of her disability.

We are glad that anti-discrimination laws are in place for people like Terri. But there's a bigger issue here: employers should not have access to health information in the first place. But they do.

I'd like to share one more story with you. Annette W. and her husband were involved in a difficult and contentious divorce. In the midst of their separation, Annette instructed her pharmacy not to disclose any medical information to her husband. Just one day later, the pharmacist gave Annette's husband a list of all her prescription drugs. Armed with this medical information her husband embarked on a campaign to label her a drug user. He sent information to friends and family, to the Department of Motor Vehicles, and threatened to have her children taken away. Annette should never have had to worry when she filled her prescription that this sensitive information could be so unfairly used against her.

Through stories like Terri's and Annette's we have learned that privacy is the first line of defense against discrimination.

People should not have to worry when they talk with their doctor, fill a prescription, or enroll in a health plan, that their medical records will be used to deny them jobs, benefits, or stigmatize them. But they do worry. We know that right now people are withdrawing from full participation in their own health care to shield themselves from the misuse of their health information. To protect themselves, people withhold information from their doctors, pay out of pocket for care, or in the most extreme cases, avoid care altogether.

These privacy-protective behaviors put people at risk for undiagnosed and untreated conditions. And the larger community suffers as well. When people are afraid to fully participate in their own care, the information available to our nation's researchers and public health officials is incomplete and unreliable.

Our health care system has changed dramatically in the last decade, bringing with it both promises and perils. We have mapped the human genome, but people are afraid to get tested. And the Internet can deliver cutting edge research and health care, but people are unwilling to trust their most sensitive health information in cyberspace. This country will never fully reap the benefits of these astounding breakthroughs until privacy is woven into the fabric of our health care system.

Through today's release of this landmark privacy rule, the Administration makes great strides to reassure people that their medical information is not up for grabs. But our work is not done. The Administration was constrained by Congress in how far it could go in this regulation. It is now up to the Congress, and the state legislatures, to finish this job. We need today's rule to be expanded to cover life insurers, drug companies and others. And we need stronger enforcement provisions to ensure that those who violate this rule are held accountable. Victims should be able to go to court to seek redress when their privacy rights are violated.

Mr. President, welcome to the best, smartest, richest, most effective—and best looking—department in government.

For eight years, I've had the pleasure of working with you...of watching you serve with courage and compassion—*and of waiting for you to finally come and visit us.*

To tell you the truth, we were starting to feel a little like Nebraska.

But that's OK—because I know that the important thing isn't that you've come here today—but how far America has come since you took office eight years ago.

You haven't just made America wealthier—you've made it fairer, kinder and better. For that, we welcome you to the Department of Health and Human Services.

We welcome you as a constant voice for change...a voice for opportunity...and a voice for the voiceless that has echoed through our inner cities...across our sweeping plains...and in the imagination of every citizen.

We welcome you for seeing things not as they are—but as they could be.

And we welcome you for bringing to Washington a dream of America where every child can enjoy a healthy start...where every young family can enjoy the fruits of our prosperity...and where every senior citizen can enjoy an old age with dignity.

I want to thank each and every one of my employees—the best and the brightest—for working so hard with you...and with me...over the past eight years to help further that dream—and the very dream of America itself.

Look at the difference eight years have made:

By extending the life of the Medicare Trust Fund for 24 years, you've helped ensure that the lifeline—and the promise—of Medicare will not be broken.

By raising childhood immunization rates to record highs...and by decreasing both infant mortality and teen pregnancy rates to all-time lows...you've opened the doors of opportunity and possibility for our children.

By helping millions of Americans to move from welfare to work—you've also helped them move from despair to dignity.

By insuring nearly 2.5 million children through S-CHIP, you've provided more children with healthy foundations on which they can build their hopes and futures.

By prohibiting federal agencies from using genetic information in hiring and promotion, you've guaranteed that no federal employer would ever review our medical records with our resumes.

By supporting—and signing—the "Health Insurance Portability and Accountability Act" you've helped ensure that genetic information couldn't be used to deny working families—and their children—health insurance.

And by ceaselessly working to eliminate racial and ethnic health disparities...to increase AIDS and cancer research...and to improve access to health insurance...you've proven that America isn't just great—but good.

These are accomplishments we are all proud of—and accomplishments that affect the life of every American.

Our new federal privacy regulation will also affect the life of every American.

It will improve patients' access and control of their medical information.

It will set boundaries on the use and release of medical information.

It will establish standards that health care providers and others must meet in protecting the privacy of health information.

It will impose penalties for violations of medical privacy standards.

And it will balance our need for privacy protection with the public responsibility to support national priorities—like public health.

Mr. President, we salute you for insisting that we move forward on privacy when Congress wouldn't—and for your sustained leadership on this issue.

For decades to come, our new federal privacy regulation will be seen as a landmark in patient protection...

...It will be remembered as a hallmark of this Administration...

...And it will set a benchmark for future Congresses.

Thank you, Mr. President.

* * *

Janlori Goldman, the Director—and founder—of the Health Privacy Project at Georgetown University will now tell you a little more about the background of our privacy regulation.

Throughout her career as a lawyer, researcher and activist, Ms. Goldman has been a leader and pioneer in efforts to protect the privacy of all health care information—including on the internet.

It's now my pleasure to introduce to you Janlori Goldman.

EXAMPLES OF MEDICAL RECORDS PRIVACY VIOLATIONS

Using medical information for marketing purposes.

- RxAmerica, a Utah based pharmaceutical benefits manager, was using patient data to solicit business for its owner American Drug Stores. Patients were asked to switch drug stores and start filling their prescriptions at Sav-on, a chain owned by American Drug Stores. [*Kiplingers*, February 2000]

Carelessly storing sensitive medical information.

- The Harvard Community Health Plan, a Boston-based HMO, admitted to maintaining detailed notes of psychotherapy sessions in computer records that were accessible by all clinical employees. [*Boston Globe*, March 1995]

- The University of Michigan Medical Center inadvertently stored several thousand patient records on a public internet site for two months. Individuals searching the internet for information about a provider were linked to patient records containing names, addresses, social security number, treatment for medical conditions and other data. [*Washington Business*, February 1999]

- Aetna health insurance claim forms blew out of a truck on the way to a recycling center and scattered on a major highway during the evening rush hour. Employees were dispatched to scoop up forms containing personal medical information. The forms should have been shredded, but weren't. [*The Hartford Courant*, May 1999]

- GlobalHealthtrax, which sells health products online, inadvertently revealed customer names, home phone numbers, bank account, and credit card information of thousands of customers on their Web site. [Bank Information Exposed Online, *MSNBC*, January 2000]

- Hundreds of patient records were found in the parking lot outside Scripps Clinic in California. Information included diagnosis, credit card numbers, and test results. The records appeared to be from multiple health care sites. [*San Diego Union-Tribune*, May 1998]

Unauthorized disclosure of sensitive medical information.

- A physician in New Jersey diagnosed with cancer agreed to allow slides of his cancer cells to be used in research. He was promised anonymity, but his name was entered into a computer associated with the slides, and colleagues quickly began calling to offer condolences. [*National Journal*, April 1998]

- After suffering a work-related injury to her wrist, a woman in California authorized her insurance company to release information about her wrist ailment to her employer. When she had the opportunity to review the information that was sent, she realized that the file contained her entire medical history, including records on recent fertility treatment and pregnancy loss. [*Sacramento Business Journal*, April 1999]

Using the results of routine medical exams to promote pharmaceutical treatments.

- An Orlando woman recently had her doctor perform some routine tests, and received a letter weeks later from a drug company touting a treatment for her high cholesterol. [*Orlando Sentinel*, November 1997]

Using confidential medical records to sabotage reputations or cause malicious harm.

- The 13 year old daughter of a hospital employee took a list of patient names and phone numbers when visiting her mother at work. As a joke, she contacted patients and told them that they were HIV positive. [*The Washington Post*, March 1995]

- New York Congresswoman Nydia Velasquez' medical records – including details of a bout with depression and a suicide attempt—were faxed from a New York hospital to a local newspaper and television station on the eve of her 1992 primary. [*USA Today*, April 1998]

- In Tampa, a friend of a public health worker sent the names of 4,000 HIV positive individuals to two newspapers. [*USA Today*, October 1996]

Selling private health benefits information to private companies.

- In Colorado, a medical student copied health records at night and sold them to medical malpractice attorneys.

- In Maryland, eight Medicaid clerks were prosecuted for selling computerized record printouts of recipients – and dependents – financial resources to sales representatives of managed care companies. [Forbes, May 1996]

EXAMPLES OF MEDICAL RECORDS PRIVACY VIOLATIONS

Using medical information for marketing purposes.

- RxAmerica, a Utah based pharmaceutical benefits manager, was using patient data to solicit business for its owner American Drug Stores. Patients were asked to switch drug stores and start filling their prescriptions at Sav-on, a chain owned by American Drug Stores. [*Kiplingers*, February 2000]

Carelessly storing sensitive medical information.

- The Harvard Community Health Plan, a Boston-based HMO, admitted to maintaining detailed notes of psychotherapy sessions in computer records that were accessible by all clinical employees. [*Boston Globe*, March 1995]

- The University of Michigan Medical Center inadvertently stored several thousand patient records on a public internet site for two months. Individuals searching the internet for information about a provider were linked to patient records containing names, addresses, social security number, treatment for medical conditions and other data. [*Washington Business*, February 1999]

- Aetna health insurance claim forms blew out of a truck on the way to a recycling center and scattered on a major highway during the evening rush hour. Employees were dispatched to scoop up forms containing personal medical information. The forms should have been shredded, but weren't. [*The Hartford Courant*, May 1999]

- GlobalHealthtrax, which sells health products online, inadvertently revealed customer names, home phone numbers, bank account, and credit card information of thousands of customers on their Web site. [Bank Information Exposed Online, *MSNBC*, January 2000]

- Hundreds of patient records were found in the parking lot outside Scripps Clinic in California. Information included diagnosis, credit card numbers, and test results. The records appeared to be from multiple health care sites. [*San Diego Union-Tribune*, May 1998]

Unauthorized disclosure of sensitive medical information.

- A physician in New Jersey diagnosed with cancer agreed to allow slides of his cancer cells to be used in research. He was promised anonymity, but his name was entered into a computer associated with the slides, and colleagues quickly began calling to offer condolences. [*National Journal*, April 1998]

- After suffering a work-related injury to her wrist, a woman in California authorized her insurance company to release information about her wrist ailment to her employer. When she had the opportunity to review the information that was sent, she realized that the file contained her entire medical history, including records on recent fertility treatment and pregnancy loss. [*Sacramento Business Journal*, April 1999]

Using the results of routine medical exams to promote pharmaceutical treatments.

- An Orlando woman recently had her doctor perform some routine tests, and received a letter weeks later from a drug company touting a treatment for her high cholesterol. [*Orlando Sentinel*, November 1997]

Using confidential medical records to sabotage reputations or cause malicious harm.

- The 13 year old daughter of a hospital employee took a list of patient names and phone numbers when visiting her mother at work. As a joke, she contacted patients and told them that they were HIV positive. [*The Washington Post*, March 1995]

- New York Congresswoman Nydia Velasquez' medical records – including details of a bout with depression and a suicide attempt—were faxed from a New York hospital to a local newspaper and television station on the eve of her 1992 primary. [*USA Today*, April 1998]

- In Tampa, a friend of a public health worker sent the names of 4,000 HIV positive individuals to two newspapers. [*USA Today*, October 1996]

Selling private health benefits information to private companies.

- In Colorado, a medical student copied health records at night and sold them to medical malpractice attorneys.

- In Maryland, eight Medicaid clerks were prosecuted for selling computerized record printouts of recipients – and dependents – financial resources to sales representatives of managed care companies. [Forbes, May 1996]

EXAMPLES OF MEDICAL RECORDS PRIVACY VIOLATIONS

Using medical information for marketing purposes.

- RxAmerica, a Utah based pharmaceutical benefits manager, was using patient data to solicit business for its owner American Drug Stores. Patients were asked to switch drug stores and start filling their prescriptions at Sav-on, a chain owned by American Drug Stores. [*Kiplingers*, February 2000]

Carelessly storing sensitive medical information.

- The Harvard Community Health Plan, a Boston-based HMO, admitted to maintaining detailed notes of psychotherapy sessions in computer records that were accessible by all clinical employees. [*Boston Globe*, March 1995]

- The University of Michigan Medical Center inadvertently stored several thousand patient records on a public internet site for two months. Individuals searching the internet for information about a provider were linked to patient records containing names, addresses, social security number, treatment for medical conditions and other data. [*Washington Business*, February 1999]

- Aetna health insurance claim forms blew out of a truck on the way to a recycling center and scattered on a major highway during the evening rush hour. Employees were dispatched to scoop up forms containing personal medical information. The forms should have been shredded, but weren't. [*The Hartford Courant*, May 1999]

- GlobalHealthtrax, which sells health products online, inadvertently revealed customer names, home phone numbers, bank account, and credit card information of thousands of customers on their Web site. [Bank Information Exposed Online, *MSNBC*, January 2000]

- Hundreds of patient records were found in the parking lot outside Scripps Clinic in California. Information included diagnosis, credit card numbers, and test results. The records appeared to be from multiple health care sites. [*San Diego Union-Tribune*, May 1998]

Unauthorized disclosure of sensitive medical information.

- A physician in New Jersey diagnosed with cancer agreed to allow slides of his cancer cells to be used in research. He was promised anonymity, but his name was entered into a computer associated with the slides, and colleagues quickly began calling to offer condolences. [*National Journal*, April 1998]

- After suffering a work-related injury to her wrist, a woman in California authorized her insurance company to release information about her wrist ailment to her employer. When she had the opportunity to review the information that was sent, she realized that the file contained her entire medical history, including records on recent fertility treatment and pregnancy loss. [*Sacramento Business Journal*, April 1999]

Using the results of routine medical exams to promote pharmaceutical treatments.

- An Orlando woman recently had her doctor perform some routine tests, and received a letter weeks later from a drug company touting a treatment for her high cholesterol. [*Orlando Sentinel*, November 1997]

Using confidential medical records to sabotage reputations or cause malicious harm.

- The 13 year old daughter of a hospital employee took a list of patient names and phone numbers when visiting her mother at work. As a joke, she contacted patients and told them that they were HIV positive. [*The Washington Post*, March 1995]

- New York Congresswoman Nydia Velasquez' medical records – including details of a bout with depression and a suicide attempt—were faxed from a New York hospital to a local newspaper and television station on the eve of her 1992 primary. [*USA Today*, April 1998]

- In Tampa, a friend of a public health worker sent the names of 4,000 HIV positive individuals to two newspapers. [*USA Today*, October 1996]

Selling private health benefits information to private companies.

- In Colorado, a medical student copied health records at night and sold them to medical malpractice attorneys.

- In Maryland, eight Medicaid clerks were prosecuted for selling computerized record printouts of recipients – and dependents – financial resources to sales representatives of managed care companies. [Forbes, May 1996]

FINAL REGULATION TO PROTECT MEDICAL RECORDS PRIVACY SUMMARY OF CHANGES		
PROVISION	**PROPOSED RULE**	**FINAL RULE**
Expanding the Scope of Protections	The proposed rule limited covered information to information that was or at one point was in electronic form.	The final rule covers all medical record information – including paper records and oral communications.
Strengthening Consent Provisions	The proposed rule did not require health care providers to obtain consent for the disclosure of protected health information for routine uses such as treatment, payment, or health care operations. The proposed rule was silent on providers providing protected health information to appropriate government agencies concerning individuals who are suspected of being victims of abuse, neglect or domestic violence.	The final rule requires health care providers to obtain written consent when disclosing information for any purpose. The final rule requires that health plans and providers attempt to determine patient preferences before disclosing information to someone involved in their care, a family member, or a disaster relief agency of the patient's location or condition. The final rule ensures that individuals who are suspected of being victims of abuse, neglect, or domestic violence are consulted before protected health information is released.
Ensuring that Providers Have the Information Necessary to Treat Their Patients	The proposed rule inadvertently limited the amount of information providers could send to other health care personnel treating a patient.	The final regulation does not apply the "minimum necessary" standard to information shared with other health care professionals for purposes of treatment.
Closing the Loophole for Employer Sponsored Health Plans	The proposed rule did not directly address employer access to protected health information held by employer-sponsored health plans.	The final regulation limits the information that employer-sponsored health plans can share with the employer to information necessary to administer the plan.

FINAL REGULATION TO PROTECT MEDICAL RECORDS PRIVACY SUMMARY OF CHANGES		
PROVISION	**PROPOSED RULE**	**FINAL RULE**
Providing Information to Patients in a Secure Manner	The proposed rule was silent on the manner in which confidential information should be communicated to patients.	The final rule requires that health plans and providers accommodate reasonable requests that information being sent to patients be handled in a manner that protects confidentiality. Health plans must accommodate these requests if the patient certifies that they are in danger if the request is not honored.
Strengthening Public Health Requirements	The proposed rule permits disclosure to individuals working under the direction of a public health authority without consent.	The final regulation narrows this exception to allow disclosure only to those individuals who are undertaking specific activities related to FDA requirements or product recalls.
Reducing the Burden on Business Associates	The proposed rule holds health plans and providers responsible for monitoring their business associates for privacy violations and holding them responsible when violations occur.	The final rule does not require monitoring and holds health plans and providers responsible only for known privacy violations.
Improving Notice of Information Practices	The proposed rule requires covered entities to inform patients of their actual information use practices.	The final rule allows covered entities to use standard language that describes all permitted or requires uses or disclosures.
Protecting the Public Safety	The proposed rule allowed disclosure of limited information to law enforcement officials to identify a suspected fugitive, witness or missing person.	The final rule clarifies the original proposal, stating that health plans and providers can alert law enforcement authorities if a patient admits to participating in a violent crime or escaping lawful custody. The final rule also permits health care providers to notify law enforcement officers of evidence of a crime.

FINAL REGULATION TO PROTECT MEDICAL RECORDS PRIVACY SUMMARY OF CHANGES		
PROVISION	**PROPOSED RULE**	**FINAL RULE**
Expanding the Scope of Protections	The proposed rule limited covered information to information that was or at one point was in electronic form.	The final rule covers all medical record information – including paper records and oral communications.
Strengthening Consent Provisions	The proposed rule did not require health care providers to obtain consent for the disclosure of protected health information for routine uses such as treatment, payment, or health care operations. The proposed rule was silent on providers providing protected health information to appropriate government agencies concerning individuals who are suspected of being victims of abuse, neglect or domestic violence.	The final rule requires health care providers to obtain written consent when disclosing information for any purpose. The final rule requires that health plans and providers attempt to determine patient preferences before disclosing information to someone involved in their care, a family member, or a disaster relief agency of the patient's location or condition. The final rule ensures that individuals who are suspected of being victims of abuse, neglect, or domestic violence are consulted before protected health information is released.
Ensuring that Providers Have the Information Necessary to Treat Their Patients	The proposed rule inadvertently limited the amount of information providers could send to other health care personnel treating a patient.	The final regulation does not apply the "minimum necessary" standard to information shared with other health care professionals for purposes of treatment.
Closing the Loophole for Employer Sponsored Health Plans	The proposed rule did not directly address employer access to protected health information held by employer-sponsored health plans.	The final regulation limits the information that employer-sponsored health plans can share with the employer to information necessary to administer the plan.

FINAL REGULATION TO PROTECT MEDICAL RECORDS PRIVACY SUMMARY OF CHANGES		
PROVISION	**PROPOSED RULE**	**FINAL RULE**
Providing Information to Patients in a Secure Manner	The proposed rule was silent on the manner in which confidential information should be communicated to patients.	The final rule requires that health plans and providers accommodate reasonable requests that information being sent to patients be handled in a manner that protects confidentiality. Health plans must accommodate these requests if the patient certifies that they are in danger if the request is not honored.
Strengthening Public Health Requirements	The proposed rule permits disclosure to individuals working under the direction of a public health authority without consent.	The final regulation narrows this exception to allow disclosure only to those individuals who are undertaking specific activities related to FDA requirements or product recalls.
Reducing the Burden on Business Associates	The proposed rule holds health plans and providers responsible for monitoring their business associates for privacy violations and holding them responsible when violations occur.	The final rule does not require monitoring and holds health plans and providers responsible only for known privacy violations.
Improving Notice of Information Practices	The proposed rule requires covered entities to inform patients of their actual information use practices.	The final rule allows covered entities to use standard language that describes all permitted or requires uses or disclosures.
Protecting the Public Safety	The proposed rule allowed disclosure of limited information to law enforcement officials to identify a suspected fugitive, witness or missing person.	The final rule clarifies the original proposal, stating that health plans and providers can alert law enforcement authorities if a patient admits to participating in a violent crime or escaping lawful custody. The final rule also permits health care providers to notify law enforcement officers of evidence of a crime.

FINAL REGULATION TO PROTECT MEDICAL RECORDS PRIVACY SUMMARY OF CHANGES		
PROVISION	**PROPOSED RULE**	**FINAL RULE**
Expanding the Scope of Protections	The proposed rule limited covered information to information that was or at one point was in electronic form.	The final rule covers all medical record information – including paper records and oral communications.
Strengthening Consent Provisions	The proposed rule did not require health care providers to obtain consent for the disclosure of protected health information for routine uses such as treatment, payment, or health care operations. The proposed rule was silent on providers providing protected health information to appropriate government agencies concerning individuals who are suspected of being victims of abuse, neglect or domestic violence.	The final rule requires health care providers to obtain written consent when disclosing information for any purpose. The final rule requires that health plans and providers attempt to determine patient preferences before disclosing information to someone involved in their care, a family member, or a disaster relief agency of the patient's location or condition. The final rule ensures that individuals who are suspected of being victims of abuse, neglect, or domestic violence are consulted before protected health information is released.
Ensuring that Providers Have the Information Necessary to Treat Their Patients	The proposed rule inadvertently limited the amount of information providers could send to other health care personnel treating a patient.	The final regulation does not apply the "minimum necessary" standard to information shared with other health care professionals for purposes of treatment.
Closing the Loophole for Employer Sponsored Health Plans	The proposed rule did not directly address employer access to protected health information held by employer-sponsored health plans.	The final regulation limits the information that employer-sponsored health plans can share with the employer to information necessary to administer the plan.

FINAL REGULATION TO PROTECT MEDICAL RECORDS PRIVACY SUMMARY OF CHANGES		
PROVISION	**PROPOSED RULE**	**FINAL RULE**
Providing Information to Patients in a Secure Manner	The proposed rule was silent on the manner in which confidential information should be communicated to patients.	The final rule requires that health plans and providers accommodate reasonable requests that information being sent to patients be handled in a manner that protects confidentiality. Health plans must accommodate these requests if the patient certifies that they are in danger if the request is not honored.
Strengthening Public Health Requirements	The proposed rule permits disclosure to individuals working under the direction of a public health authority without consent.	The final regulation narrows this exception to allow disclosure only to those individuals who are undertaking specific activities related to FDA requirements or product recalls.
Reducing the Burden on Business Associates	The proposed rule holds health plans and providers responsible for monitoring their business associates for privacy violations and holding them responsible when violations occur.	The final rule does not require monitoring and holds health plans and providers responsible only for known privacy violations.
Improving Notice of Information Practices	The proposed rule requires covered entities to inform patients of their actual information use practices.	The final rule allows covered entities to use standard language that describes all permitted or requires uses or disclosures.
Protecting the Public Safety	The proposed rule allowed disclosure of limited information to law enforcement officials to identify a suspected fugitive, witness or missing person.	The final rule clarifies the original proposal, stating that health plans and providers can alert law enforcement authorities if a patient admits to participating in a violent crime or escaping lawful custody. The final rule also permits health care providers to notify law enforcement officers of evidence of a crime.

HIPAA Health Privacy Regulation:
DRAFT Questions and Answers –SHORT

I. GENERAL

Q: Will providers and plans support this regulation?

A: Providers and plans have been clear that they support privacy protections. Their primary concerns have been that such protections support the effective delivery and payment of health care services.

We've worked closely with provider and health plan representatives to design a system of protections that meshes smoothly with current delivery and payment systems.

We carefully considered the comments and suggestions made by providers and plans and modified provisions to make them less burdensome for providers and plans, while also ensuring that they offer real privacy protection for the individual.

Q: Did any groups comments come as a surprise, meaning were you alerted to consequences that had not been evident previously? If so, can you give us any examples.

A: We learned a great deal from the comments, and the improvements we made in privacy protections reflect the input they provided. Because of the comments this rule directly addresses concerns of victims of domestic violence. Many commenters pointed out that our proposed rule may have prevented plans and providers from doing such common activities as printing enrollee ID cards or training new staff.

Q: Did you hear from any Federal agencies?

A: We always work closely with other Federal agencies when we develop important and comprehensive rules like this one. Americans want and need protection of their personal health information as well as public safety and protection from crime. We worked with the other agencies to protect the privacy rights of American consumers without sacrificing their other interests.

Q: Which sector was the most vocal in the their comments?

A: American consumers themselves, who took the time as individual citizens to let us know that they wanted all of their health information protected, regardless of form.

Q: Did you look to any of the proposed bills for guidance?

A: We looked for guidance to all the bills of the last two Congresses. [what else?]

Q: How many groups did you meet with between the time the comment period closed and the publication of the final rule?

A: We did not accept comments from any groups after the comment period closed. My staff conducted numerous fact finding discussions to clarify issues and explore the potential effects of various options–we have not counted the number of people we contacted.

Q: When will the regulations take effect?

A: Health care providers, health care clearinghouses and health plans with more than $5 million in annual revenues will have 2 years to comply. Small health plans (those with less than $5 million in annual revenues) will be given 36 months. The HHS Office for Civil Rights will provide assistance during the start-up period to help covered entities prepare. OCR will begin investigating and acting on complaints after that period.

Q: Because of the limited HIPAA authority what protections were you not able to address?

A: The most significant drawback to our authority is that we could not cover all persons or entities that use and share personal health information. We also could not provide individuals with a key enforcement tool – a private right of action when their privacy rights have been compromised.

Q: Is additional legislative action still needed?

A: Yes. While this rule is a significant step in protecting the privacy of individuals, more remains to be done to ensure that all parties that have health information protect that information.

HIPAA only covers certain health care providers, health plans, and health care clearinghouses. Congress will need to take action to extend these requirements to all other parties who use or disclose health information. We also need Congressional action to improve our enforcement capacity – by adding a private right of action for consumers when their privacy has been violated.

Q: The Paperwork Reduction Act grants Congress the right to review all 'major' regulations. Clearly, this regulation falls into that category. Do you think that Congress will use its authority to block this rule?

A: I don't think that will happen. Protection of consumer privacy is a bipartisan concern, and Members realize that if we delay taking this first step, our ability to provide real protection for this most sensitive of personal information slips further away. Members made a lot of progress in the last session of Congress. I'm hopeful these regulations will provide a solid base for their efforts to finish the job.

Q: Do you think that medical privacy will be an important issue for the next administration?

A: Absolutely. Today, providers submit almost 5 billion health care claims annually. About 64% are transmitted electronically. In our increasingly 'wired' economy, this proportion will increase very quickly. And as in every industry, ever more health care information is stored and shared electronically as well. As that happens more sensitive health information will lack full privacy protection absent more comprehensive legislation.

We'll read more media accounts of medical records being inadvertently placed on unsecured websites, about individual's losing their jobs or insurance because an employer had access to health information indicating a genetic test or a psychiatric visit.

The next administration and Congress both will need to put this high on their legislative agendas.

Q: How much involvement did the White House have in shaping the policies in this regulation?

A: President Clinton has been completely committed to the creation and release of this rule. The White House played an important role in coordinating the input of other federal agencies and ensuring that all voices were heard as we developed these policies.

Q: Is it possible that a new administration will try to block these regulations?

A: We see no reason for a new administration to try to block these regulations. Americans have been overwhelmingly clear that they want and expect privacy protection for their medical records. As the use of electronic records and the internet has increased, so too have Americans become even more conscious of and concerned about their privacy.

Q: Isn't it possible for a new Administration to just invalidate these regulations?

A: HIPAA (Kassebaum/Kennedy) was bipartisan legislation, and the desire for health information privacy protection is a bipartisan priority. It important to get this clock started, and not delay. Meanwhile, remember that we still encourage Congress to come back and pass legislation to fill in the gaps in our authority. We think the new administration will find this rule to be a good foundation.

II. BACKGROUND

Q: Why is this regulation needed?

A: Surprising as it may seem, there is no common set of rules or standards to ensure that Americans' personal medical information is protected. We have only a patchwork of protection, which is inadequate for today's needs: various professional standards that largely pre-date the electronic age, and a confusing array of different state laws. In other areas, like banking and credit records, there are federal laws that protect our personal information - but no federal protection for our medical records, even as those records are increasingly being stored and moved electronically.

There is no bedrock of protection for patients regarding some of their most personal and sensitive information: no way for patients to find out how their records are being used ... and no right under federal law to control the release of their personal health information, or even to see their own health files.

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 may 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.

Q: Can you provide examples of the types privacy breaches that need to be addressed?

A: Sure.

Medical Information Used for Marketing
A pharmaceutical benefits manager was using patient data to solicit business for its owner, a drug store chain. Patients were asked to switch drugstores and start filling their prescriptions at the chain.

Unauthorized Access
Several health plan clerks were prosecuted for selling computerized record printouts of recipients' and dependents' financial resources to sales representatives of managed care companies.

Researchers
A physician, agreed to allow slides of his cancer cells to be used in research. He was promised anonymity, but his name was entered into a computer associated with the slides, and colleagues quickly began calling to offer condolences.

Poor Disposal
Hundreds of patient records were found in the parking lot outside a California clinic. Information included diagnosis, credit card numbers, and test results. The records appeared to be from multiple health care sites.

Individuals Exposed
After suffering a work-related injury to her wrist, Roni Breite authorized her insurance company to release information pertaining to her wrist ailment to her employer. When she had the opportunity to review her employee record, the file contained her *entire* medical history, including records on recent fertility treatment and pregnancy loss.

Q: Is broader legislation still needed?

A: Yes. Congress still needs to act ensure that all health information, regardless of who holds it, how they use it, or disclose it, are subject to the same rules. HHS also cannot extend protection directly to insurers and others who do not qualify as providers, health plans or health care clearinghouses. In addition, Congress should provide more effective sanctions when privacy rights are violated - higher penalties than the amounts provided in the current law, as well as a federal right for individuals to bring their own legal action when they believe their rights to privacy of medical information have been violated.

Q: Approximately what portion of medical records are paper-only? Approximately how many exchanges of medical information occur every year, and what portion involve paper-only records?

A: We do not know what number of medical records exist *only* in paper form. Increasingly, of course, records are being kept electronically. We do know, however, that 64% of all health care claims are transmitted electronically. (Overall, there are 4.7 billion health care claims made annually.) And we know that most health care providers and health plans share health information electronically.

The number of transactions involving exchange of personal medical information is in the billions each year. Medicare alone processes about a billion payment claims per year.

Q: Why did this final regulation take so long? Did you intentionally wait until after the election to publish it? And now are you rushing to publish in order to beat the incoming Administration?

A: Simply put, this is an extremely complex rule that will have a significant impact on one of the largest segments of our economy. We needed time to consider all the comments fully and develop the best possible set of standards to protect American health care consumers.

The NPRM generated an extraordinary number of comments (about 52,000) and we had to extend the comment period to accommodate the degree of interest and detailed nature of the subject. The comments in many case were quite extensive (some 100 pages and more) and addressed the full range of issues presented in the NPRM.

The task fell to us to promulgate this regulation in August 1999. We have moved as quickly as we could to fulfill our Congressional mandate. But there is nothing preemptive about this publication Americans want privacy protection for their medical records, and we see no reason to delay publication now that the final regulation is ready.

III. GENERAL REQUIREMENTS OF THE RULE

Privacy Protections of the Rule

Q: What does this regulation do?

A: The regulation is an historic watershed for patients and for our health care system.

It establishes, for the first time, a national foundation of federal privacy protections for personal medical records.

It achieves the goals that the Administration laid out for Congress three years ago:

- It provides consumer control over their health information
- It sets boundaries on the use and release of health records
- It establishes security safeguards that health care providers and others must achieve in protecting the privacy of health information
- It provides for accountability, with civil and criminal penalties that can be imposed if privacy standards are violated
- And it strikes a balance where public responsibility requires release of some forms of data - for example, to protect public health.

For patients - it means being able to seek care without fear that personal health information may be misused:

- It gives patients the right to control release of their medical information.
- It provides patients the right to a notice from their health plan or provider explaining how their personal health information is used and shared.
- It enables patients to find out what disclosures of their information have been made.
- It limits release of information to the minimum needed for the purpose of the disclosure.
- It ensures patients' right to examine their own health records and request corrections.

For our health care system - it means we will be able to realize the benefits and savings of electronic storage and transfer of records without jeopardizing the privacy of personal medical information.

Q: Are the rules the same for especially sensitive information, such as psychiatric conditions, substance abuse and/or HIV status?

A: Many states have passed laws that establish more stringent protections for certain types of information, and these national standards would not pre-empt those protections. We also do not preempt state laws that may require patient consent for disclosure of certain information, such as mental health records, even for treatment or payment purposes.

In general, we believe that all individually identifiable health information is potentially sensitive and therefore must be protected. **However, we are requiring additional protections for two kinds of information.** To protect psychological notes, which aren't needed by health plans or many other health care providers in order to provide treatment or pay for care, we require specific patient authorization for their disclosure by the practitioner who created them to any other person, including other health-care providers.

Second, we provide additional protections for research information unrelated to treatment, because, by definition, that information is not needed for treatment or payment purposes. This might include genetic information that is collected during a clinical trial, where the purpose is not to advance the patient's treatment but to identify a genetic marker for the underlying disease or condition. This **heightened** protection should allay researchers' concerns that patients would not participate in this type of genetic research if the results could be disseminated throughout the health-care system.

Q: By putting so many exceptions into law, aren't you opening up access to records instead of closing it off?

A: The regulation does not -- and cannot -- reduce current privacy protections.

In fact, the law that allowed us to develop these regulations specifically mandates that the regulation will not preempt state laws that are more protective of privacy.

Overall, this regulation ensures national minimum requirements for federal privacy protections far beyond what has been in place in the past , while preserving any additional protections offered by various state laws.

Q: Why did you move from prohibiting written patient consent to requiring it?

A: One of our guiding principles has been to give consumers clear control of their personal medical information.

People are more comfortable with this type of system, which reflects what typically takes place today in a doctor's office -- patients are used to signing a routine consent form when they first visit a provider.

After reviewing the comments, we realized that it made more sense for patients to give consent to their treating health care providers even for routine uses of their medical records - for treatment, payment or health-care operations.

The final rule however, requires a higher standard - with special, separate authorization by the patient - for other disclosures not related to treatment and payment, such as for certain marketing purposes or to employers. This higher standard reflects what most patients expect when they seek medical treatment: that there be clear boundaries separating what they tell their doctors for treatment purposes from what gets used for unrelated purposes.

The final regulation also requires providers to give patients written notice about their medical privacy policies and patients' privacy rights.

Q: Could providers or insurers refuse to treat or cover patients who refuse to give their consent?

A: As they can today, under the rule a provider could refuse to treat a person who would not consent to the use or disclosure of their health information for treatment, payment and related purposes. We do not require health plans to obtain a consent in order to enroll members, but if they do request a consent to use information and are refused, they also may deny enrollment. This is also the same as today's situation. However, experience indicates this is not a serious or wide-spread problem. The regulation does include provisions for emergency care and other situations, to ensure that providers will be able to treat patients when consent cannot be given.

The regulation does prohibit providers and health plans from denying services or coverage if they request an authorization to use or disclose information for other types of activities and the individual refuses.

Q: What does this regulation require the average provider to do? Does it create new burdens for doctors and hospitals?

A: This regulation strikes a common-sense balance that ensures privacy protections for patients, while keeping burdens on providers to a minimum. We want to make it easy to use medical information for health purposes, and difficult to use it for other purposes.

The regulation sets overall standards - but its provisions are flexible and "scalable," so they allow different entities to meet the standards in different ways that work for their individual nature and size. The basic goal is simply to ensure that every provider focuses clear attention on privacy needs and achieves the basic privacy standards.

Also, one of the most problematic provisions of the NPRM, requiring providers to limit disclosures *for treatment*, has been eliminated in the final rule.

For the average provider, the regulation will require:

- providing information to patients on how their information will be used, and their privacy rights
- adopting clear privacy procedures for their practice or hospital
- providing enough training so that employees understand those procedures
- designating an individual to be responsible for ensuring the procedures are followed
- assuring that records are secure, and not available to those who DON'T need access to them
- obtaining consent to share information for health related purposes, as is commonly done today.

Covered entities will have two years to prepare, before the regulations come into force. HHS will work with the health care community to help providers comply.

Q: How will this effect pharmacy benefit management, which oversee drug benefits, and/or disease management, which may use patient data to target special programs to serve specific types of patients, such as those with diabetes or asthma?

A: If these activities are done for a health plan or covered provider, they would be subject to these rules just like other health care operations.

Under the regulation, health plans and providers will need to make sure that their business associates, including PBMs or disease management providers, protect their patients' private medical information. If a business associate fails to respect those agreed-upon standards, a plan or provider must be prepared to demand corrections or end the business relationship.

Scope of the Rule

Q: Why have you elected to cover all records, including paper-only records? What gives HHS authority to regulate so widely? (Why did your NPRM press release say you didn't have the authority to do this?)

A: In our proposed rule, we specifically asked for comment on this provision. We received thousands of comments in response, and they overwhelmingly favored a comprehensive system that protected all records. When we re-examined our proposal, especially from the standpoint of the individual patient, we agreed with the comments.

Protection for all records creates a system that is not only more comprehensive, but also more workable and easier to understand, for patients and providers alike. Protecting all records, including paper ones, under the same set of rules both strengthens the privacy protections and simplifies the requirements for providers.

Background

The proposed rule provided protection for paper records that had at some point existed in electronic form - but it did not extend to paper records which had never existed in electronic form. However, in our proposal, we made clear that HHS has the authority to extend protection to all personal health records, and GAO has concurred with that finding.

[If asked: Our press release accompanying the NPRM was also wrong - it said HHS didn't have authority to cover paper-only records, but the NPRM itself made clear that we do have the authority]

Q: Why did you decide to cover all individually identifiable health information in any form? Does the Secretary have the authority to apply the rule to "paper records"?

A: First, let's be clear about what kinds of information the proposed rule would have covered. We had proposed to apply the rule to individually identifiable health information that was or had been electronically transmitted or maintained by a covered entity.

The provisions would have applied to the information itself, referred to as protected health information in the rule, and not to the particular records in which the information is contained. We proposed that once information was maintained or transmitted electronically by a covered entity, the protections would follow the information in whatever form, including paper records, in which it existed while held by a covered entity.

The only form of information that the proposal would not have applied to would have been information that never had been electronically maintained or transmitted by a covered entity.

In the final rule, we extend the scope of protections to all individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity. This includes even individually identifiable health information in paper records that never has been electronically stored or transmitted. (Of course, information, whether electronic or paper, held by an entity not covered by the rule, would not be affected by the rule.)

In the NPRM, we explained that the Secretary has the legal authority to cover all forms of individually identifiable health information held by a covered entity, but we stopped short of covering "purely paper" health information and invited comment.

A substantial number of commenters urged the Department to expand privacy protection to all individually identifiable health information, regardless of form. They asserted that expanding the scope of covered information under the rule would increase patient confidence in their health care providers and the health care system in general. They also argued that a more uniform standard which covered all records would reduce the complexity, burden, cost, and enforcement problems that would result from treating electronic and non-electronic records differently.

Q: What about health information that is "discussed orally"? Isn't it going too far to apply the rule to such information?

A: Congress explicitly included "oral" information in the statutory definition of health information, and therefore we have covered it.

Furthermore, the rule would leave a huge gap in the confidentiality of people's health information if it did not apply protections to information simply because it is conveyed orally.

Q: How does this regulation effect medical records or PHI transmitted across the Internet?

A: Patients should not -- and will not -- lose their privacy rights simply because they provide protected medical information over the Internet. To the extent that online companies are health-care plans, clearinghouses, or providers -- such as Internet pharmacies -- they must meet these national privacy standards just like their bricks-and-mortar counterparts. In other cases, they could qualify as "business associates" of a health plan or provider, and therefore would need to follow its privacy policies.

Again, as in other areas, our reach is limited. This is another area which would benefit from the enactment of comprehensive privacy legislation.

Q: The proposed regulation only applied to health-care providers, health plans and health-care clearinghouses. What happens if others who aren't covered obtain and misuse personal medical information?

A: HIPAA only allows us to establish privacy standards for health care providers, health plans and health care clearinghouses.

However, to provide the greatest protection these regulations also require those covered groups to require their business associates take appropriate steps to protect patient privacy.

All health plans and providers must ensure that their contractors and other business associates use or share sensitive information responsibly, and to include those protective provisions in their contracts. If their business associates (eg., administrators, billing firms, accountants and lawyers) violate those agreements, doctors and health plans would need to take action.

It would be much simpler to regulate these other businesses directly, rather than through their relationships with providers or health plans, but HIPAA does not give us the authority to do so.

Q: If it's so obvious that all paper records should be covered, why didn't you proposed that to begin with?

A: We proposed the minimum level of protection that we believed could work, and asked for comment. We learned from the comment that extending coverage to all paper records was necessary.

In the absence of comprehensive privacy legislation, we believed it was our responsibility to put forward a rule which would provide the greatest protection possible.

Q: How important is this "all paper records provision?" Are most records still in paper form?

A: We don't know actually know the number or percent of records which exist only in paper form.

Requiring protection of all paper records is important because (as the comments told us) we need to have a coherent, workable system - not a fractured system that treats some records one way and some another way.

We expect the number of paper-only records to decrease as the health care system, like the rest of our world, becomes more and more electronically based.

Q: Where does HHS get the legal authority to extend coverage to paper records?

A: HIPAA called on Congress to enact health information privacy legislation, and in the absence of legislation, required HHS to promulgate these regulations.

As we stated in the proposed rule, HIPAA itself calls for protection of individually identifiable health information. The statute did not limit these protections to information in electronic files. The GAO agreed with our assessment, as did most of the commenters.

Q: Are tissues/biological material protected under this rule?

A: Tissues and biological materials are not themselves protected but any descriptions of them, including test results, are protected if the information is held or disclosed by a covered provider or health plan. For example, the rule does not cover cells taken for testing, but it does protect the written information that names the person whose cells are tested and the results of the test.

Interaction with State Law

Q: How does the regulation change current law? Will this regulation pre-empt state laws?

A: This is the first time federal law will provide for national protection of medical records privacy. The privacy of Americans is protected in their bank transactions, their credit card statements, and even their video rentals. Yet, until now, Americans have had no federal privacy protections for medical records - some of our most personal information.

Today there is a patchwork of different state laws on medical records privacy. The new regulation will for the first time provide a nationwide standard of protection, and it will pre-empt state law in those instances where the state provisions are weaker than the regulation. However, in those instances where states have provided stronger privacy protection than the regulation, the state law will continue to prevail.

Q: Do you know if you are preempting any State laws?

A: We don't believe that we have preempted very many state laws. The preemption structure under HIPAA establishes a federal floor. So, state laws which provide consumers with greater protection than these regulations will take precedence. Also, if a state has mandated a type of disclosure to address a specific health need of their populations, we have given deference to such laws.

Q: Won't it be confusing and costly for providers to comply with the federal standards as well as potentially 50 different state standards?

A: These regulations provide a national foundation of protections for all Americans, while allowing states the freedom to respond to the unique concerns of their residents. As HIPAA provides, these privacy standards pre-empt state laws except in those cases where states have stronger privacy protections (with some exceptions for public health activities).

We believe this is a good approach. Providers will simply need to comply with these comprehensive national standards in addition to meeting the additional state protections that they already follow today.

Q: What are the rules on releasing personal health data to law enforcement officers? Will police be able to obtain people's health information without their consent?

A: Just like free speech rights, privacy rights can not be absolute. Our goal has been to guard the privacy of health information while promoting our public responsibilities, including law enforcement.. In order to strike the right balance, the privacy regulation includes narrow provisions for law enforcement – to protect public safety, and for investigating health care fraud and abuse.

Generally under the rule, covered entities may disclose records to law enforcement officials only following a warrant or other written legal order. This ensures that they can continue to protect the public as we give consumers strong privacy rights.

Background: In a few emergency cases, a legal process may be followed that would not require a written order. For example, when information about a victim's medical condition is needed immediately, no warrant or similar process is required. Where officials are seeking to identify a suspect, fugitive, material witness or missing person, then limited identifying information can be released, which could then form the basis for obtaining a search warrant or other legal requirement.