Order Code RL30620

CRS Report for Congress
Received through the CRS Web

Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations

Updated June 14, 2001

C. Stephen Redhead
Specialist in Life Sciences
Domestic Social Policy Division

Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations

Summary

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) instructed the Secretary of Health and Human Services (HHS) to issue standards to support the electronic transmission of health information. HIPAA also gave Congress 3 years to enact health privacy legislation, otherwise the Secretary was required to develop health privacy standards. Congress failed to meet its own deadline, so Clinton Administration issued a health privacy rule on December 28, 2000. The rule took effect on April 14, 2001.

The privacy rule gives patients the right to inspect and amend their medical records and restricts access to and disclosure of individually identifiable health information. Health care providers must obtain a patient's general consent to use or disclose their medical information for treatment, payment, and other health care operations. In addition, both health plans and providers must obtain a patient's specific authorization in order to use and disclose information for non-routine and most non-health care purposes. The rule specifies certain national priority activities for which health information may be disclosed without a patient's authorization.

Hospitals, health insurers, and pharmaceutical companies claim the privacy rule will compromise patient care by placing unacceptable restrictions on access to health information and be extremely costly to implement. They are especially critical of the rule's general consent provision and the requirement that, with the exception of treatment-related disclosures, providers and health plans use or disclose no more than the minimum amount of information necessary to accomplish the intended purpose. Industry groups have also criticized the rule for requiring providers and plans to enter into contracts with their business associates to ensure that these groups, which are not directly covered under HIPAA, adhere to the same privacy protections. In response to industry concerns, HHS will soon release a guidance document to help covered entities implement the privacy rule. Patient privacy advocates strongly support the rule, though they too have concerns. HIPAA did not grant HHS the authority to cover all entities that handle medical information, nor did it give patients the right to sue for violations of their health information privacy. Consumer advocates have urged HHS not to weaken any of the rule's privacy protections.

Under HIPAA, HHS is also developing electronic health information standards. On August 17, 2000, HHS issued standards that specify the content and format for electronic health care claims and other common health care transactions. The transactions standards are intended to reduce the administrative burden on health plans and providers, which today exchange information using many different paper and electronic formats. On August 12, 1998, HHS proposed a set of administrative, physical, and technical security standards, which health plans and providers must include in their operations to safeguard confidential patient information against unauthorized access, use, and disclosure. A final security rule is expected later this year. Lawmakers have introduced two bills (S. 836, H.R. 1975) that would delay implementation of HIPAA until all the standards and enforcement regulations, with the exception of the privacy rule, are published in final form.

Contents

List of Tables

Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations

Introduction

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, P.L. 104-191, 42 U.S.C. 1320d) instructed the Secretary of Health and Human Services (HHS) to develop standards to support electronic data interchange for a variety of administrative and financial health care transactions. The intent of the legislation is to improve health care system efficiency and effectiveness, make it easier to detect fraud and abuse, facilitate access to health and medical information by researchers, and reduce administrative costs.

HIPAA's Administrative Simplification provisions required the Secretary to issue regulations to establish standard electronic formats for billing and other common transactions, including the use of uniform data codes for reporting diagnoses, referrals, authorizations, and medical procedures. The legislation also mandated the development of unique identifiers (i.e., ID numbers) for patients, employers, health plans, and health care providers. In addition, HIPAA required the Secretary to issue security standards, including an electronic signature standard, to safeguard confidential health information against unauthorized access, use, and disclosure. Finally, the legislation included a timetable for Congress and the Secretary to develop comprehensive medical records privacy standards to give patients the right to access their health information and control of use and disclosure of such information by others.

The Administrative Simplification provisions cover health plans, health care clearinghouses (i.e., entities that facilitate and process the flow of information between providers and payers), and health care providers who transmit health information electronically. Covered entities have up to 24 months to comply with the standards established by the regulations. Small health plans with annual receipts of $5 million or less have an additional 12 months to comply. Although HIPAA does not mandate electronic transmission of health information, the standards are intended to catalyze the health care industry's gradual shift away from paper-based medical records and transactions to electronic record keeping and data transmission. **Table 1** provides a summary of all the Administrative Simplification provisions in HIPAA, including civil penalties for failure to comply with the standards, and criminal penalties for wrongful disclosure of personally identifiable health information.

This report is divided into two sections. The first section provides some background on electronic health information security and privacy. The second section describes each of the HIPAA Administrative Simplification standards, including the

status of their implementation. To date, HHS has issued two final rules: electronic transactions and code sets; and privacy. The agency has also proposed standards for security and electronic signatures, and for unique employer and provider identifiers. There is an expanded discussion of the privacy rule, which has generated a great deal of public debate and congressional interest.

Electronic Interchange of Health Care Information

Uses and Transmission of Health Information

The U.S. health care industry is made up of more than 12 million providers, payers, researchers, and suppliers in more than 500,000 companies, nonprofit organizations, and research facilities. The transition from fee-for-service health care to managed health care has fueled enormous growth in the demand for patient data by an increasing number of entities. The development of integrated health care delivery systems has, in turn, led to the development of large, integrated databases of personal health information. With access to these data, people are seeking new and improved ways to deliver effective care, identify and treat those at risk for disease, conduct research, assess and improve quality, detect fraud and abuse, and market their services (see text box on following page).

However, today's health care system is still largely paper-based and unstandardized. By some estimates, paperwork alone accounts for more than 20% of all health care costs. In addition, health care providers spend a significant amount of their time filling out forms rather than attending to additional patients. Routine tasks, such as filing a claim for payment from an insurer, checking insurance eligibility for a particular treatment, or responding to requests for additional information to support a claim, can involve numerous paper forms and telephone calls. Physicians often bill multiple health plans, each of which may use a different format for its claims forms. Paper-based medical records confine medical history to one physical location, which may limit patients' ability to share their medical information with other physicians and specialists in order to receive the best possible diagnosis and treatment.

The nation's health insurance payers have employed an enormous variety of formats and data requirements to handle claims and other transactions. Competing parties have developed proprietary formats for electronic data interchange, but there is no uniform set of standards.[1] Under HIPAA, HHS has mandated the adoption of standardized electronic formats for several common health care transactions (e.g., health plan enrollment, health insurance claims, payment and remittance), and the use of five medical data code sets for encoding data elements in those transactions. The industry estimates that full implementation of the transactions standards could yield a net savings of up to $9 billion a year by reducing administrative overhead, while at the same time helping improve the quality of health care by freeing up resources now devoted to paperwork and administration. Adoption of the HIPAA-mandated electronic transactions and codes standards is also likely to increase substantially the

---

[1]HHS estimates that there are about 400 formats for electronic health care claims currently in use in the United States.

use of electronic data interchange (EDI) in health care and help move the country towards the eventual replacement of paper-based transactions with EDI. Details on the status of the standards for electronic transactions, code sets, and unique identifiers appear later in the report.

Growing Uses of Health Care Information

Primary users of health care information include physicians, clinics, and hospitals that provide care to patients. Patients provide background medical information to their physicians, who use it to develop treatment plans and order diagnostic tests. Physicians maintain detailed records of medical services provided to patients. Hospitals and clinics use health care information to provide patient care ordered by physicians and maintain ongoing records of medical services provided. In order to be reimbursed by health insurers, health care providers submit claims that often include detailed information about a patient's diagnosis, treatment, and prognosis.

Secondary users of health care information include organizations that pay for health care benefits, such as traditional fee-for-service health insurance companies, managed care providers, and government programs, like Medicare and Medicaid. These health care payers also use health care information to analyze the cost and quality of health care delivered by providers, and to prevent fraud and abuse. Other secondary users of health information include medical and social science researchers, employers, and public health services, who use the information for purposes such as researching the costs and benefits of alternative medical interventions, determining eligibility for social programs, and understanding state and local health care needs. Much of the health data available to secondary users specifically identifies individual patients.

The expansion of managed care has stimulated a demand for patient data that could barely be imagined a decade ago. Managed care organizations (MCOs) operate on the principle that by monitoring and controlling patient care, they can deliver care more efficiently and reduce costs. To achieve these objectives, many different groups employed by or under contract to MCOs must analyze patient data for a wide variety or purposes, including utilization review (How are participating providers using services?), risk management (Is the MCO at legal or financial risk?), and quality assessment (How can patient care and outcomes be improved?).

Health Information Security

There has always been a need to protect confidential medical information against unauthorized access and disclosure. For paper records, physical protections such as locks, safes, and controlled-access buildings often provided adequate security. In addition, the time and effort required to copy extensive health records and transport them from one location to another effectively discouraged widespread dissemination and disclosure of health information. But those safeguards may also impede the delivery of quality patient care, because important information is not always available when and where it is needed. While electronic data interchange holds great promise for improving health care delivery, it also raises serious security concerns. Digital records may easily be copied, modified, or viewed remotely by people seeking to misuse the information. Health information that used to be protected by physical

means can now be copied and transmitted across the country with the click of a mouse.

Information technology experts estimate that more than 120 eHealth companies were created in 1999. They predict that within a few years we will be able to access all our medical information online from our homes and offices. Routine tasks such as selecting physicians, identifying medical care options, viewing medical test results, and scheduling appointments will be conducted over the Internet. Hospitals, physicians, and health insurance companies will also conduct business over the Internet. However, the health care industry lags behind other industries (e.g., financial services) in implementing security technologies to protect electronic health information. Without appropriate security processes and technologies in place, security threats to electronic health information are likely to increase dramatically.

There are many different components that are required to establish and maintain information security both in the paper world and the digital world. For any domain, there must be an authority that creates an identity for itself and issues identities at lower levels. For example, a private company may issue employee identity cards that enable access to facilities, benefits, or systems within the company. Those identities would not be valid at a government facility because the private company has no authority outside its own domain. Identities issued by authorities are part of the authentication process, by which individuals are positively identified in order to gain access to information systems. An identity is only valid if the person or system that is authenticating it recognizes the authority of the issuing body.

Signed paper documents and identification cards, such as a driver's license, are often used to verify a person's identity. People trust a driver's license because they are aware of the steps required to obtain one and they recognize that there are controls in place to protect against modification and forgery. Authentication is more difficult in the digital world, because information can be more easily obtained, copied, and modified. User passwords are a common form of authentication used by digital information systems, but they are easy to obtain and exploit. Digital signatures (discussed below) and biometrics (i.e., use of unique physical attributes such as fingerprints, or retina patterns), though more expensive and difficult to implement, provide a very high degree of authentication. Once a user's identity has been authenticated, that individual may then receive authorization to access, modify, create, or delete information within a system.

Confidentiality and Cryptography. In digital information systems, confidentiality can be achieved through the use of cryptography (i.e., disguising a message with code). To send a message via insecure channels, the message is encoded, or encrypted, using a cryptographic formula called an encryption key. The resulting encrypted message can only be unscrambled, or decrypted, using a decryption key, which is either the same as the encryption key or mathematically related to it. With cryptography, any kind of digital information — text, data, voice, images — can be encrypted. There are two types of cryptography.

In **secret key cryptography**, the key used by the sender to encrypt the message is also used by the recipient to decrypt the message. Both parties must therefore arrange to share the same key. If the key has to be transmitted from the sender to the

recipient, both parties must ensure that the transmission system is secure so that the key cannot be intercepted.

In **public key cryptography**, each person gets a pair of keys, a private key and a public key. The private key is kept secure, known only to the user, while the public key is published in the electronic equivalent of a telephone book. To use this kind of system, the sender encrypts the message using the recipient's public key. The message can only be decrypted by the recipient using her private key. Public key cryptography thus permits the secure transmission of information across open networks, such as the Internet, without senders and recipients having to exchange secret keys.

Public key cryptography requires an infrastructure (Public Key Infrastructure, or PKI) to support the information technology applications and manage the generation, certification, and distribution of public and private keys. For more information on cryptography and encryption, see CRS Issue Brief IB96039, *Encryption Technology: Congressional Issues* (updated regularly).

While encryption ensures confidentiality, it does not by itself guarantee data integrity and non-repudiation. Integrity is the assurance that a message remains unaltered during transit and storage. For example, sealing an envelope provides some guarantee of integrity for paper documents. Non-repudiation is the guarantee that a particular transmission actually occurred, and that neither the sender nor the receiver are able to deny it. In the digital world, integrity and non-repudiation are accomplished through the use of digital signatures.

Digital Signatures. A digital signature is a type of electronic signature that is attached to an electronic document to provide authentication of the signer's identity, much like a handwritten signature on a printed document. The recipient of a document with a digital signature is able to verify that the document did indeed originate from the person whose signature is attached (i.e., sender authentication) and that the document has not been altered since it was signed (i.e., data integrity). Moreover, digital signatures cannot be repudiated, that is, the signer of a document cannot later disown it by claiming it was forged (i.e., non-repudiation). The use of digital signatures grew out of the development of public key cryptography (see text box on the following page). Digital signatures are an important component of information security systems and their use, though not widespread, is growing rapidly. For more information about digital signatures and other electronic signature technologies, see CRS Report RS20344, *Electronic Signatures: Technology Development and Legislative Issues* (updated regularly).

HIPAA's Administrative Simplification provisions instructed the Secretary to issue security standards to ensure the integrity and confidentiality of electronic health information, and to protect such information against unauthorized use and disclosure. The law also required the Secretary to develop an electronic signature standard. The provisions and implementation status of the proposed security and electronic signature rule are summarized below.

What is a Digital Signature?

A digital signature is a method of authenticating electronic documents that combines the use of public key cryptography with mathematical algorithms known as hash functions. When you apply a hash function to a document, it creates a concise digital fingerprint of the document called a message digest. The message digest is of fixed length, regardless of the length of the original document. Hash functions are designed so that a small change in the document produces a large change in the resulting message digest. Once you have created a message digest from a document, you cannot re-create the document from the digest.

To create a digital signature, the sender first passes the document through a hash function to produce a message digest. The sender then encrypts the message digest using her private key. The result is a digital signature, which is appended to the original document (which the sender may also encrypt using her private key). The document is then transmitted to the intended recipient, who decrypts the digital signature using the sender's public key to change it back into a message digest. The recipient creates a second message digest by passing the document through the same hash function as used by the sender.

The recipient then compares the two digests. If they are identical, the recipient can be sure that the document was not altered during transmission. Because the sender is the only individual with access to the private key used to encrypt the digest, the recipient is also assured that the information has indeed been sent by the sender, who is unable to deny that fact. Although the entire process sounds complicated, in practice it requires little more than selecting an icon on a computer screen.

Health Information Privacy

The growing use of information technology in the management, administration, and delivery of health care has led to increasing public concern over the privacy of medical information. Polls indicate that people are worried about who has access to their medical records without their express authorization. They fear that their personal health information will be used against them to deny insurance, employment, and housing, or to expose them to unwanted judgment and scrutiny.[2]

Information privacy, as distinct from information security, may be defined as the right of individuals to determine when, how, and to what extent they will share personal information about themselves with others. Use and disclosure of anonymized information, from which all personal identifiers have been removed, is generally not considered to compromise privacy. The degree of privacy protection afforded to personal medical information provided to a physician or health insurance company by a patient varies from state to state. There is no comprehensive federal law that protects the privacy of medical information.[3]

---

[2]A national survey conducted by Princeton Survey Research Associations and released in January 1999 found that one in five people believe that their personal health information has been used inappropriately, without their knowledge or consent.

[3]The Privacy Act of 1974 (5 U.S.C. 552a) protects personally identifiable information (continued...)

Advocates of strong privacy protection insist that patients be given the ability to deny access to their medical information to virtually any third party. They also seek to prohibit health care plans and providers from requiring patients to waive those rights as a condition of participation in the health care system. But health plans, researchers, pharmaceutical companies, and others argue that too much privacy (i.e., strict patient consent requirements for the release of personally identifiable health information) may suppress the flow of information and stifle efforts to improve the quality and efficiency of health care.

The implied conflict between patient privacy protection and the promotion of health care quality and efficiency may be an exaggeration. There is growing evidence from polls and surveys that some people are withdrawing from full participation in their own health care because they are afraid their health records will be disclosed to employers and others and lead to discrimination, loss of benefits, stigma, or unwanted exposure. A January 1999 survey by the California Health Care Foundation found that one of every six people engaged in some form of privacy-protective behavior, including lying to their doctor, refusing to provide information or providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out-of-pocket for care that is covered by insurance, or avoiding care altogether. As a result, patients risk inadequate medical care, and the data disclosed and used for payment, outcomes analysis, research, and public health reporting are compromised. Thus, some advocates argue that strong privacy protection goes hand-in-hand with promoting health care quality, access, and efficiency.

House and Senate conferees added privacy language to the Administrative Simplification provisions of HIPAA during the bill's conference, after lawmakers had failed to pass stand-alone health privacy legislation. HIPAA required the Secretary to report to Congress by August 1997 on ways to protect the privacy of personally identifiable health information. It then gave Congress until August 21, 1999 to enact health privacy legislation. If Congress failed to act, then the Secretary was instructed to issue health privacy regulations by February 21, 2000.

The Secretary presented her recommendations on health privacy legislation to Congress on September 11, 1997, at a hearing before the Senate Committee on Labor and Human Resources.[4] The recommendations were intended to serve as guidance to Congress in developing comprehensive privacy legislation. The Secretary outlined the following five key principles as being fundamental to the protection of personally identifiable health information:

- Boundaries: Limit, with few exceptions, the use of an individual's health information to health purposes only.

---

[3](...continued)
collected and held by federal agencies. Federal law also provides substantial privacy protection for people who receive drug and alcohol treatment at federally funded clinics (42 U.S.C. 290dd-2). Several other statutes provide limited protection under specific circumstances.

[4]The Secretary's report on the confidentiality of personally identifiable health information is available online at [http://aspe.os.dhhs.gov/admnsimp/pvcrec.htm].

- Security: Require organizations that handle health information to provide adequate security against unauthorized access, disclosure, and misuse.
- Consumer Control: Provide patients with the right to inspect, copy, and, if necessary, correct their health information, and provide patients with details of who has access to their information, how that information will be used, and how they can restrict or limit access to it.
- Accountability: Penalize those who misuse health information and provide redress for those harmed by improper use and disclosure.
- Public Responsibility: Balance privacy protections with public responsibility to support national priorities, including public health and safety, research, and law enforcement.

Several health privacy bills were introduced during 1999, but lawmakers were unable to meet the HIPAA-imposed deadline for enacting comprehensive health privacy legislation.[5] In June 1999, the Senate Committee on Health, Education, Labor, and Pensions delayed indefinitely an attempt to mark up a health privacy bill after lawmakers failed to agree on whether to give patients the right to sue over breaches of medical record confidentiality, and whether to allow preemption of all state health privacy laws. With the failure of Congress to meet its self-imposed deadline, the Secretary proceeded to develop health privacy regulations based on the five principles outlined in her report to Congress.

HHS issued a proposed rule on November 3, 1999. At the request of several health care groups, the 60-day public comment period was extended by an additional 45 days, during which time the agency received more than 52,000 comments. Numerous stakeholders provided extensive comments on the proposed rule, including patient privacy advocates, health care providers, standards and accrediting organizations, government entities, health care clearinghouses, employers, health plans, and research and pharmaceutical groups. HHS issued a final health privacy rule on December 28, 2000. An overview of the rule's provisions and a discussion of some of the key concerns and issues raised by stakeholders is provided below.

HIPAA's Administrative Simplification Standards

Electronic Transactions and Code Sets

On August 17, 2000, HHS published a final rule to implement standards for electronic health care transactions.[6] The standards are intended to reduce the administrative burden on health plans and health care providers, which today exchange information using many different paper and electronic formats. Each standard specifies the content and format of a common administrative or financial transaction between health plans and health care providers. The eight transactions

---

[5]The following health privacy bills were introduced in the 106th Congress: S. 573 (Leahy), S. 578 (Jeffords), S. 881 (Bennett), H.R. 1057 (Markey, identical to S. 573), H.R. 1941 (Condit), H.R. 2404 (Murtha), H.R. 2455 (Shays), and H.R. 2470 (Greenwood).

[6]65 *Federal Register* 50311–50373.

covered under the rule are: health care claims; eligibility for health care; referral certification and authorization; health care claim status; enrollment and disenrollment in a health plan; health care payment and remittance advice; health plan premium payments; and coordination of benefits.[7] The rule defines the specific standard to be used for each transaction, the standard-setting organization whose standard must be used, and where implementation specifications can be obtained.

HIPAA required the Secretary, where possible, to adopt standards developed by private standards development organizations (SDOs), which are accredited by the American National Standards Institute (ANSI). HHS chose to use standards developed by the Accredited Standards Committee (ASC) X12N, except for the standards for retail pharmacy transactions, which are from the National Council for Prescription Drug Programs (NCPDP).[8] Both sets of standards are already in widespread use.

All health plans (except for self-administered, employer-sponsored plans serving fewer than 50 employees) and health care clearinghouses, and all health care providers that choose to submit or receive a HIPAA-covered transaction are required to use these standards. Neither HIPAA nor the final rule requires physicians or other providers to submit transactions electronically. However, if they submit a HIPAA-covered transaction electronically, it must comply with the standard specified in the rule. Health care clearinghouses may accept non-standard transactions for the sole purpose of translating them into standard transactions for sending providers, and may accept standard transactions and translate them into non-standard transactions for receiving providers.

The rule names six organizations that have agreed to serve as Designated Standards Maintenance Organizations (DSMOs).[9] These organizations will evaluate requests for changes to the standards and make recommendations for the Secretary's consideration. Under HIPAA, the Secretary may modify a standard no more frequently than once every 12 months.

In addition to the standards for electronic transactions, the rule adopts several widely used code sets for encoding data elements in the transactions. Medical data code sets include diagnostic codes and medical procedure codes. The code sets adopted under the rule are:

---

[7]HIPAA required the Secretary to adopt standards for two additional transactions: first report of injury, and health claims attachments (i.e., extra documentation, such as operative notes, pathology reports, or medical history, used to support or supplement a request for payment). The first report of injury standard was not finalized because an implementation guide was not available in time. HIPAA gave the Secretary an extra 12 months to issue a claims attachments standard.

[8]ACS X12 was chartered by ANSI in 1979 to develop and promote standards to facilitate the electronic exchange of data. The "N" denotes the insurance subcommittee.

[9]The six DSMOs are: Accredited Standards Committee X12; Dental Content Committee; Health Level Seven; National Council for Prescription Drug Programs; National Uniform Billing Committee; and National Uniform Claims Committee.

- International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2, for diagnosing diseases, injuries, impairments and other health problems, and identifying their causes.
- International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volume 3, for reporting inpatient medical procedures by hospitals.
- Current Procedural Terminology, 4th Edition, (CPT-4), and Health Care Financing Administration Procedure Coding System (HCPCS), Level 1, for reporting physician services and other health care services (e.g., radiological procedures, clinical diagnostic tests, hearing and vision services).
- Health Care Financing Administration Procedure Coding System (HCPCS), Level 2, for reporting all other substances, equipment, supplies, or other items used in health care services (e.g., medical supplies, orthotic and prosthetic devices, durable medical equipment).
- Code on Dental Procedures and Nomenclature, 2nd Edition, for reporting dental services.
- National Drug Codes (NDC) for reporting prescription drugs and biologics.

The rule eliminates the use of local HCPCS codes (i.e., Level 3), which state Medicaid programs and other health insurers have developed to identify many of the services for which they pay. Public and private insurers may submit local codes to HCFA for review and inclusion in the appropriate national code set. Local codes generally fall into one of three categories. The first category includes local codes that are basically the same as existing national codes that describe services commonly provided by other payers. These local codes are sometimes used to facilitate special payment arrangements with certain providers. Secondly, there are local codes that reflect services, including new and emerging technologies (e.g., telemedicine), that are covered by state Medicaid programs and other payers, for which no national code currently exists. Finally, many local codes are used to describe special or unique services covered by a state Medicaid program, but not generally covered by other health insurers. For example, Medicaid Home and Community-Based Waiver programs may cover a wide range of non-medical services such as case management, homemaker services, respite care, and transportation.

In November 1999, the National Association of State Medicaid Directors established the National Medicaid EDI HIPAA (NMEH) Workgroup to assess the impact of HIPAA's Administrative Simplification standards on state Medicaid programs. Using a 49-state database of local codes, workgroup participants have prepared a consolidated and prioritized list of a few thousand codes to submit to the HCFA HCPCS Committee. Medicaid officials question whether HCFA currently has the resources to process such a large submission in a timely manner. They are concerned that states will have to continue to use local codes beyond the compliance deadline.

The electronic transactions and code sets rule took effect on October 16, 2000. Covered entities have 2 years to come into compliance (i.e., October 16, 2002). Small health plans with a maximum of $5 million in annual receipts have an additional year to comply (see **Table 2**). HCFA estimates that the rule will provide a net savings to the health care industry of $29.9 billion over 10 years.

National Provider Identifier

HHS proposed standards for a national health care provider identifier on May 7, 1998.[10] Under the proposal, each provider would be required to use a unique eight-character, alphanumeric identifier on all health care transactions, including electronic ones.[11] The identifier would contain no embedded intelligence (i.e., no information about the provider). At present, health plans assign identification numbers to health care providers. Providers that do business with multiple health plans often have multiple identification numbers, which can slow administrative activities and increase costs.

National provider identifiers would be issued by the National Provider System (NPS), based on information entered into the NPS by one or more organizations known as enumerators. HHS asked for comment on whether a federally directed registry should act at the sole enumerator of all health care providers nationwide, or whether a combination of federal and state entities should act as enumerators. HHS received and reviewed about 5000 public comments on its proposal and expects to issue a final rule later this year (see **Table 2**).

National Health Plan Identifier

A Notice of Proposed Rulemaking (NPRM) for the national health plan identifier is under development at HHS and is expected to be published later this year (see **Table 2**).

National Employer Identifier

In a June 16, 1998 NPRM, HHS proposed adopting the Employer Identification Number (EIN) to identify employers in all health care transactions.[12] The EIN is a nine-digit taxpayer identification number for employers that is assigned by the Internal Revenue Service. Unlike the social security number, the EIN does not contain any embedded information and is not considered confidential. EINs are freely exchanged by employers and others. HHS received and reviewed about 800 public comments on the employer identifier NPRM. The agency expects to issue a final rule later this year (see **Table 2**).

National Individual Identifier

In contrast to the public's general acceptance of the health information standards discussed above, public opinion on the unique individual identifier is deeply divided. On July 31, 1998, in response to widespread public concern, then Vice President Gore announced that the Administration would not develop a unique individual identifier until health privacy protections were in place. Lawmakers also introduced legislation

---

[10]63 *Federal Register* 25320–25357.

[11]Many commenters on the proposed rule preferred a 10-digit numeric identifier with a check digit in the last position to help detect keying error.

[12]63 *Federal Register* 32784–32798.

during the 105th Congress to repeal the HIPAA requirement for HHS to adopt standards for a unique individual identifier, but the bills died in committee without hearings.[13] Congress included a provision in the FY1999 Omnibus Appropriations Act (P.L. 105-277) that prohibited HHS from developing a unique individual identifier standard until legislation is enacted specifically approving the standard. The same provision appeared in the FY2000 Consolidated Appropriations Act (P.L. 106-113) and again in the FY2001 Consolidated Appropriations Act (P.L. 106-554).[14]

HIPAA recognized the unique identifier for individuals as an essential component of administrative simplification. Evidence suggests that the use of a unique individual identifier would improve the quality of health care and reduce administrative costs. Today, organizations and individuals involved in health care, including health insurance companies, health plans, managed care organizations, clinics, hospitals, physicians, and pharmacies, frequently assign identifiers to individuals for use within their systems. Those identifiers often vary among organizations, so it is not uncommon for providers and plans to use different identifiers for the same patient. Having multiple identifiers for the same individual within or across organizations may prevent or inhibit timely access to integrated information. There is substantial support within the health industry for the adoption of a unique identifier for individuals, provided there are appropriate protections against misuse and unauthorized use outside of health care.

Controversy over the adoption of a standard for a unique individual identifier has largely focused on privacy concerns. Opponents of a unique individual identifier argue that its use could facilitate access to personal information by unscrupulous employers and insurers, who might then use the information to discriminate in hiring and insuring individuals with serious or costly health problems. Proposals to use the social security number as a unique health identifier have been strongly criticized because of the concern that it would make it easier to link medical records with other information about an individual, including financial and employment data. For many advocates, privacy threats outweigh any practical benefits of adopting a unique individual health identifier, such as improved patient care or administrative savings.

In an attempt to address the controversy surrounding the use of a unique health identifier, HHS departed from its customary rulemaking process and decided to solicit information and public input on a variety of options and approaches for individual health identifiers before issuing a proposed standard. The agency released a White Paper discussing those options and planned a series of public hearings by the National Committee on Vital and Health Statistics (NCVHS).[15] The initial NCVHS hearing, which was held in Chicago on July 20-21, 1998, drew significant media attention and sparked widespread public concern, which led to the Administration's announcement

---

[13](i) H.R. 4312 (Barr), Medical Privacy Protection Act of 1998; (ii) S. 2352 (Leahy), Patient Privacy Rights Act of 1998.

[14]The provision was Section 516 of the FY1999 Labor/HHS/Education Appropriations Act, and Section 514 in both the FY2000 and FY2001 Labor/HHS/Education Appropriations Act.

[15]NCVHS serves as the statutory public advisory body to the Secretary of HHS in the area of health data and statistics [http://www.ncvhs.hhs.gov].

that it was putting development of the unique individual identifier on hold until privacy protections were issued. Even though the health privacy rule recently took effect (see discussion below), the legislative rider in this year's appropriations bill prohibits HHS from resuming work on developing a unique individual identifier.

Security and Electronic Signature

HHS proposed health information security and electronic signature standards on August 12, 1998.[16] There are no existing standards that integrate all the security components necessary to protect health information confidentiality. Therefore, HHS developed new standards, which define a set of requirements that health care plans, providers, and clearinghouses must include in their operations to ensure that electronic health information remains secure. The proposed rule also describes the implementation features that must be present in order to satisfy each requirement.

The agency received and reviewed more than 2000 public comments on the proposed standards and is expected to issue a final rule in the next few months. Analysts anticipate that the definitions in the final rule will be aligned with those that appeared in the final transactions and privacy rules. They also expect a clarification that the final security rule covers health information transmitted or maintained in any form or medium (including paper records and oral communications), as does the final privacy rule. Beyond that, analysts are not expecting any substantial changes in the final security rule. Prior to the Bush Administration, HHS indicated that it intended to carve out the electronic signature standard and issue it as a separate rule.

Security. The proposed security standards do not mandate specific technologies to be used. HHS opted for a technologically neutral approach so as not to bind the health care community to systems and/or software that may soon be superceded by new products in the rapidly developing field of information security technology. The standards include a compendium of organizational and technical practices and procedures that must be adopted. The proposal is also designed to give health care entities of different size and complexity the flexibility to develop their own particular implementation solutions as long as the basic requirements are met. The proposed security standards include four sets of provisions.

Administrative Procedures. Most of HIPAA security compliance will be administrative and operational in nature. The proposed rule requires a security assessment and risk analysis. Policy and procedure requirements include: assigning authorities to individuals assigned to authorize various level of physical access; defining physical and data access levels based on role; employee security orientation; tracking employee access to applications, systems, data, and physical areas; and termination procedures that ensure recovery of keys and access cards, and removal of access to applications, systems, and data.

Physical Safeguards. The proposed rule contains several requirements to protect computers and physical records. They include: facility management; physical

---

[16] 63 *Federal Register* 43241–43280.

access controls; computer room access; medical records access/tracking; shredding policies; and workstation location policies.

Technical Security Services. The technical security services provisions deal with systems and software applications that protect and control access to electronic information. They are designed to ensure that users only have access to those systems, applications, and data for which they are authorized. Technical solutions may be as simple as user passwords or include more complex devices such as biometrics. The proposed rule also requires an audit trail policy to track user access.

Technical Security Mechanisms. These provisions are intended to protect the transmission of patient data over public networks (e.g., Intranet, Internet). They require the appropriate deployment of security software, including Internet use monitoring, encryption, digital signatures, firewalls, and virus protection.

Electronic Signature. HHS proposed adopting digital signatures (with properties that ensure message integrity, non-repudiation, and user authentication) as the electronic signature standard. The standard applies only to HIPAA-specified transactions that employ an electronic signature. It does not mandate the use of electronic signatures. None of the transactions adopted under HIPAA currently require an electronic signature, though they may do so in the future. As previously mentioned, HHS is expected to remove electronic signatures from the final security rule. At the request of the Commerce Department's National Institute of Standards and Technology (NIST), HHS agreed to defer issuing a final electronic signature standard until an assessment of this evolving technology has been completed.

Standardization and Interoperability of Information Technologies. At a March 2000 hearing before the House Science Subcommittee on Technology, a panel of health care information technology experts urged federal agencies to develop a set of technology standards by which all health care information security systems could be evaluated.[17] Without such standards, health care plans and providers who seek to integrate information technology systems have no way of knowing whether the security components of the products they purchase will perform as expected. By one estimate, there are more than 1600 companies developing and selling health care information technology, with no underlying industry standard security requirements for their products. A wide variety of commercial products are available, including operating systems, database management systems, firewalls, smartcards, network devices, and PKI applications, each with different capabilities and limitations. Without technology standards, consumers may be left wondering how to choose the product that best suits their needs and which provides the appropriate level of security.

The experts also testified that the lack of interoperability among information technology systems presents a barrier to the widespread utilization of electronic

---

[17]U.S. Congress. House. Committee on Science. Subcommittee on Technology. *The Changing Face of Healthcare in the Electronic Age*, Mar. 10, 2000. Testimony and opening statements are available online at [http://www.house.gov/science/106_hearing.htm].

information in health care. For example, there is currently no way of ensuring that the system used by one physician will be compatible with that of another physician with whom she plans to share data electronically. The current situation in the health care industry is in stark contrast to the banking industry. Early in the development of the banking industry's information infrastructure, financial institutions saw the value of interoperability that would allow a customer from any bank to execute certain financial transactions from automated teller machines (ATMs) all over the world. Instead of developing proprietary technologies, these companies adhered to uniform standards and sought competitive advantage in other ways.

The National Information Assurance Partnership (NIAP), a joint initiative between NIST and the National Security Agency, is seeking to establish cost-effective testing, evaluation, and certification programs for information technology security products. The program will benefit producers by increasing the value and competitiveness of their products through the availability of formal, independent testing and certificates of validation. NIAP efforts will also help users by providing a sound and reliable basis for the evaluation, comparison, and selection of security products.[18]

Working together with industry, NIAP is using the Common Criteria for Information Technology Security Evaluation to develop generic testing specifications for particular information technology products. The Common Criteria are a set of internationally developed standards for evaluating the security properties of information technology products and systems. Last year, NIAP and NIST helped establish an industry-led health care security forum to discuss security requirements for health care information technology systems, and the potential for developing specific sets of security requirements using the Common Criteria.

Privacy Rule: Overview and Issues

On December 28, 2000, HHS published a final rule to protect the privacy of medical records and other personally identifiable health information.[19] The rule took effect on April 14, 2001(see **Table 2**).[20] Covered entities have 2 years (i.e., April 14, 2003) to come into compliance.[21] The privacy rule covers health care providers who electronically transmit health information in connection with one of the HIPAA-specified transactions, health plans, and health care clearinghouses. HIPAA did not provide HHS with the authority to regulate directly the actions of other entities that

---

[18]NIAP information is available online at [http://niap.nist.gov].

[19]65 *Federal Register* 82461–82829.

[20]Initially, the privacy rule was set to take effect on February 26, 2001. However, that date was delayed in accordance with the Congressional Review Act of 1996, which requires a major rule to be submitted to Congress for a 60-day review period before it becomes effective. Congress did not receive the rule from HHS until February 13, thereby pushing back the effective date to April 14.

[21]Small health plans with annual receipts of no more than $5 million have an additional year (i.e., April 14, 2004) to comply.

collect and maintain health information, such as life insurers, researchers, and employers (unless they are acting as providers or plans). However, the rule requires covered entities to enter into contracts with each of their business associates with whom they share personal health information for purposes other than consultation, referral, or treatment.[22] The contracts bind the business associates to comply with the covered entities' privacy practices and safeguard the confidentiality of protected health information.

Table 3 summarizes the key provisions of the health privacy rule, which applies to all personally identifiable health information handled by covered entities, regardless of the form or format in which it is maintained or transmitted.[23] The rule establishes new rights for patients regarding access to and use of their health information. It gives patients the right to view and copy their medical records, request that their medical records be amended, and obtain a history of authorized disclosures of their records. Covered entities must provide patients with written notice of their privacy procedures and the anticipated uses and disclosures of patient information. Patients will also be able to file a complaint with HHS if they believe their privacy rights have been violated.

The rule establishes two distinct forms of patient release for the use and disclosure of identifiable health information. First, providers must obtain a patient's one-time, general consent to use or disclose their information for treatment, payment, and other health care operations. Providers may make patient consent a condition of receiving treatment. Health plans and clearinghouses have the option to obtain patient consent to use and disclose health information for their own health care operations. The general consent document must inform patients of their privacy rights, including the right to request restrictions on the use and disclosure of their medical information for routine health care functions.

Second, all covered entities must obtain a patient's specific authorization in order to use or disclose information for non-routine uses and most non-health care purposes, such as releasing information to lending institutions or life insurers. The authorization form must specify the type of information to be disclosed, the person(s) authorized to disclose the information, and the person(s) who will receive the information.

The rule specifies certain national priority activities in which patient information may be used and disclosed without authorization, consistent with other applicable laws and regulations. These activities include health care system oversight, public health activities, research (see discussion below), and law enforcement. Covered entities may also use certain patient information, without first seeking authorization, to develop mailing lists for fundraising appeals, but they must give patients the opportunity to opt out of receiving future appeals. Also, while the rule prohibits

---

[22]A business associate is any person or organization that performs a function involving the use or disclosure of identifiable health information on behalf of a covered entity or provides legal, actuarial, accounting, or other services.

[23]Medical information in education records covered by the Family Educational Right and Privacy Act (FERPA) is excluded from the privacy rule.

covered entities from releasing patient information to marketing companies without prior authorization, a covered entity may itself use such information for marketing on behalf of third parties, provided patients are given the opportunity to opt out of receiving further marketing communications.

With the exception of uses and disclosures of patient information for the purpose of treatment, covered entities must limit the information disclosed to the minimum necessary to accomplish the purpose of disclosure. Within covered entities, employees' access to health information must be limited to the minimum needed to do their jobs. Employers that sponsor health plans may not obtain and use employees' health information for purposes unrelated to providing and paying for health care (e.g., hiring and promotion decisions) without explicit authorization.

Concerns and Issues Dividing Stakeholders

A coalition of hospitals, health maintenance organizations, insurers, and pharmaceutical companies mounted an aggressive lobbying effort at the beginning of the year to scale back the privacy rule. These groups are critical of the rule's general consent requirement, the minimum necessary standard, and business associate contracts. They claim that the rule, as currently written, will compromise patient care by placing unacceptable restrictions on access to health information and be extremely costly to implement. The critics had hoped to delay the rule's implementation and reopen the rulemaking process to amend the rule and make it administratively and financially less burdensome.

On February 28, the Bush Administration responded to the health care industry's concerns by opening the rule for an additional 30-day period of public comment.[24] After the comment period closed on March 30, HHS officials indicated that they would likely delay implementation of the rule in order to make changes to simplify it and lessen its financial burden. However, the Administration announced on April 12 that the rule would take effect on schedule.

Patient privacy advocates firmly support the health privacy rule, though they too have concerns with some of its provisions. They are chiefly concerned about the constraints that HIPAA placed on HHS. They favor legislation that would allow the agency to broaden federal privacy protections to cover all entities that handle medical information and provide patients with the right to sue in federal court for violations of their health information privacy. Consumer advocacy groups have fought health care industry efforts to lobby HHS for modifications to the rule, which they claim would weaken the rule's privacy protections.

Stakeholders presented their views on the privacy rule in testimony before the Senate Health, Education, Labor, and Pensions Committee and the House Energy and Commerce Subcommittee on Health in early 2001.[25] Key concerns and issues raised

---

[24]66 *Federal Register* 12738–12739.

[25]The Senate HELP Committee hearing was held on February 8, and the House Health Subcommittee hearing was held on March 22. Testimony is available on the committee Web

(continued...)

during those hearings, which are likely to remain central to the debate over the rule's implementation, are discussed below.

Patient Consent. The most controversial provision in the privacy rule is the requirement that health care providers obtain patient consent prior to using or disclosing health information for treatment, payment, and other health care operations. Consent is optional for providers who have an indirect relationship with patients (i.e., they have no direct contact with the patient, or they provide services at the request of another provider). Health plans and clearinghouses also have the option, but are not required, to obtain consent in order to use or disclose information for payment and health care operations. Patients have the right to request restrictions on how their information is used or disclosed, though covered entities are not required to agree to any such restrictions. Patients may revoke their consent at any time.

Privacy advocates and the American Medical Association (AMA) support the requirement that direct health care providers must obtain consent prior to routine uses and disclosures, but question why health plans and clearinghouses are not held to the same standard. According to the AMA, patient trust in the health care system can only be assured when all entities that maintain health information have an obligation to safeguard the confidentiality of that information, and when patients have control over decisions by those entities to use and disclose the information. Requiring consent before any use or disclosure of health information for health care operations also creates an incentive to de-identify information at the earliest possible opportunity.

The AMA is especially concerned that consent is optional for health plans in view of the rule's broad definition of health care operations. The definition includes conducting quality assessment and improvement activities; reviewing and evaluating provider performance, and health plan performance; underwriting, premium rating, and other activities relating to the creation, renewal or replacement of health insurance contract; conducting or arranging for medical review, legal services, and auditing functions; and business planning, development, and management. The AMA contends that the definition of health care operations is sufficiently broad to encompass virtually all uses of information.

Health insurers are extremely critical of the consent requirement. They point out that physicians will be unable to use patient information without a signed consent, and that the effort and cost of obtaining consent from over 200 million Americans will be daunting. They also fear that the consent requirement may unintentionally delay and impede routine operations that are essential to providing quality care and timely payment. For example, when a physician calls in a prescription, the pharmacist would need to have the patient's consent on file in order to fill the prescription and process the insurance claim. Family members and friends would also be unable to pick up prescriptions on behalf of the patient.

Privacy advocates dismiss these arguments as misplaced and inaccurate. They point out that the rule permits covered entities to use their professional judgement and

---

[25](...continued)
sites [http://www.senate.gov/~labor]; [http://www.house.gov/commerce].

experience in allowing family members and others to pick up items like prescriptions, medical supplies, or x-rays. They also believe that the problem of a pharmacist needing a patient's consent on file in advance of filling a prescription is easily remedied. HHS could, for example, issue a guidance that would allow a pharmacist in such a situation to be considered to have an indirect treatment relationship with the patient.

The American Hospital Association (AHA) has complained that it did not have adequate opportunity to comment on how the prior consent provision would impact patient care or hospital operations. HHS did not include prior consent in the proposed rule, though the agency did invite comments on whether other approaches to protecting health information would be more effective. The agency added the consent provision to the final rule in response to the comments it received. The AHA is also concerned about the impact of the consent requirement on routine hospital operations. For example, hospitals would be unable to obtain background medical information and schedule surgery without first getting a patient's consent.

Minimum Necessary. Stakeholders are also divided over the requirement that, with the exception of treatment-related disclosures, covered entities must make a reasonable effort to disclose no more than the minimum amount of information necessary to accomplish the intended purpose of the disclosure. The minimum necessary standard also applies to internal uses of information and requires entities to define what information will be made available to each employee by role.

Privacy advocates and the AMA are generally supportive of the minimum necessary standard. Physicians are responsible for determining the minimum amount necessary, except when responding to requests for information from health insurers, in which case it becomes the responsibility of the payer to request only the minimum amount necessary. The AMA is concerned that some health plans may request more information than a physician would judge to be the minimum necessary. However, the rule allows physicians to review all non-routine requests to determine whether they meet the minimum necessary standard. The AMA supports the exception to the minimum necessary standard for disclosures to or requests by a health care provider for treatment purposes, which is designed to give physicians the freedom to exchange and review information to provide patients the treatment they need.

The AMA is critical of the requirement that physician's offices establish and implement policies and procedures for complying with the minimum necessary standard, and review non-routine requests for disclosures. It questions the added benefit of such a requirement in view of physicians' ethical and professional obligations to keep patient information confidential.

Health insurers argue that the minimum necessary standard could jeopardize the quality of patient care. Most health care services today are delivered in an integrated system. Health plans are concerned that the minimum necessary standard will limit the flow of information that they say is essential to good patient care and prompt payment. HMOs, in particular, fear that physicians might use the minimum necessary standard to justify withholding patient information. Insurers are also critical of the fact that the exemption for treatment purposes covers only disclosures of information and not uses of information. As a result, the rule may limit a physician's access to

vital information during critical treatment situations. In fact, the rule allows the use of the entire medical record when it is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use.[26]

Business Associate Contracts. The rule requires covered entities to enter into contracts with their business associates to ensure that these groups, which are not directly covered by HIPAA, adhere to the same privacy protections.[27] HHS adopted this arrangement as a way of extending the rule's protections to information shared with others in the health care system. The agency proposed requiring covered entities to monitor the activities of their business associates. That language was amended in the final rule by limiting a covered entity's liability to those circumstances where the entity has knowledge of a breach of contract by the business associate and fails to take action. The rule exempts providers from having to enter into contracts when the disclosure of patient information is for treatment purposes. Examples of such exemptions include consultations between physicians at separate facilities, and physicians writing prescriptions to be filled by pharmacists.

Patients rights groups have applauded the use of business associate contracts, though they point out that many entities that handle health information remain unregulated (e.g., financial institutions, marketing firms, researchers, and employers who are not acting as providers or plans). They view the rule as an intermediate step and have urged Congress to pass a more comprehensive health privacy law applicable to all entities that handle personal health information.

Health plans, employers, and provider groups are opposed to the business associate contracts, which they argue will result in covered entities having to develop hundreds, if not thousands, of privacy contracts. They complain that drafting the contracts will be a lengthy and complex process. Privacy advocates respond that the rule's implementation specifications for business associate contracts are clear and straightforward and should not result in complicated contracts. In order to reduce the administrative burden, covered entities have the option of developing standard contracts or standard addenda to existing contracts.

The rule requires business associates to use and disclose health information in accordance with the policies and procedures established by the covered entity with whom they contract. Critics are concerned that business associates who contract with multiple covered entities may find themselves subject to differing standards. The situation is further complicated by the fact that some covered entities, such as health insurers, may also act as business associates to other covered entities. Health plans argue that keeping track of all these potential relationships and contractual obligations will be confusing and time-consuming.

---

[26]HHS states, in the preamble to the rule, that it expects that covered entities will implement policies that allow persons involved in treatment to have access to the entire record, as needed.

[27]The rule defines business associates based on their relationship with covered entities. A business associate is any individual or entity, other than a member of the workforce of a covered entity, which provides services to or on behalf of a covered entity and uses or discloses personal health information that belongs to a covered entity. Business associates include accountants, attorneys, auditors, and billing and data management firms.

Accrediting bodies, such as the Joint Commission for the Accreditation of Healthcare Organizations (JCAHO), claim that they act as health oversight agencies on behalf of government programs and should not be treated as business associates. JCAHO estimates that it would need to enter into contracts with each of the 18,000 facilities—including hospitals, nursing homes, and home health agencies—that it surveys for accreditation. Several groups contend that HHS exceeded its statutory authority by including the business associate contract provisions in the rule. They point out that HIPAA clearly delineates the entities that are covered under the rule (i.e., health plans, clearinghouses, and providers conducting standard electronic transactions).

Marketing by Covered Entities. Patient advocacy groups are concerned about a provision in the rule that allows physicians, hospitals, and other covered entities (or their business associates) to market products and services to patients without their prior authorization. For example, health care providers are permitted to use or disclose a patient's medical information to prescribe, recommend or sell their own products and services, or the products and services of others, as part of the treatment of that individual. Covered entities must identify themselves when making a marketing appeal, indicate whether they are being paid to do so, and give patients the opportunity to opt out of receiving any further such communications.

Commercial use of patient information without authorization is one of the issues that is fueling the public's health privacy concerns. Representatives of patient advocacy groups caution that public confidence in the privacy rule may suffer as a result of the marketing provision. They would like the rule amended to give patients the opportunity to opt out in advance of all marketing communications. Such a change in the rule, they argue, would help allay the public's concerns.

Research. The Association of American Medical Colleges (AAMC), which represents the nation's medical schools and teaching hospitals, has raised several concerns about the potentially negative impact of the rule on medical research. Epidemiologists and health services researchers rely on access to archived, de-identified patient records in order to study the incidence and expression of diseases in specified populations, the beneficial and adverse outcomes of new therapies, and the cost-effectiveness of the health care system. However, the AAMC fears that in order the meet the rule's definition of de-identified information, medical records have to be stripped of so many identifying elements as to render them useless for most research. The association favors a de-identification standard that reflects the realities of medical research and the motivations of researchers, rather than one which it claims is designed to address the exaggerated fear of threats from decryption experts with criminal intentions.

The AAMC is also critical of some of the rule's new criteria that must be met in order for researchers to obtain a waiver of patient authorization to access identifiable health information. Federally funded research involving human subjects, and clinical trials of new drugs and medical devices, are subject to a set of federal regulations called the Common Rule. Under the Common Rule, research proposals must be approved by an Institutional Review Board (IRB) to ensure that the rights and welfare of the research subjects are protected. IRBs also decide whether or not to waive informed consent based on the level of risk to the participants. The health privacy

rule requires all research involving human subjects, regardless of its source of funding, to undergo review by an IRB or a newly created Privacy Board (PB). The IRB or PB must determine that the research meets eight new criteria regarding privacy rights and risks, in addition to the provisions of the Common Rule, before it can approve a waiver. The AAMC is concerned that some of the criteria are contradictory and that IRBs have no experience or training to make those determinations.

For research performed under an informed consent waiver, the rule requires the IRB or PB to determine that the information requested by the investigator meets the minimum necessary requirement. The AAMC is unclear how IRB or PB members will be able to make this determination in judging proposals for research that requires access to very large medical databases. Moreover, the association is concerned that the expectation that the minimum necessary standard has been met will generate a risk of liability for covered entities. Add to that the rule's general complexity and the administrative burdens it places of covered entities, and the AAMC argues that covered entities may be reluctant to make health information accessible to researchers.

State Law Preemption. Preemption of state laws is one of the most controversial issues in the health privacy debate. As required by HIPAA, the rule does not preempt state laws that are more protective of individual privacy. Although most states do not have comprehensive health privacy laws, nearly all states have condition-specific privacy requirements that protect individuals with mental illness, communicable diseases (e.g., HIV/AIDS), cancer, and other sensitive or stigmatized diseases from having their health information disclosed without their authorization. Such laws aim to bolster public trust and confidence in the health care system and encourage patients to seek treatment and counseling without fear of disclosure of sensitive information. Under the rule, those condition-specific protections would remain in effect. However, less protective state laws would be preempted. The rule, therefore, serves as a baseline (i.e., a federal "floor") of minimum privacy protection.

The rule allows any person to submit to the Secretary in writing a request to exempt a provision of state law from preemption. It is unclear from the rule to what extent, and how, the Secretary will allow public comment on such preemption decisions.

Large health plans and employers that operate in more than one state have strongly criticized the rule for not preempting all state laws to create a single, national privacy standard for health information. They argue that the rule's partial preemption of state law will be extremely burdensome and costly to implement and only add to the difficulties of navigating through the existing maze of state privacy laws. Critics of the rule's preemption provisions contend that covered entities will have to maintain some form of state-to-federal regulation matrix to ensure that they are complying with the correct laws and/or regulations. Because HIPAA specifically provided for establishing a federal floor of privacy protections, several stakeholders are calling for new legislation to establish full federal preemption.

Patient and privacy advocates, state governments, and providers strongly support partial federal preemption, as provided in the rule. They believe that a federal floor guarantees a minimum level of protection for everyone, while still allowing states to enact more stringent protections and address future privacy concerns. A recent

survey of state health privacy statutes suggests that the rule would significantly improve the privacy protections afforded to patients' medical information by requiring states with fairly minimal privacy protections to come up to the federal baseline.[28]

Privacy advocates are critical of a provision that excludes state parental notification laws from the rule's general preemption requirements. Under the rule, laws that authorize (or prohibit) disclosure of health information about a minor to a parent or guardian would not be preempted. Advocates for patients' privacy argue that minors should enjoy the same protections as adults. However, some conservative groups are opposed to minors being able to conceal reproductive health information from their parents (e.g., use of birth control, abortion).

Finally, HIPAA excludes state public health laws from federal preemption. States have traditionally exercised oversight and authority over public health. Under the rule, therefore, disclosures made for public health purposes, as mandated by state laws, do not require patient authorization. Such laws include reporting diseases and injuries, collecting vital statistics, public health surveillance, and public health investigation and intervention.

Compliance Costs. Groups that represent health plans and health care providers have criticized HHS' impact analysis and expressed concern about the potential cost of complying with the privacy rule. HHS estimates that the rule will cost $17.6 billion over 10 years. Two provisions—restricting disclosures to the minimum amount of necessary information and establishing a privacy official—account from more than half of HHS' cost estimate. According to the agency, the cost of the privacy rule is more than offset by implementation of the transaction and code sets rule, which is estimated to save the health care industry $29.9 over 10 years. Together, the two rules will produce a net savings of about $12.3 billion in improved health care efficiency and privacy protection.

Industry groups believe that the actual compliance costs will substantially exceed HHS' estimates. An independent assessment commissioned by the Blue Cross Blue Shield Association (BCBSA) estimated that the proposed health privacy rule would cost the health care industry more than $40 billion over 5 years. According to the BCBSA, most of these costs remain applicable to the final rule. The BCBSA also believes that HHS overestimated the savings from implementing the transactions standards.

A study commissioned by the AHA, looking at hospital costs alone, found that the cost of only three key provisions of the proposed rule—minimum necessary, business associates, and state law preemption—could be as much as $22.5 billion over 5 years. Other provider groups are concerned that spending additional time with patients to explain the rule's requirements and obtain consent will compete with time for direct patient care.

---

[28] *The State of Health Privacy: An Uneven Terrain* was prepared in 1999 by the Health Privacy Project and is available online at [http://www.healthprivacy.org].

Several groups have expressed concern about being able to implement the rule within the two-year time frame. Despite their concerns, however, organizations that represent plans and providers are developing model forms for patient consent, notices explaining privacy practices, business associate contracts, and compliance plans.

HHS Implementation Guidelines

HHS sources have indicated that the agency is about to release a detailed guidance document to help covered entities implement the privacy rule. The document is expected to address industry concerns by providing explanations of intent and clarifying some of the rule's key provisions. It is unclear to what extent, if any, the implementation guidelines will alter the rule. Under HIPAA, the Secretary has the authority to modify the rule after it takes effect in order to permit compliance. However, any significant modifications to the rule's provisions would require reopening the rulemaking process.

Legislative Activity in the 107th Congress

Lawmakers have introduced two bills (S. 836, H.R. 1975) that would delay the scheduled compliance dates of HIPAA's Administrative Simplification standards (i.e., transactions and codes, security, and unique identifiers). Both bills would set October 16, 2004 as the uniform compliance date, or 24 months after all the final rules are published, whichever is later. Neither bill directly covers the privacy rule, and H.R. 1975 includes language that specifically excludes the privacy rule from its provisions.

The legislation is in response to efforts by Blue Cross Blue Shield (BCBS) and other health care industry groups to delay implementation of HIPAA until all the standards and enforcement regulations, with the exception of the privacy rule, are published in final form. BCBS claims that without this extension there will be substantial disruptions in payments to providers. In congressional testimony, industry groups stressed the importance of synchronizing the compliance dates for the HIPAA standards to ensure that covered entities have a complete picture of what is required before they purchase new information technology systems and retrain their employees. They argue that having to comply with each new rule in turn will only add to HIPAA's overall administrative and financial burden.

Additional Information and Web Sites

For more information on the health privacy rule, see CRS Report RS20500, *Medical Records Privacy: Questions and Answers on the HIPAA Final Rule*. Detailed information on all the HIPAA standards, including the text of all *Federal Register* notices, summaries of all proposed and final regulations, public comments, and the HHS implementation plant can be found on the department's Administrative Simplification home page [http://aspe.hhs.gov/admnsimp]. HHS's Office of Civil Rights, which is responsible for implementing and enforcing the privacy rule and is responding to questions about the rule, has established a privacy home page

[http://www.hhs.gov/ocr/hipaa]. Additional information on the HIPAA Administrative Simplification standards may be found at the following Web sites.

General HIPAA Information

Phoenix Health Systems	[http://www.hipaadvisory.com]
HIPAA Comply	[http://www.hipaacomply.com]
National Committee on Vital and Health Statistics	[http://ncvhs.hhs.gov]

Electronic Transactions and Code Sets

Accredited Standards Committee X12	[http://www.x12.org]
Washington Pub. Co. (X12N implementation guides)	[http://www.wpc-edi.com]
National Uniform Billing Committee	[http://www.nubc.org]
National Uniform Claims Committee	[http://www.nucc.org]
National Council for Prescription Drug Programs	[http://www.ncpdp.org]
Workgroup for Electronic Data Interchange	[http://www.wedi.org]
Medicaid HIPAA Information	[http://www.hcfa.gov/medicaid/hipaa/adminsim]
HCPCS	[http://www.hcfa.gov/medicare/hcpcs.htm]

Privacy

Patient Privacy Advocates.

Health Privacy Project, Washington DC	[http://www.healthprivacy.org]
National Coalition for Patient Rights	[http://www.nationalcpr.org]
American Civil Liberties Union	[http://www.aclu.org]

Health Care Plans, Providers, and Clearinghouses.

Association for Electronic Health Care Transactions	[http://www.afehct.org]
American Health Information Management Association	[http://www.ahima.org]
American Hospital Association	[http://www.aha.org]
American Medical Association	[http://www.ama-assn.org]
American Association of Health Plans	[http://www.aahp.org]
Health Insurance Association of America	[http://www.hiaa.org]
Blue Cross Blue Shield Association	[http://www.bluecares.com]
Association of American Medical Colleges	[http://www.aamc.org]

GAO Reports

GAO has provided the Senate Committee on Health Education, Labor, and Pensions with analysis of the health privacy rule. The following reports are available on GAO's Web site [http://www.gao.gov].

Privacy Standards: Issues in HHS' Proposed Rule on Confidentiality of Personal Health Information, GAO/T-HEHS-00-106, April 6, 2000.

Health Privacy: Regulation Enhances Protection of Patient Records but Raises Practical Concerns, GAO/T-01-387, Feb. 8, 2001.

Medical Privacy Regulation: Questions Remain About Implementing the New Consent Requirement, GAO-01-584, April 6, 2001.

Table 1. Summary of HIPAA's Administrative Simplification Provisions

Purpose (Section 261)	To improve the efficiency and effectiveness of the health care system by establishing standards and requirements for the electronic transmission of certain types of health information. Amends Title XI of the Social Security Act by adding Part C—Administrative Simplification.
Administrative Simplification (Section 262)	
- Definitions	Defines health care clearinghouse, health care provider, health plan, personally identifiable health information, and standard setting organization.
- General Requirements for Adoption of Standards	Specifies that the standards apply to health plans, health care clearinghouses, and health care providers that transmit health information electronically. Requires the Secretary either to adopt standards that have already been developed by standard setting organizations or to develop different standards, provided they substantially reduce administrative costs to health plans and providers. If no standard has been adopted by a standard setting organization, the Secretary must develop a new standard based on the recommendations of the NCVHS and consultations with standard setting organizations and other appropriate agencies. For all the standards, the Secretary is required to consult with the National Uniform Billing Committee, the National Uniform Claim Committee, the Workgroup for Electronic Data Interchange, and the American Dental Association.
- Standards for Electronic Health Care Transactions	Instructs the Secretary to issue the following standards: (1) Uniform formats for use in the electronic exchange of health information, including health claims and attachments, health plan eligibility and enrollment, and health care payment, and health claim status. (2) Code sets for data elements in standard electronic transactions. (3) Unique identifiers for individuals, employers, health plans, and health care providers. (4) Security standards to provide administrative, technical, and physical safeguards for protecting medical record confidentiality. (5) An electronic signature standard to verify the authenticity of the signer and the transaction.
- Timetable for Adoption of Standards	Requires the Secretary to adopt all the standards within 18 months of HIPAA's enactment (i.e., by February 21, 1998), except for the standards for claims attachments, which are due within 30 months of enactment (i.e., by February 21, 1999). Permits the Secretary to modify the standards as frequently as once every 12 months.
- Requirements for Compliance	Requires health plans and providers that process electronic transactions to use standard formats and data elements. Plans and providers may transmit and receive such data either directly or by contracting with a clearinghouse to convert nonstandard data elements into standard transactions. Gives entities covered by the standards up to 24 months to comply. Small health plans have 36 months to comply.[a]

- Civil Penalties for Failure to Comply	Establishes a civil monetary penalty of $100 per person per violation of a specific standard, up to a maximum of $25,000 per person for all such violations in any calender year. Allows the penalty to be waived if the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that the standard had been violated. Also waives the penalty if failure to comply was due to reasonable cause and not willful neglect.
- Criminal Penalties for Wrongful Disclosures	Establishes criminal penalties for wrongfully using a unique health identifier, or wrongfully obtaining or disclosing personally identifiable health information. Penalties range from a $50,000 fine and/or 1 year in prison, up to a $250,000 fine and 10 years in prison if the offense is committed with intent to sell, transfer, or use the information for commercial advantage, personal gain, or do malicious harm.
- Impact on State Law	Standards preempt contrary provisions in state law pertaining to health information, including provisions that require medical records to be maintained in written rather than electronic form. However, the standards may not preempt or limit state laws that are necessary to prevent fraud and abuse, regulate health insurance companies, or report on health care delivery and costs. The standards may not limit the authority of states to collect and report public health statistics (e.g., births, deaths, diseases, injuries).
- Financial Institutions	Standards do not apply to the processing of payment transactions by financial institutions (e.g., exchanging information during a credit care payment for health care).
National Committee on Vital and Health Statistics (Section 263)	Amends Section 306(k) of the Public Health Service Act to increase NCVHS membership from 16 to 18 members and requires NCVHS to advise the Secretary on issues related to the collection, processing, and tabulation of health statistics. Requires NCVHS to study the adoption of uniform health data standards and the electronic exchange of such information, and report its recommendations to Congress within 4 years of HIPAA's enactment (i.e., by August 21, 2000). Instructs NCVHS to report annually to Congress on the implementation of HIPAA's Administrative Simplification provisions.[b]
Health Information Privacy (Section 264)	Requires the Secretary to submit to Congress within 1 year of HIPAA's enactment (i.e., by August 21, 1997) recommendations for standards to protect the privacy of personally identifiable health information.[c] Mandates the Congress to pass health privacy legislation within 3 years of HIPAA's enactment (i.e., by August 21, 1999), otherwise the Secretary is instructed, in consultation with NCVHS, to issue privacy standards within the following 6 months (i.e., by February 21, 2000). Such standards may not preempt state laws that are more protective of health information privacy.

Source: Text of HIPAA, as enacted into law (P.L. 104-191).

[a] HCFA defines small health plans as those with annual receipts of $5 million or less.

[b] NCVHS reports are available on its Web site at [http://www.ncvhs.hhs.gov].

[c] The Secretary's recommendations, which were presented before the Senate Committee on Labor and Human Resources on September 11, 1997, are available online at [http://aspe.os.dhhs.gov/admnsimp/pvcrec.htm].

Table 2. Implementation Status of HIPAA's Standards

Standards[a]	NPRM[b]	Final Rule	Effective Date[c]
Electronic Transactions and Code Sets	May 7, 1998	August 17, 2000	October 16, 2000
Provider Identifier	May 7, 1998	Expected 2001	
Health Plan Identifier	Expected 2001		
Employer Identifier	June 16, 1998	Expected 2001	
Individual Identifier	On hold		
Security and Electronic Signatures	August 12, 1998	Expected 2001	
Privacy	November 3, 1999	December 28, 2000	April 14, 2001

Source: Health Care Financing Administration.

[a] HHS plans to issue an enforcement rule that applies to all the HIPAA Administrative Simplification standards. The rule will address the imposition of civil monetary penalties and the referral of criminal cases where there has been a violation of the standards.

[b] Notice of Proposed Rulemaking.

[c] Covered entities have 2 years to come into compliance. Small health plans with revenues of $5 million or less have an additional year to comply.

Table 3. Key Provisions of the Health Privacy Rule (45 CFR 160, 164)

Covered Entities	Applies to health care providers who electronically transmit health information in connection with any of the HIPAA-covered transactions, health plans, and health care clearinghouses. [160.102, 164.500]
Covered Health Information	Applies to personally identifiable health information created or received by a covered entity and transmitted or maintained in any form or medium (e.g., paper, electronic, oral). [164.501]
Patient Access	Gives patients the right to access, inspect and copy their health information within 30 days of making a request for access, if the information is maintained or accessible on-site (otherwise within 60 days). Allows covered entities to impose reasonable cost-based fees for copying the information. Covered entities may deny access under certain circumstances. [164.524]
Amendment of Health Information	Gives patients the right to request amendment of their health information and requires covered entities to act on such a request within 60 days. Allows covered entities to deny a request if they determine that the patient's information is accurate and complete, or was not created by the covered entity. Permits requester to submit a written statement of disagreement with the denial. [164.526]
Accounting of Disclosures	Gives patients the right to receive, within 60 days, an accounting of disclosures over the past 6 years, except for disclosures for treatment, payment, and health care operations, and for certain other specified purposes. Accounting must include a brief statement of the purpose of each disclosure and the address of the recipient of the information. [164.528]
Patient Notice	Requires covered entities to provide patients with written notice of their privacy rights, as well as notice of the entities' legal duties and privacy practices. Specifies the content of the notice. [164.520]
Minimum Necessary	Requires covered entities to make a reasonable effort to use or disclose the minimum amount of information necessary to accomplish the intended purpose, except for disclosures related to treatment. [164.502(b), 164.514(d)]
De-identified Information	Defines de-identified health information as information from which 18 specified types of identifiers have been removed, or information for which an expert determines that the risk of identification is very small. De-identified information is not subject to the rule. Disclosure of a code or other means of enabling de-identified information to be re-identified constitutes disclosure of protected health information. [164.502(d), 164.514(a)-(c)]
Payment, Treatment, and Health Care Operations	Health care providers must obtain a patient's one-time consent in writing before using or disclosing health information for treatment, payment, or other routine health care operations. Providers may condition treatment on obtaining such consent. (Health plans and clearinghouses may also obtain consent for their own use and disclosure of health information for treatment, payment, or other routine health care operations, and may condition enrollment on obtaining such consent.) Patients have the right to request restrictions on these types of use and disclosure, but covered entities are not required to agree to such a request. Patients may in writing revoke their consent at any time. [164.506, 164.522(a)]
Directory Assistance and Next of Kin	Requires covered entities to give patients notice and the opportunity to opt out before information is disclosed to a facility directory or provided to next of kin or other persons involved in the patients' care. [164.510]
Non-Routine and Non-Health Care Disclosures	Covered entities must obtain a patient's specific authorization in writing before using or disclosing health information for non-routine uses and most non-health care purposes (see Disclosures Not Requiring Authorization below). Covered entities may not condition services or payment on receipt of such authorization. Patients may revoke their authorization at any time. [164.508]

Business Associates	Allows a covered entity to disclose health information to a business associate without further authorization if it obtains satisfactory assurances, though a written contract, that the business associate will safeguard the information. The contract must establish the permitted and required uses and disclosures of such information by the business associate. A business associate may use health information for its own management and administration, and may disclose it to others if it obtains assurances that the information will be held in confidence and the recipient will notify the business associate of breaches of confidentiality. [164.502(e), 164.504(e)]
Employers	Employers that sponsor health plans may not obtain and use employees' health information for employment or other non-health purposes without their specific authorization. [164.504(f)]
Hybrid Entities	Requires hybrid entities (i.e., companies with multiple lines of business) to restrict disclosure of health information between their health care and non-health care components. Such disclosures are governed by the same restrictions as disclosures between two separate and distinct legal entities. [164.504(b)(c)]
Disclosures Not Requiring Authorization	Covered entities may use and disclose health information without a patient's authorization for the following national priority activities, consistent with other applicable laws and regulations: (a) uses and disclosures required by law; (b) public health activities; (c) abuse, neglect, and domestic violence; (d) health oversight; (e) judicial and administrative proceedings; (f) law enforcement; (g) coroners, medical examiners, and funeral directors; (h) organ donation and transplantation; (i) research; (j) imminent and serious threats to health and safety; (k) specialized government functions; (l) workers' compensation programs. [164.512]
Marketing and Fundraising	Covered entities may use or disclose information without a patient's authorization to market their own products and services, or the products and services of others, as part of the treatment of that individual. Covered entities must identity themselves when making a marketing appeal and give patients the opportunity to opt out of any further communications. Covered entities also may disclose certain patient information to a foundation or business associate that contacts patients for fundraising purposes, provided that patients are given the opportunity to opt out of any further communications. [164.514(e)(f)]
Psychotherapy Notes	Provides higher level of protection than for other types of health information. Requires authorization for most uses or disclosures. Health plans may not condition enrollment or eligibility for benefits on obtaining such authorization. [164.508(a)(2)]
Preemption of State Laws	Preempts all contrary state laws unless they are more stringent (i.e., more protective of privacy). Does not preempt state parental notification laws or state laws used to administer health care, regulate controlled substances, or protect public health, safety and welfare. Allows states to apply to HHS for a determination on whether a state law meets the requirements of these exclusions. [160.201 *et seq.*]
Safeguards	Requires covered entities to establish and implement various administrative procedures, commensurate with the size and scope of their business, to protect the confidentiality of health information. These include designating a privacy officer, training employees, and developing a system of sanctions for employees who violate an entity's privacy policies. [164.530]
Compliance	Permits an individual, who believes a covered entity is not compliant, to file a written complaint with the Secretary. Authorizes Secretary to conduct a compliance review of such an entity. [160.300 *et seq.*]
Enforcement	HIPAA imposes civil monetary penalties against covered entities that fail to comply with the rule and imposes criminal penalties for certain wrongful disclosures of health information. Civil fines are $100 per person for unintentional disclosures, capped at $25,000 per year. Criminal penalties for selling, transferring, or using health information for commercial advantage, personal gain, or malicious harm include fines of up to $250,000 and/or up to 10 years in prison. [42 USC 1320d-5,6]