Federal Register

Thursday,
December 28, 2000

Part II

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160 and 164

Standards for Privacy of Individually Identifiable Health Information; Final Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

Rin: 0991–AB08

Standards for Privacy of Individually Identifiable Health Information

AGENCY: Office of the Assistant Secretary for Planning and Evaluation, DHHS.

ACTION: Final rule.

SUMMARY: This rule includes standards to protect the privacy of individually identifiable health information. The rules below, which apply to health plans, health care clearinghouses, and certain health care providers, present standards with respect to the rights of individuals who are the subjects of this information, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information.

The use of these standards will improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information. These protections will begin to address growing public concerns that advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors. This rule implements the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996.

DATES: The final rule is effective on February 26, 2001.

FOR FURTHER INFORMATION CONTACT: Kimberly Coleman, 1–866–OCR–PRIV (1–866–627–7748) or TTY 1–866–788–4989.

SUPPLEMENTARY INFORMATION: Availability of copies, and electronic access.

Copies: To order copies of the **Federal Register** containing this document, send your request to: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250–7954. Specify the date of the issue requested and enclose a check or money order payable to the Superintendent of Documents, or enclose your Visa or Master Card number and expiration date. Credit card orders can also be placed by calling the order desk at (202) 512–1800 or by fax to (202) 512–2250. The cost for each copy is $8.00. As an alternative, you can view and photocopy the **Federal Register** document at most libraries designated as Federal Depository Libraries and at many other public and academic libraries throughout the country that receive the **Federal Register**.

Electronic Access: This document is available electronically at http://aspe.hhs.gov/admnsimp/ as well as at the web site of the Government Printing Office at http://www.access.gpo.gov/su_docs/aces/aces140.html.

I. Background

Table of Contents

Purpose of the Administrative Simplification Regulations

This regulation has three major purposes: (1) To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information; (2) to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care; and (3) to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

This regulation is the second final regulation to be issued in the package of rules mandated under title II subtitle F section 261–264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, titled ''Administrative Simplification.'' Congress called for steps to improve ''the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.'' To achieve that end, Congress required the Department to promulgate a set of interlocking regulations establishing standards and protections for health information systems. The first regulation in this set, Standards for Electronic Transactions 65 FR 50312, was published on August 17, 2000 (the ''Transactions Rule''). This regulation establishing Standards for Privacy of Individually Identifiable Health Information is the second final rule in the package. A rule establishing a unique identifier for employers to use in electronic health care transactions, a rule establishing a unique identifier for providers for such transactions, and a rule establishing standards for the security of electronic information systems have been proposed. See 63 FR 25272 and 25320 (May 7, 1998); 63 FR 32784 (June 16, 1998); 63 FR 43242 (August 12, 1998). Still to be proposed are rules establishing a unique identifier for health plans for electronic transactions, standards for claims attachments, and standards for transferring among health plans appropriate standard data elements needed for coordination of benefits. (See section C, below, for a more detailed explanation of the statutory mandate for these regulations.)

In enacting HIPAA, Congress recognized the fact that administrative simplification cannot succeed if we do not also protect the privacy and confidentiality of personal health information. The provision of high-quality health care requires the exchange of personal, often-sensitive information between an individual and a skilled practitioner. Vital to that interaction is the patient's ability to trust that the information shared will be protected and kept confidential. Yet many patients are concerned that their information is not protected. Among the factors adding to this concern are the growth of the number of organizations involved in the provision of care and the processing of claims, the growing use of electronic information technology, increased efforts to market health care and other products to consumers, and the increasing ability to collect highly sensitive information about a person's current and future health status as a result of advances in scientific research.

Rules requiring the protection of health privacy in the United States have been enacted primarily by the states. While virtually every state has enacted one or more laws to safeguard privacy, these laws vary significantly from state to state and typically apply to only part of the health care system. Many states have adopted laws that protect the health information relating to certain health conditions such as mental illness, communicable diseases, cancer, HIV/AIDS, and other stigmatized conditions. An examination of state health privacy laws and regulations,

however, found that ''state laws, with a few notable exceptions, do not extend comprehensive protections to people's medical records.'' Many state rules fail to provide such basic protections as ensuring a patient's legal right to see a copy of his or her medical record. See Health Privacy Project, ''The State of Health Privacy: An Uneven Terrain,'' Institute for Health Care Research and Policy, Georgetown University (July 1999) (http://www.healthprivacy.org) (the ''Georgetown Study'').

Until now, virtually no federal rules existed to protect the privacy of health information and guarantee patient access to such information. This final rule establishes, for the first time, a set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care. The rule sets a floor of ground rules for health care providers, health plans, and health care clearinghouses to follow, in order to protect patients and encourage them to seek needed care. The rule seeks to balance the needs of the individual with the needs of the society. It creates a framework of protection that can be strengthened by both the federal government and by states as health information systems continue to evolve.

Need for a National Health Privacy Framework

The Importance of Privacy

Privacy is a fundamental right. As such, it must be viewed differently than any ordinary economic good. The costs and benefits of a regulation must, of course, be considered as a means of identifying and weighing options. At the same time, it is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom.

A right to privacy in personal information has historically found expression in American law. All fifty states today recognize in tort law a common law or statutory right to privacy. Many states specifically provide a remedy for public revelation of private facts. Some states, such as California and Tennessee, have a right to privacy as a matter of state constitutional law. The multiple historical sources for legal rights to privacy are traced in many places, including Chapter 13 of Alan Westin's Privacy and Freedom and in Ellen Alderman & Caroline Kennedy, The Right to Privacy (1995).

Throughout our nation's history, we have placed the rights of the individual at the forefront of our democracy. In the Declaration of Independence, we asserted the ''unalienable right'' to ''life, liberty and the pursuit of happiness.'' Many of the most basic protections in the Constitution of the United States are imbued with an attempt to protect individual privacy while balancing it against the larger social purposes of the nation.

To take but one example, the Fourth Amendment to the United States Constitution guarantees that ''the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated.'' By referring to the need for security of ''persons'' as well as ''papers and effects'' the Fourth Amendment suggests enduring values in American law that relate to privacy. The need for security of ''persons'' is consistent with obtaining patient consent before performing invasive medical procedures. The need for security in ''papers and effects'' underscores the importance of protecting information about the person, contained in sources such as personal diaries, medical records, or elsewhere. As is generally true for the right of privacy in information, the right is not absolute. The test instead is what constitutes an ''unreasonable'' search of the papers and effects.

The United States Supreme Court has upheld the constitutional protection of personal health information. In *Whalen* v. *Roe,* 429 U.S. 589 (1977), the Court analyzed a New York statute that created a database of persons who obtained drugs for which there was both a lawful and unlawful market. The Court, in upholding the statute, recognized at least two different kinds of interests within the constitutionally protected ''zone of privacy.'' ''One is the individual interest in avoiding disclosure of personal matters,'' such as this regulation principally addresses. This interest in avoiding disclosure, discussed in Whalen in the context of medical information, was found to be distinct from a different line of cases concerning ''the interest in independence in making certain kinds of important decisions.''

Individuals' right to privacy in information about themselves is not absolute. It does not, for instance, prevent reporting of public health information on communicable diseases or stop law enforcement from getting information when due process has been observed. But many people believe that individuals should have some right to control personal and sensitive information about themselves. Among different sorts of personal information, health information is among the most sensitive. Many people believe that details about their physical self should not generally be put on display for neighbors, employers, and government officials to see. Informed consent laws place limits on the ability of other persons to intrude physically on a person's body. Similar concerns apply to intrusions on information about the person.

Moving beyond these facts of physical treatment, there is also significant intrusion when records reveal details about a person's mental state, such as during treatment for mental health. If, in Justice Brandeis' words, the ''right to be let alone'' means anything, then it likely applies to having outsiders have access to one's intimate thoughts, words, and emotions. In the recent case of *Jaffee* v. *Redmond,* 116 S.Ct. 1923 (1996), the Supreme Court held that statements made to a therapist during a counseling session were protected against civil discovery under the Federal Rules of Evidence. The Court noted that all fifty states have adopted some form of the psychotherapist-patient privilege. In upholding the federal privilege, the Supreme Court stated that it ''serves the public interest by facilitating the appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance.''

Many writers have urged a philosophical or common-sense right to privacy in one's personal information. Examples include Alan Westin, Privacy and Freedom (1967) and Janna Malamud Smith, Private Matters: In Defense of the Personal Life (1997). These writings emphasize the link between privacy and freedom and privacy and the ''personal life,'' or the ability to develop one's own personality and self-expression. Smith, for instance, states:

> The bottom line is clear. If we continually, gratuitously, reveal other people's privacies, we harm them and ourselves, we undermine the richness of the personal life, and we fuel a social atmosphere of mutual exploitation. Let me put it another way: Little in life is as precious as the freedom to say and do things with people you love that you would not say or do if someone else were present. And few experiences are as fundamental to liberty and autonomy as maintaining control over when, how, to whom, and where you disclose personal material. Id. at 240–241.

In 1890, Louis D. Brandeis and Samuel D. Warren defined the right to privacy as ''the right to be let alone.'' See L. Brandeis, S. Warren, ''The Right

To Privacy,'' 4 Harv.L.Rev. 193. More than a century later, privacy continues to play an important role in Americans' lives. In their book, The Right to Privacy, (Alfred A. Knopf, New York, 1995) Ellen Alderman and Caroline Kennedy describe the importance of privacy in this way:

> Privacy covers many things. It protects the solitude necessary for creative thought. It allows us the independence that is part of raising a family. It protects our right to be secure in our own homes and possessions, assured that the government cannot come barging in. Privacy also encompasses our right to self-determination and to define who we are. Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized.

Or, as Cavoukian and Tapscott observed the right of privacy is: ''the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated.'' See A. Cavoukian, D. Tapscott, ''Who Knows: Safeguarding Your Privacy in a Networked World,'' Random House (1995).

Increasing Public Concern About Loss of Privacy

Today, it is virtually impossible for any person to be truly ''let alone.'' The average American is inundated with requests for information from potential employers, retail shops, telephone marketing firms, electronic marketers, banks, insurance companies, hospitals, physicians, health plans, and others. In a 1998 national survey, 88 percent of consumers said they were ''concerned'' by the amount of information being requested, including 55 percent who said they were ''very concerned.'' See Privacy and American Business, 1998 Privacy Concerns & Consumer Choice Survey (http://www.pandab.org). These worries are not just theoretical. Consumers who use the Internet to make purchases or request ''free'' information often are asked for personal and financial information. Companies making such requests routinely promise to protect the confidentiality of that information. Yet several firms have tried to sell this information to other companies even after promising not to do so.

Americans' concern about the privacy of their health information is part of a broader anxiety about their lack of privacy in an array of areas. A series of national public opinion polls conducted by Louis Harris & Associates documents a rising level of public concern about privacy, growing from 64 percent in 1978 to 82 percent in 1995. Over 80 percent of persons surveyed in 1999 agreed with the statement that they had ''lost all control over their personal information.'' See Harris Equifax, Health Information Privacy Study (1993) (http://www.epic.org/privacy/medical/polls.html). A Wall Street Journal/ABC poll on September 16, 1999 asked Americans what concerned them most in the coming century. ''Loss of personal privacy'' was the first or second concern of 29 percent of respondents. All other issues, such a terrorism, world war, and global warming had scores of 23 percent or less.

This growing concern stems from several trends, including the growing use of interconnected electronic media for business and personal activities, our increasing ability to know an individual's genetic make-up, and, in health care, the increasing complexity of the system. Each of these trends brings the potential for tremendous benefits to individuals and society generally. At the same time, each also brings new potential for invasions of our privacy.

Increasing Use of Interconnected Electronic Information Systems

Until recently, health information was recorded and maintained on paper and stored in the offices of community-based physicians, nurses, hospitals, and other health care professionals and institutions. In some ways, this imperfect system of record keeping created a false sense of privacy among patients, providers, and others. Patients' health information has never remained completely confidential. Until recently, however, a breach of confidentiality involved a physical exchange of paper records or a verbal exchange of information. Today, however, more and more health care providers, plans, and others are utilizing electronic means of storing and transmitting health information. In 1996, the health care industry invested an estimated $10 billion to $15 billion on information technology. See National Research Council, Computer Science and Telecommunications Board, ''For the Record: Protecting Electronic Health Information,'' (1997). The electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time. While the majority of medical records still are in paper form, information from those records is often copied and transmitted through electronic means.

This ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology affords many benefits to individuals and to the health care industry. Use of electronic information has helped to speed the delivery of effective care and the processing of billions of dollars worth of health care claims. Greater use of electronic data has also increased our ability to identify and treat those who are at risk for disease, conduct vital research, detect fraud and abuse, and measure and improve the quality of care delivered in the U.S. The National Research Council recently reported that ''the Internet has great potential to improve Americans'' health by enhancing communications and improving access to information for care providers, patients, health plan administrators, public health officials, biomedical researchers, and other health professionals.'' See ''Networking Health: Prescriptions for the Internet,'' National Academy of Sciences (2000).

At the same time, these advances have reduced or eliminated many of the financial and logistical obstacles that previously served to protect the confidentiality of health information and the privacy interests of individuals. And they have made our information available to many more people. The shift from paper to electronic records, with the accompanying greater flows of sensitive health information, thus strengthens the arguments for giving legal protection to the right to privacy in health information. In an earlier period where it was far more expensive to access and use medical records, the risk of harm to individuals was relatively low. In the potential near future, when technology makes it almost free to send lifetime medical records over the Internet, the risks may grow rapidly. It may become cost-effective, for instance, for companies to offer services that allow purchasers to obtain details of a person's physical and mental treatments. In addition to legitimate possible uses for such services, malicious or inquisitive persons may download medical records for purposes ranging from identity theft to embarrassment to prurient interest in the life of a celebrity or neighbor. The comments to the proposed privacy rule indicate that many persons believe that they have a right to live in society without having these details of their lives laid open to unknown and possibly hostile eyes. These technological changes, in short, may provide a reason for institutionalizing

privacy protections in situations where the risk of harm did not previously justify writing such protections into law.

The growing level of trepidation about privacy in general, noted above, has tracked the rise in electronic information technology. Americans have embraced the use of the Internet and other forms of electronic information as a way to provide greater access to information, save time, and save money. For example, 60 percent of Americans surveyed in 1999 reported that they have a computer in their home; 82 percent reported that they have used a computer; 64 percent say they have used the Internet; and 58 percent have sent an e-mail. Among those who are under the age of 60, these percentages are even higher. See ''National Survey of Adults on Technology,'' Henry J. Kaiser Family Foundation (February, 2000). But 59 percent of Americans reported that they worry that an unauthorized person will gain access to their information. A recent survey suggests that 75 percent of consumers seeking health information on the Internet are concerned or very concerned about the health sites they visit sharing their personal health information with a third party without their permission. Ethics Survey of Consumer Attitudes about Health Web Sites, California Health Care Foundation, at 3 (January, 2000).

Unless public fears are allayed, we will be unable to obtain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data. Many plans, providers, and clearinghouses have taken steps to safeguard the privacy of individually identifiable health information. Yet they must currently rely on a patchwork of State laws and regulations that are incomplete and, at times, inconsistent. States have, to varying degrees, attempted to enhance confidentiality by establishing laws governing at least some aspects of medical record privacy. This approach, though a step in the right direction, is inadequate. These laws fail to provide a consistent or comprehensive legal foundation of health information privacy. For example, there is considerable variation among the states in the type of information protected and the scope of the protections provided. See Georgetown Study, at Executive Summary; Lawrence O. Gostin, Zita Lazzarrini, Kathleen M. Flaherty, Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization, Report to Centers for Disease Control, Council of State and Territorial Epidemiologists, and Task Force for Child Survival and Development, Carter Presidential Center (1996) (Gostin Study).

Moreover, electronic health data is becoming increasingly ''national''; as more information becomes available in electronic form, it can have value far beyond the immediate community where the patient resides. Neither private action nor state laws provide a sufficiently comprehensive and rigorous legal structure to allay public concerns, protect the right to privacy, and correct the market failures caused by the absence of privacy protections (see discussion below of market failure under section V.C). Hence, a national policy with consistent rules is necessary to encourage the increased and proper use of electronic information while also protecting the very real needs of patients to safeguard their privacy.

Advances in Genetic Sciences

Recently, scientists completed nearly a decade of work unlocking the mysteries of the human genome, creating tremendous new opportunities to identify and prevent many of the leading causes of death and disability in this country and around the world. Yet the absence of privacy protections for health information endanger these efforts by creating a barrier of distrust and suspicion among consumers. A 1995 national poll found that more than 85 percent of those surveyed were either ''very concerned'' or ''somewhat concerned'' that insurers and employers might gain access to and use genetic information. See Harris Poll, 1995 #34. Sixty-three percent of the 1,000 participants in a 1997 national survey said they would not take genetic tests if insurers and employers could gain access to the results. See ''Genetic Information and the Workplace,'' Department of Labor, Department of Health and Human Services, Equal Employment Opportunity Commission, January 20, 1998. ''In genetic testing studies at the National Institutes of Health, thirty-two percent of eligible people who were offered a test for breast cancer risk declined to take it, citing concerns about loss of privacy and the potential for discrimination in health insurance.'' Sen. Leahy's comments for March 10, 1999 Introduction of the Medical Information Privacy and Security Act.

The Changing Health Care System

The number of entities who are maintaining and transmitting individually identifiable health information has increased significantly over the last 10 years. In addition, the rapid growth of integrated health care delivery systems requires greater use of integrated health information systems. The health care industry has been transformed from one that relied primarily on one-on-one interactions between patients and clinicians to a system of integrated health care delivery networks and managed care providers. Such a system requires the processing and collection of information about patients and plan enrollees (for example, in claims files or enrollment records), resulting in the creation of databases that can be easily transmitted. This dramatic change in the practice of medicine brings with it important prospects for the improvement of the quality of care and reducing the cost of that care. It also, however, means that increasing numbers of people have access to health information. And, as health plan functions are increasingly outsourced, a growing number of organizations not affiliated with our physicians or health plans also have access to health information.

According to the American Health Information Management Association (AHIMA), an average of 150 people ''from nursing staff to x-ray technicians, to billing clerks'' have access to a patient's medical records during the course of a typical hospitalization. While many of these individuals have a legitimate need to see all or part of a patient's records, no laws govern who those people are, what information they are able to see, and what they are and are not allowed to do with that information once they have access to it. According to the National Research Council, individually identifiable health information frequently is shared with:

- Consulting physicians;
- Managed care organizations;
- Health insurance companies
- Life insurance companies;
- Self-insured employers;
- Pharmacies;
- Pharmacy benefit managers;
- Clinical laboratories;
- Accrediting organizations;
- State and Federal statistical agencies; and
- Medical information bureaus.

Much of this sharing of information is done without the knowledge of the patient involved. While many of these functions are important for smooth functioning of the health care system, there are no rules governing how that

information is used by secondary and tertiary users. For example, a pharmacy benefit manager could receive information to determine whether an insurance plan or HMO should cover a prescription, but then use the information to market other products to the same patient. Similarly, many of us obtain health insurance coverage though our employer and, in some instances, the employer itself acts as the insurer. In these cases, the employer will obtain identifiable health information about its employees as part of the legitimate health insurance functions such as claims processing, quality improvement, and fraud detection activities. At the same time, there is no comprehensive protection prohibiting the employer from using that information to make decisions about promotions or job retention.

Public concerns reflect these developments. A 1993 Lou Harris poll found that 75 percent of those surveyed worry that medical information from a computerized national health information system will be used for many non-health reasons, and 38 percent are very concerned. This poll, taken during the health reform efforts of 1993, showed that 85 percent of respondents believed that protecting the confidentiality of medical records is ''absolutely essential'' or ''very essential'' in health care reform. An ACLU Poll in 1994 also found that 75 percent of those surveyed are concerned a ''great deal'' or a ''fair amount''' about insurance companies putting medical information about them into a computer information bank to which others have access. Harris Equifax, Health Information Privacy Study 2,33 (1993) http://www.epic.org/privacy/medical/poll.html. Another survey found that 35 percent of Fortune 500 companies look at people's medical records before making hiring and promotion decisions. Starr, Paul. ''Health and the Right to Privacy,'' American Journal of Law and Medicine, 1999. Vol 25, pp. 193–201.

Concerns about the lack of attention to information privacy in the health care industry are not merely theoretical. In the absence of a national legal framework of health privacy protections, consumers are increasingly vulnerable to the exposure of their personal health information. Disclosure of individually identifiable information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security. Examples of recent privacy breaches include:

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (The Ann Arbor News, February 10, 1999).
- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 2000).
- An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).
- The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).
- A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).
- A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (The New York Times, April 4, 1997 and April 12, 1997).
- A speculator bid $4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients. (New York Times, August 14, 1991).
- In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).
- A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (Orlando Sentinel, November 30, 1997).

No matter how or why a disclosure of personal information is made, the harm to the individual is the same. In the face of industry evolution, the potential benefits of our changing health care system, and the real risks and occurrences of harm, protection of privacy must be built into the routine operations of our health care system.

Privacy Is Necessary To Secure Effective, High Quality Health Care

While privacy is one of the key values on which our society is built, it is more than an end in itself. It is also necessary for the effective delivery of health care, both to individuals and to populations. The market failures caused by the lack of effective privacy protections for health information are discussed below (see section V.C below). Here, we discuss how privacy is a necessary foundation for delivery of high quality health care. In short, the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers.

The need for privacy of health information, in particular, has long been recognized as critical to the delivery of needed medical care. More than anything else, the relationship between a patient and a clinician is based on trust. The clinician must trust the patient to give full and truthful information about their health, symptoms, and medical history. The patient must trust the clinician to use that information to improve his or her health and to respect the need to keep such information private. In order to receive accurate and reliable diagnosis and treatment, patients must provide health care professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives. The provision of health information assists in the diagnosis of an illness or condition, in the development of a treatment plan, and in the evaluation of the effectiveness of that treatment. In the absence of full and accurate information, there is a serious risk that the treatment plan will be inappropriate to the patient's situation.

Patients also benefit from the disclosure of such information to the health plans that pay for and can help them gain access to needed care. Health plans and health care clearinghouses rely on the provision of such information to accurately and promptly process claims for payment and for other administrative functions that directly affect a patient's ability to receive needed care, the quality of that care, and the efficiency with which it is delivered.

Accurate medical records assist communities in identifying troubling public health trends and in evaluating the effectiveness of various public health efforts. Accurate information helps public and private payers make correct payments for care received and lower costs by identifying fraud. Accurate information provides scientists with data they need to conduct research. We cannot improve the quality of health care without information about which treatments work, and which do not.

Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or

shared inappropriately. Privacy violations reduce consumers' trust in the health care system and institutions that serve them. Such a loss of faith can impede the quality of the health care they receive, and can harm the financial health of health care institutions.

Patients who are worried about the possible misuse of their information often take steps to protect their privacy. Recent studies show that a person who does not believe his privacy will be protected is much less likely to participate fully in the diagnosis and treatment of his medical condition. A national survey conducted in January 1999 found that one in five Americans believe their health information is being used inappropriately. See California HealthCare Foundation, ''National Survey: Confidentiality of Medical Records'' (January, 1999) (http://www.chcf.org). More troubling is the fact that one in six Americans reported that they have taken some sort of evasive action to avoid the inappropriate use of their information by providing inaccurate information to a health care provider, changing physicians, or avoiding care altogether. Similarly, in its comments on our proposed rule, the Association of American Physicians and Surgeons reported 78 percent of its members reported withholding information from a patient's record due to privacy concerns and another 87 percent reported having had a patient request to withhold information from their records. For an example of this phenomenon in a particular demographic group, see Drs. Bearman, Ford, and Moody, ''Foregone Health Care among Adolescents,'' JAMA, vol. 282, no. 23 (999); Cheng, T.L., et al., ''Confidentiality in Health Care: A Survey of Knowledge, Perceptions, and Attitudes among High School Students,'' JAMA, vol. 269, no. 11 (1993), at 1404–1407.

The absence of strong national standards for medical privacy has widespread consequences. Health care professionals who lose the trust of their patients cannot deliver high-quality care. In 1999, a coalition of organizations representing various stakeholders including health plans, physicians, nurses, employers, disability and mental health advocates, accreditation organizations as well as experts in public health, medical ethics, information systems, and health policy adopted a set of ''best principles'' for health care privacy that are consistent with the standards we lay out here. (See the Health Privacy Working Group, ''Best Principles for Health Privacy'' (July, 1999) (Best Principles Study). The Best Principles Study states that—

> To protect their privacy and avoid embarrassment, stigma, and discrimination, some people withhold information from their health care providers, provide inaccurate information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by insurance, and—in some cases—avoid care altogether.

Best Principles Study, at 9. In their comments on our proposed rule, numerous organizations representing health plans, health providers, employers, and others acknowledged the value of a set of national privacy standards to the efficient operation of their practices and businesses.

Breaches of Health Privacy Harm More Than Our Health Status

A breach of a person's health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation. For example:

- A banker who also sat on a county health board gained access to patients' records and identified several people with cancer and called in their mortgages. See the National Law Journal, May 30, 1994.
- A physician was diagnosed with AIDS at the hospital in which he practiced medicine. His surgical privileges were suspended. See *Estate of Behringer* v. *Medical Center at Princeton,* 249 N.J. Super. 597.
- A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt. See New York Times, October 10, 1992, Section 1, page 25.
- A 30-year FBI veteran was put on administrative leave when, without his permission, his pharmacy released information about his treatment for depression. (Los Angeles Times, September 1, 1998) Consumer Reports found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission. ''Who's reading your Medical Records,'' Consumer Reports, October 1994, at 628, paraphrasing Sweeny, Latanya, ''Weaving Technology and Policy Together to Maintain Confidentiality,'' The Journal Of Law Medicine and Ethics (Summer & Fall 1997) Vol. 25, Numbers 2,3.

The answer to these concerns is not for consumers to withdraw from society and the health care system, but for society to establish a clear national legal framework for privacy. By spelling out what is and what is not an allowable use of a person's identifiable health information, such standards can help to restore and preserve trust in the health care system and the individuals and institutions that comprise that system. As medical historian Paul Starr wrote: ''Patients have a strong interest in preserving the privacy of their personal health information but they also have an interest in medical research and other efforts by health care organizations to improve the medical care they receive. As members of the wider community, they have an interest in public health measures that require the collection of personal data.'' (P. Starr, ''Health and the Right to Privacy,'' American Journal of Law & Medicine, 25, nos. 2&3 (1999) 193–201). The task of society and its government is to create a balance in which the individual's needs and rights are balanced against the needs and rights of society as a whole.

National standards for medical privacy must recognize the sometimes competing goals of improving individual and public health, advancing scientific knowledge, enforcing the laws of the land, and processing and paying claims for health care services. This need for balance has been recognized by many of the experts in this field. Cavoukian and Tapscott described it this way: ''An individual's right to privacy may conflict with the collective rights of the public * * *. We do not suggest that privacy is an absolute right that reigns supreme over all other rights. It does not. However, the case for privacy will depend on a number of factors that can influence the balance—the level of harm to the individual involved versus the needs of the public.''

The Federal Response

There have been numerous federal initiatives aimed at protecting the privacy of especially sensitive personal information over the past several years—and several decades. While the rules below are likely the largest single federal initiative to protect privacy, they are by no means alone in the field. Rather, the rules arrive in the context of recent legislative activity to grapple with advances in technology, in addition to an already established body of law granting federal protections for personal privacy.

In 1965, the House of Representatives created a Special Subcommittee on Invasion of Privacy. In 1973, this Department's predecessor agency, the Department of Health, Education and Welfare issued The Code of Fair Information Practice Principles establishing an important baseline for

information privacy in the U.S. These principles formed the basis for the federal Privacy Act of 1974, which regulates the government's use of personal information by limiting the disclosure of personally-identifiable information, allows consumers access to information about them, requires federal agencies to specify the purposes for collecting personal information, and provides civil and criminal penalties for misuse of information.

In the last several years, with the rapid expansion in electronic technology—and accompanying concerns about individual privacy—laws, regulations, and legislative proposals have been developed in areas ranging from financial privacy to genetic privacy to the safeguarding of children on-line. For example, the Children's Online Privacy Protection Act was enacted in 1998, providing protection for children when interacting at web-sites. In February, 2000, President Clinton signed Executive Order 13145, banning the use of genetic information in federal hiring and promotion decisions. The landmark financial modernization bill, signed by the President in November, 1999, likewise contained financial privacy protections for consumers. There also has been recent legislative activity on establishing legal safeguards for the privacy of individuals' Social Security numbers, and calls for regulation of on-line privacy in general.

These most recent laws, regulations, and legislative proposals come against the backdrop of decades of privacy-enhancing statutes passed at the federal level to enact safeguards in fields ranging from government data files to video rental records. In the 1970s, individual privacy was paramount in the passage of the Fair Credit Reporting Act (1970), the Privacy Act (1974), the Family Educational Rights and Privacy Act (1974), and the Right to Financial Privacy Act (1978). These key laws were followed in the next decade by another series of statutes, including the Privacy Protection Act (1980), the Electronic Communications Privacy Act (1986), the Video Privacy Protection Act (1988), and the Employee Polygraph Protection Act (1988). In the last ten years, Congress and the President have passed additional legal privacy protection through, among others, the Telephone Consumer Protection Act (1991), the Driver's Privacy Protection Act (1994), the Telecommunications Act (1996), the Children's Online Privacy Protection Act (1998), the Identity Theft and Assumption Deterrence Act (1998), and Title V of the Gramm-Leach-Bliley Act (1999) governing financial privacy.

In 1997, a Presidential advisory commission, the Advisory Commission on Consumer Protection and Quality in the Health Care Industry, recognized the need for patient privacy protection in its recommendations for a Consumer Bill of Rights and Responsibilities (November 1997). In 1997, Congress enacted the Balanced Budget Act (Public Law 105–34), which added language to the Social Security Act (18 U.S.C. 1852) to require Medicare+Choice organizations to establish safeguards for the privacy of individually identifiable patient information. Similarly, the Veterans Benefits section of the U.S. Code provides for confidentiality of medical records in cases involving drug abuse, alcoholism or alcohol abuse, HIV infection, or sickle cell anemia (38 U.S.C. 7332).

As described in more detail in the next section, Congress recognized the importance of protecting the privacy of health information by enacting the Health Insurance Portability and Accountability Act of 1996. The Act called on Congress to enact a medical privacy statute and asked the Secretary of Health and Human Services to provide Congress with recommendations for protecting the confidentiality of health care information. The Congress further recognized the importance of such standards by providing the Secretary with authority to promulgate regulations on health care privacy in the event that lawmakers were unable to act within the allotted three years.

Finally, it also is important for the U.S. to join the rest of the developed world in establishing basic medical privacy protections. In 1995, the European Union (EU) adopted a Data Privacy Directive requiring its 15 member states to adopt consistent privacy laws by October 1998. The EU urged all other nations to do the same or face the potential loss of access to information from EU countries.

Statutory Background

History of the Privacy Component of the Administrative Simplification Provisions

The Congress addressed the opportunities and challenges presented by the rapid evolution of health information systems in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, which was enacted on August 21, 1996. Sections 261 through 264 of HIPAA are known as the Administrative Simplification provisions. The major part of these Administrative Simplification provisions are found at section 262 of HIPAA, which enacted a new part C of title XI of the Social Security Act (hereinafter we refer to the Social Security Act as the ''Act'' and we refer to all other laws cited in this document by their names).

In section 262, Congress primarily sought to facilitate the efficiencies and cost savings for the health care industry that the increasing use of electronic technology affords. Thus, section 262 directs HHS to issue standards to facilitate the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with such transactions.

At the same time, Congress recognized the challenges to the confidentiality of health information presented by the increasing complexity of the health care industry, and by advances in health information systems technology and communications. Section 262 thus also directs HHS to develop standards to protect the security, including the confidentiality and integrity, of health information.

Congress has long recognized the need for protection of health information privacy generally, as well as the privacy implications of electronic data interchange and the increased ease of transmitting and sharing individually identifiable health information. Congress has been working on broad health privacy legislation for many years and, as evidenced by the self-imposed three year deadline included in the HIPAA, discussed below, believes it can and should enact such legislation. A significant portion of the first Administrative Simplification section debated on the floor of the Senate in 1994 (as part of the Health Security Act) consisted of privacy provisions. In the version of the HIPAA passed by the House of Representatives in 1996, the requirement for the issuance of privacy standards was located in the same section of the bill (section 1173) as the requirements for issuance of the other HIPAA Administrative Simplification standards. In conference, the requirement for privacy standards was moved to a separate section in the same part of HIPAA, section 264, so that Congress could link the Privacy standards to Congressional action.

Section 264(b) requires the Secretary of HHS to develop and submit to the Congress recommendations for:

- The rights that an individual who is a subject of individually identifiable health information should have.

• The procedures that should be established for the exercise of such rights.

• The uses and disclosures of such information that should be authorized or required.

The Secretary's Recommendations were submitted to the Congress on September 11, 1997. Section 264(c)(1) provides that:

> If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by [August 21, 1999], the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than [February 21, 2000]. Such regulations shall address at least the subjects described in subsection (b).

As the Congress did not enact legislation regarding the privacy of individually identifiable health information prior to August 21, 1999, HHS published proposed rules setting forth such standards on November 3, 1999, 64 FR 59918, and is now publishing the mandated final regulation.

These privacy standards have been, and continue to be, an integral part of the suite of Administrative Simplification standards intended to simplify and improve the efficiency of the administration of our health care system.

The Administrative Simplification Provisions, and Regulatory Actions to Date

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose several requirements on HHS, health plans, health care clearinghouses, and health care providers who conduct the identified transactions electronically.

The first section, section 1171 of the Act, establishes definitions for purposes of part C of title XI for the following terms: code set, health care clearinghouse, health care provider, health information, health plan, individually identifiable health information, standard, and standard setting organization.

Section 1172 of the Act makes the standard adopted under part C applicable to: (1) Health plans, (2) health care clearinghouses, and (3) health care providers who transmit health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act (hereinafter referred to as the ''covered entities''). Section 1172 also contains procedural requirements concerning the adoption of standards, including the role of standard setting organizations and required consultations, summarized in subsection F and section VI, below.

Section 1173 of the Act requires the Secretary to adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically. Section 1173(a)(1) describes the transactions to be promulgated, which include the nine transactions listed in section 1173(a)(2) and other transactions determined appropriate by the Secretary. The remainder of section 1173 sets out requirements for the specific standards the Secretary is to adopt: Unique health identifiers, code sets, security standards, electronic signatures, and transfer of information among health plans. Of particular relevance to this proposed rule is section 1173(d), the security standard provision. The security standard authority applies to both the transmission and the maintenance of health information, and requires the entities described in section 1172(a) to maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the information, protect against reasonably anticipated threats or hazards to the security or integrity of the information or unauthorized uses or disclosures of the information, and to ensure compliance with part C by the entity's officers and employees.

In section 1174 of the Act, the Secretary is required to establish standards for all of the above transactions, except claims attachments, by February 21, 1998. The statutory deadline for the claims attachment standard is February 21, 1999.

As noted above, a proposed rule for most of the transactions was published on May 7, 1998, and the final Transactions Rule was promulgated on August 17, 2000. The delay was caused by the deliberate consensus building process, working with industry, and the large number of comments received (about 17,000). In addition, in a series of Notices of Proposed Rulemakings, HHS published other proposed standards, as described above. Each of these steps was taken in concert with the affected professions and industries, to ensure rapid adoption and compliance.

Generally, after a standard is established, it may not be changed during the first year after adoption except for changes that are necessary to permit compliance with the standard. Modifications to any of these standards may be made after the first year, but not more frequently than once every 12 months. The Secretary also must ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets and that there are crosswalks from prior versions.

Section 1175 of the Act prohibits health plans from refusing to process, or from delaying processing of, a transaction that is presented in standard format. It also establishes a timetable for compliance: each person to whom a standard or implementation specification applies is required to comply with the standard within 24 months (or 36 months for small health plans) of its adoption. A health plan or other entity may, of course, comply voluntarily before the effective date. The section also provides that compliance with modifications to standards or implementation specifications must be accomplished by a date designated by the Secretary, which date may not be earlier than 180 days from the notice of change.

Section 1176 of the Act establishes civil monetary penalties for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than $100 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year. The procedural provisions of section 1128A of the Act apply to actions taken to obtain civil monetary penalties under this section.

Section 1177 establishes penalties for any person that knowingly uses a unique health identifier, or obtains or discloses individually identifiable health information in violation of the part. The penalties include: (1) A fine of not more than $50,000 and/or imprisonment of not more than 1 year; (2) if the offense is ''under false pretenses,'' a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years.

Under section 1178 of the Act, the requirements of part C, as well as any standards or implementation specifications adopted thereunder, preempt contrary state law. There are three exceptions to this general rule of preemption: State laws that the Secretary determines are necessary for certain purposes set forth in the statute; state laws that the Secretary determines address controlled substances; and state laws relating to the privacy of

individually identifiable health information that are contrary to and more stringent than the federal requirements. There also are certain areas of state law (generally relating to public health and oversight of health plans) that are explicitly carved out of the general rule of preemption and addressed separately.

Section 1179 of the Act makes the above provisions inapplicable to financial institutions (as defined by section 1101 of the Right to Financial Privacy Act of 1978) or anyone acting on behalf of a financial institution when ''authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution.''

Finally, as explained above, section 264 requires the Secretary to issue standards with respect to the privacy of individually identifiable health information. Section 264 also contains a preemption provision that provides that contrary provisions of state laws that are more stringent than the federal standards, requirements, or implementation specifications will not be preempted.

Our Approach to This Regulation

Balance

A number of facts informed our approach to this regulation. Determining the best approach to protecting privacy depends on where we start, both with respect to existing legal expectations and also with respect to the expectations of individuals, health care providers, payers and other stakeholders. From the comments we received on the proposed rule, and from the extensive fact finding in which we engaged, a confused picture developed. We learned that stakeholders in the system have very different ideas about the extent and nature of the privacy protections that exist today, and very different ideas about appropriate uses of health information. This leads us to seek to balance the views of the different stakeholders, weighing the varying interests on each particular issue with a view to creating balance in the regulation as a whole.

For example, we received hundreds of comments explaining the legitimacy of various uses and disclosure of health information. We agree that many uses and disclosures of health information are ''legitimate,'' but that is not the end of the inquiry. Neither privacy, nor the important social goals described by the commenters, are absolutes. In this regulation, we are asking health providers and institutions to add privacy into the balance, and we are asking individuals to add social goals into the balance.

The vast difference among regulated entities also informed our approach in significant ways. This regulation applies to solo practitioners, and multi-national health plans. It applies to pharmacies and information clearinghouses. These entities differ not only in the nature and scope of their businesses, but also in the degree of sophistication of their information systems and information needs. We therefore designed the core requirements of this regulation to be flexible and ''scalable.'' This is reflected throughout the rule, particularly in the implementation specifications for making the minimum necessary uses and disclosures, and in the administrative policies and procedures requirements.

We also are informed by the rapid evolution in industry organization and practice. Our goal is to enhance privacy protections in ways that do not impede this evolution. For example, we received many comments asking us to assign a status under this regulation based on a label or title. For example, many commenters asked whether ''disease management'' is a ''health care operation,'' or whether a ''pharmacy benefits manager'' is a covered entity. From the comments and our fact-finding, however, we learned that these terms do not have consistent meanings today; rather, they encompass diverse activities and information practices. Further, the statutory definitions of key terms such as health care provider and health care clearinghouse describe functions, not specific types of persons or entities. To respect both the Congressional approach and industry evolution, we design the rule to follow activities and functions, not titles and labels.

Similarly, many comments asked whether a particular person would be a ''business associate'' under the rule, based on the nature of the person's business. Whether a business associate arrangement must exist under the rule, however, depends on the relationship between the entities and the services being performed, not on the type of persons or companies involved.

Our approach is also significantly informed by the limited jurisdiction conferred by HIPAA. In large part, we have the authority to regulate those who create and disclose health information, but not many key stakeholders who receive that health information from a covered entity. Again, this led us to look to the balance between the burden on covered entities and need to protect privacy in determining our approach to such disclosures. In some instances, we approach this dilemma by requiring covered entities to obtain a representation or documentation of purpose from the person requesting information. While there would be advantages to legislation regulating such third persons directly, we cannot justify abandoning any effort to enhance privacy.

It also became clear from the comments and our fact-finding that we have expectations as a society that conflict with individuals' views about the privacy of health information. We expect the health care industry to develop treatment protocols for the delivery of high quality health care. We expect insurers and the government to reduce fraud in the health care system. We expect to be protected from epidemics, and we expect medical research to produce miracles. We expect the police to apprehend suspects, and we expect to pay for our care by credit card. All of these activities involve disclosure of health information to someone other than our physician.

While most commenters support the concept of health privacy in general, many go on to describe activities that depend on the disclosure of health information and urge us to protect those information flows. Section III, in which we respond to the comments, describes our approach to balancing these conflicting expectations.

Finally, we note that many commenters were concerned that this regulation would lessen current privacy protections. It is important to understand this regulation as a new federal floor of privacy protections that does not disturb more protective rules or practices. Nor do we intend this regulation to describe a set of a ''best practices.'' Rather, this regulation describes a set of basic consumer protections and a series of regulatory permissions for use and disclosure of health information. The protections are a mandatory floor, which other governments and any covered entity may exceed. The permissions are just that, permissive—the only disclosures of health information required under this rule are to the individual who is the subject of the information or to the Secretary for enforcement of this rule. We expect covered entities to rely on their professional ethics and use their own best judgements in deciding which of these permissions they will use.

Combining Workability With New Protections

This rule establishes national minimum standards to protect the privacy of individually identifiable health information in prescribed

settings. The standards address the many varied uses and disclosures of individually identifiable health information by health plans, certain health care providers and health care clearinghouses. The complexity of the standards reflects the complexity of the health care marketplace to which they apply and the variety of subjects that must be addressed. The rule applies not only to the core health care functions relating to treating patients and reimbursing health care providers, but also to activities that range from when individually identifiable health information should be available for research without authorization to whether a health care provider may release protected health information about a patient for law enforcement purposes. The number of discrete provisions, and the number of commenters requesting that the rule recognize particular activities, is evidence of the significant role that individually identifiable health information plays in many vital public and private concerns.

At the same time, the large number of comments from individuals and groups representing individuals demonstrate the deep public concern about the need to protect the privacy of individually identifiable health information. The discussion above is rich with evidence about the importance of protecting privacy and the potential adverse consequences to individuals and their health if such protections are not extended.

The need to balance these competing interests—the necessity of protecting privacy and the public interest in using identifiable health information for vital public and private purposes—in a way that is also workable for the varied stakeholders causes much of the complexity in the rule. Achieving workability without sacrificing protection means some level of complexity, because the rule must track current practices and current practices are complex. We believe that the complexity entailed in reflecting those practices is better public policy than a perhaps simpler rule that disturbed important information flows.

Although the rule taken as a whole is complicated, we believe that the standards are much less complex as they apply to particular actors. What a health plan or covered health care provider must do to comply with the rule is clear, and the two-year delayed implementation provides a substantial period for trade and professional associations, working with their members, to assess the effects of the standards and develop policies and procedures to come into compliance with them. For individuals, the system may look substantially more complicated because, for the first time, we are ensuring that individuals will receive detailed information about how their individually identifiable health information may be used and disclosed. We also provide individuals with additional tools to exercise some control over those uses and disclosures. The additional complexity for individuals is the price of expanding their understanding and their rights.

The Department will work actively with members of the health care industry, representatives of individuals and others during the implementation of this rule. As stated elsewhere, our focus is to develop broader understanding of how the standards work and to facilitate compliance. We intend to provide guidance and check lists as appropriate, particularly to small businesses affected by the rule. We also will work with trade and professional associations to develop guidance and provide technical assistance so that they can help their members understand and comply with these new standards. If this effort is to succeed, the various public and private participants inside and outside of the health care system will need to work together to assure that the competing interests described above remain in balance and that an ethic that recognizes their importance is established.

Enforcement

The Secretary has decided to delegate her responsibility under this regulation to the Department's Office for Civil Rights (OCR). OCR will be responsible for enforcement of this regulation. Enforcement activities will include working with covered entities to secure voluntary compliance through the provision of technical assistance and other means; responding to questions regarding the regulation and providing interpretations and guidance; responding to state requests for exception determinations; investigating complaints and conducting compliance reviews; and, where voluntary compliance cannot be achieved, seeking civil monetary penalties and making referrals for criminal prosecution.

Consent

Current Law and Practice

The issue that drew the most comments overall is the question of when individuals' permission should be obtained prior to use or disclosure of their health information. We learned that individuals' views and the legal view of ''consent'' for use and disclosure of health information are different and in many ways incompatible. Comments from individuals revealed a common belief that, today, people must be asked permission for each and every release of their health information. Many believe that they ''own'' the health records about them. However, current law and practice do not support this view.

Current privacy protection practices are determined in part by the standards and practices that the professional associations have adopted for their members. Professional codes of conduct for ethical behavior generally can be found as opinions and guidelines developed by organizations such as the American Medical Association, American Nurses' Association, the American Hospital Association, the American Psychiatric Association, and the American Dental Association. These are generally issued though an organization's governing body. The codes do not have the force of law, but providers often recognize them as binding rules.

Our review of professional codes of ethics revealed partial, but loose, support for individuals' expectations of privacy. For example, the American Medical Association's Code of Ethics recognizes both the right to privacy and the need to balance it against societal needs. It reads in part: ''conflicts between a patient's right to privacy and a third party's need to know should be resolved in favor of the patient, except where that would result in serious health hazard or harm to the patient or others.'' AMA Policy No 140.989. See also, Mass. Med. Society, Patient Privacy and Confidentiality (1996), at 14:

> Patients enter treatment with the expectation that the information they share will be used exclusively for their clinical care. Protection of our patients' confidences is an integral part of our ethical training.

These codes, however, do not apply to many who obtain information from providers. For example, the National Association of Insurance Commissioners model code, ''Health Information Privacy Model Act'' (1998), applies to insurers but has not been widely adopted. Codes of ethics are also often written in general terms that do not provide guidance to providers and plans confronted with specific questions about protecting health information.

State laws are a crucial means of protecting health information, and today state laws vary dramatically. Some states defer to the professional codes of conduct, others provide general guidelines for privacy protection, and

others provide detailed requirements relating to the protection of information relating to specific diseases or to entire classes of information. Cf., D.C. Code Ann. § 2–3305.14(16) and Haw. Rev. Stat. 323C, *et seq.* In general, state statutes and case law addressing consent to use of health information do not support the public's strong expectations regarding consent for use and disclosure of health information. Only about half of the states have a general law that prohibits disclosure of health information without patient authorization and some of these are limited to hospital medical records.

Even when a state has a law limiting disclosure of health information, the law typically exempts many types of disclosure from the authorization requirement. Georgetown Study, Key Findings; Lisa Dahm, ''50-State Survey on Patient Health Care Record Confidentiality,'' American Health Lawyers Association (1999). One of the most common exemptions from a consent requirement is disclosure of health information for treatment and related purposes. See, *e.g.,* Wis.Stat. § 164.82; Cal. Civ. Code 56:10; National Conference of Commissioners on Uniform State Laws, *Uniform Health-Care Information Act, Minneapolis, MN, August 9, 1985.* Some states include utilization review and similar activities in the exemption. See, *e.g.,* Ariz. Rev. Stat. § 12–2294. Another common exemption from consent is disclosure of health information for purposes of obtaining payment. See, *e.g.,* Fla. Stat. Ann. § 455.667; Tex. Rev. Civ. Stat. Art. 4495, § 5.08(h); 410 Ill. Comp. Stat. 50/3(d). Other common exemptions include disclosures for emergency care, and for disclosures to government authorities (such as a department of public health). See Gostin Study, at 1–2; 48–51. Some states also exempt disclosure to law enforcement officials (*e.g.,* Massachusetts, Ch. 254 of the Acts of 2000), coroners (Wis. Stat. § 146.82), and for such purposes as business operations, oversight, research, and for directory information. Under these exceptions, providers can disclose health information without any consent or authorization from the patient. When states require specific, written authorization for disclosure of health information, the authorizations are usually only required for certain types of disclosures or certain types of information, and one authorization can suffice for multiple disclosures over time.

The states that do not have laws prohibiting disclosure of health information impose no specific requirements for consent or authorization prior to release of health information. There may, however, be other controls on release of health information. For instance, most health care professional licensure laws include general prohibitions against ''breaches of confidentiality.'' In some states, patients can hold providers accountable for some unauthorized disclosures of health information about them under various tort theories, such as invasion of privacy and breach of a confidential relationship. While these controls may affect certain disclosure practices, they do not amount to a requirement that a provider obtain authorization for each and every disclosure of health information.

Further, patients are typically not given a choice; they must sign the ''consent'' in order to receive care. As the Georgetown Study points out, ''In effect, the authorization may function more as a waiver of consent—the patient may not have an opportunity to object to any disclosures.'' Georgetown Study, Key Findings.

In the many cases where neither state law nor professional ethical standards exist, the only privacy protection individuals have is limited to the policies and procedures that the health care entity adopts. Corporate privacy policies are often proprietary. While several professional associations attached their privacy principles to their comments, health care entities did not. One study we found indicates that these policies are not adequate to provide appropriate privacy protections and alleviate public concern. The Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure made multiple findings highlighting the need for heightened privacy and security, including:

> Finding 5: The greatest concerns regarding the privacy of health information derives from widespread sharing of patient information throughout the health care industry and the inadequate federal and state regulatory framework for systematic protection of health information.
>
> *For the Record: Protecting Electronic Health Information*, National Academy Press, Washington DC, 1997.

Consent Under This Rule

In the NPRM, we expressed concern about the coercive nature of consents currently obtained by providers and plans relating to the use and disclosure of health information. We also expressed concern about the lack of information available to the patient during the process, and the fact that patients often were not even presented with a copy of the consent that they have signed. These and other concerns led us to propose that covered entities be permitted to use and disclose protected health information for treatment, payment and health care operations without the express consent of the subject individual.

In the final rule, we alter our proposed approach and require, in most instances, that health care providers who have a direct treatment relationship with their patients obtain the consent of their patients to use and disclose protected health information for treatment, payment and health care operations. While our concern about the coerced nature of these consents remains, many comments that we received from individuals, health care professionals, and organizations that represent them indicated that both patients and practitioners believe that patient consent is an important part of the current health care system and should be retained.

Providing and obtaining consent clearly has meaning for patients and practitioners. Patient advocates argued that the act of signing focuses the patient's attention on the substance of the transaction and provides an opportunity for the patient to ask questions about or seek modifications in the provider's practices. Many health care practitioners and their representatives argued that seeking a patient's consent to disclose confidential information is an ethical requirement that strengthens the physician-patient relationship. Both practitioners and patients argued that the approach proposed in the NPRM actually reduced patient protections by eliminating the opportunity for patients to agree to how their confidential information would be used and disclosed.

While we believe that the provisions in the NPRM that provided for detailed notice to the patient and the right to request restrictions would have provided an opportunity for patients and providers to discuss and negotiate over information practices, it is clear from the comments that many practitioners and patients believe the approach proposed in the NPRM is not an acceptable replacement for the patient providing consent.

To encourage a more informed interaction between the patient and the provider during the consent process, the final rule requires that the consent form that is presented to the patient be accompanied by a notice that contains a detailed discussion of the provider's health information practices. The consent form must reference the notice and also must inform the patient that he

or she has the right to ask the health care provider to request certain restrictions as to how the information of the patient will be used or disclosed. Our goal is to provide an opportunity for and to encourage more informed discussions between patients and providers about how protected health information will be used and disclosed within the health care system.

We considered and rejected other approaches to consent, including those that involved individuals providing a global consent to uses and disclosures when they sign up for insurance. While such approaches do require the patient to provide consent, it is not really an informed one or a voluntary one. It is also unclear how a consent obtained at the enrollment stage would be meaningfully communicated to the many providers who create the health information in the first instance. The ability to negotiate restrictions or otherwise have a meaningful discussion with the front-line provider would be independent of, and potentially in conflict with, the consent obtained at the enrollment stage. In addition, employers today are moving toward simplified enrollment forms, using check-off boxes and similar devices. The opportunity for any meaningful consideration or interaction at that point is slight. For these and other reasons, we decided that, to the extent a consent can accomplish the goal sought by individuals and providers, it must be focused on the direct interaction between an individual and provider.

The comments and fact-finding indicate that our approach will not significantly change the administrative aspect of consent as it exists today. Most direct treatment providers today obtain some type of consent for some uses and disclosures of health information. Our regulation will ensure that those consents cover the routine uses and disclosures of health information, and provide an opportunity for individuals to obtain further information and have further discussion, should they so desire.

Administrative Costs

Section 1172(b) of the Act provides that ''[a]ny standard adopted under this part [part C of title XI of the Act] shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.'' The privacy and security standards are the platform on which the remaining standards rest; indeed, the design of part C of title XI makes clear that the various standards are intended to function together. Thus, the costs of privacy and security are properly attributable to the suite of administrative simplification regulations as a whole, and the cost savings realized should likewise be calculated on an aggregated basis, as is done below. Because the privacy standards are an integral and necessary part of the suite of Administrative Simplification standards, and because that suite of standards will result in substantial administrative cost savings, the privacy standards are ''consistent with the objective of reducing the administrative costs of providing and paying for health care.''

As more fully discussed in the Regulatory Impact and Regulatory Flexibility analyses below, we recognize that these privacy standards will entail substantial initial and ongoing administrative costs for entities subject to the rules. It is also the case that the privacy standards, like the security standards authorized by section 1173(d) of the Act, are necessitated by the technological advances in information exchange that the remaining Administrative Simplification standards facilitate for the health care industry. The same technological advances that make possible enormous administrative cost savings for the industry as a whole have also made it possible to breach the security and privacy of health information on a scale that was previously inconceivable. The Congress recognized that adequate protection of the security and privacy of health information is a *sine qua non* of the increased efficiency of information exchange brought about by the electronic revolution, by enacting the security and privacy provisions of the law. Thus, as a matter of policy as well as law, the administrative standards should be viewed as a whole in determining whether they are ''consistent with'' the objective of reducing administrative costs.

Consultations

The Congress required the Secretary to consult with specified groups in developing the standards under sections 262 and 264. Section 264(d) of HIPAA specifically requires the Secretary to consult with the National Committee on Vital and Health Statistics (NCVHS) and the Attorney General in carrying out her responsibilities under the section. Section 1172(b)(3) of the Act, which was enacted by section 262, requires that, in developing a standard under section 1172 for which no standard setting organization has already developed a standard, the Secretary must, before adopting the standard, consult with the National Uniform Billing Committee (NUBC), the National Uniform Claim Committee (NUCC), the Workgroup for Electronic Data Interchange (WEDI), and the American Dental Association (ADA). Section 1172(f) also requires the Secretary to rely on the recommendations of the NCVHS and consult with other appropriate federal and state agencies and private organizations.

We engaged in the required consultations including the Attorney General, NUBC, NUCC, WEDI and the ADA. We consulted with the NCVHS in developing the Recommendations, upon which this proposed rule is based. We continued to consult with this committee by requesting the committee to review the proposed rule and provide comments prior to its publication, and by reviewing transcripts of its public meeting on privacy and related topics. We consulted with representatives of the National Congress of American Indians, the National Indian Health Board, and the self governance tribes. We also met with representatives of the National Governors' Association, the National Conference of State Legislatures, the National Association of Public Health Statistics and Information Systems, and a number of other state organizations to discuss the framework for the proposed rule, issues of special interests to the states, and the process for providing comments on the proposed rule.

Many of these groups submitted comments to the proposed rule, and those were taken into account in developing the final regulation.

In addition to the required consultations, we met with numerous individuals, entities, and agencies regarding the regulation, with the goal of making these standards as compatible as possible with current business practices, while still enhancing privacy protection. During the open comment period, we met with dozens of groups.

Relevant federal agencies participated in the interagency working groups that developed the NPRM and the final regulation, with additional representatives from all operating divisions and many staff offices of HHS. The following federal agencies and offices were represented on the interagency working groups: the Department of Justice, the Department of Commerce, the Social Security Administration, the Department of Defense, the Department of Veterans Affairs, the Department of Labor, the Office of Personnel Management, and the Office of Management and Budget.

II. Section-by-Section Description of Rule Provisions

Part 160—Subpart A—General Provisions

Part 160 applies to all the administrative simplification regulations. We include the entire regulation text in this rule, not just those provisions relevant to this Privacy regulation. For example, the term ''trading partner'' is defined here, for use in the Health Insurance Reform: Standards for Electronic Transactions regulation, published at 65 FR 50312, August 17, 2000 (the ''Transactions Rule''). It does not appear in the remainder of this Privacy rule.

Sections 160.101 and 160.104 of Subpart A of part 160 were promulgated in the Transactions Rule, and we do not change them here. We do, however, make changes and additions to § 160.103, the definitions section of Subpart A. The definitions that were promulgated in the Transactions Rule and that remain unchanged here are: Act, ANSI, covered entity, compliance date, group health plan, HCFA, HHS, health care provider, health information, health insurance issuer, health maintenance organization, modify or modification, Secretary, small health plan, standard setting organization, and trading partner agreement. Of these terms, we discuss further in this preamble only covered entity and health care provider.

Section 160.102—Applicability

The proposed rule stated that the subchapter (Parts 160, 162, and 164) applies to the entities set out at section 1172(a) of the Act: Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction covered by the subchapter. The final rule adds a provision (§ 160.102(b)) clarifying that to the extent required under section 201(a)(5) of HIPAA, nothing in the subchapter is to be construed to diminish the authority of any Inspector General. This was done in response to comment, to clarify that the administrative simplification rules, including the rules below, do not conflict with the cited provision of HIPAA.

Section 160.103—Definitions

Business Associate

We proposed to define the term ''business partner'' to mean, with respect to a covered entity, a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. ''Business partner'' would have included contractors or other persons who receive protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities. ''Business partner'' would have excluded persons who are within the covered entity's workforce, as defined in this section.

This rule reflects the change in the name from ''business partner'' to ''business associate,'' included in the Transactions Rule.

In the final rule, we change the definition of ''business associate'' to clarify the circumstances in which a person is acting as a business associate of a covered entity. The changes clarify that the business association occurs when the right to use or disclose the protected health information belongs to the covered entity, and another person is using or disclosing the protected health information (or creating, obtaining and using the protected health information) to perform a function or activity on behalf of the covered entity. We also clarify that providing specified services to a covered entity creates a business associate relationship if the provision of the service involves the disclosure of protected health information to the service provider. In the proposed rule, we had included a list of persons that were considered to be business partners of the covered entity. However, it is not always clear whether the provision of certain services to a covered entity is ''for'' the covered entity or whether the service provider is acting ''on behalf of'' the covered entity. For example, a person providing management consulting services may need protected health information to perform those services, but may not be acting ''on behalf of'' the covered entity. This we believe led to some general confusion among the commenters as to whether certain arrangements fell within the definition of a business partner under the proposed rule. The construction of the final rule clarifies that the provision of the specified services gives rise to a business associate relationship if the performance of the service involves disclosure of protected health information by the covered entity to the business associate. The specified services are legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, and financial services. The list is intended to include the types of services commonly provided to covered entities where the disclosure of protected health information is routine to the performance of the service, but when the person providing the service may not always be acting ''on behalf of'' the covered entity.

In the final rule, we reorganize the list of examples of the functions or activities that may be conducted by business associates. We place a part of the proposed list in the portion of the definition that addresses when a person is providing functions or activities for or on behalf of a covered entity. We place other parts of the list in the portion of the definition that specifies the services that give rise to a business associate relationship, as discussed above. We also have expanded the examples to provide additional guidance and in response to questions from commenters.

We have added data aggregation to the list of services that give rise to a business associate relationship. Data aggregation, as discussed below, is where a business associate in its capacity as the business associate of one covered entity combines the protected health information of such covered entity with protected health information received by the business associate in its capacity as a business associate of another covered entity in order to permit the creation of data for analyses that relate to the health care operations of the respective covered entities. Adding this service to the business associate definition clarifies the ability of covered entities to contract with business associates to undertake quality assurance and comparative analyses that involve the protected health information of more than one contracting covered entity. For example, a state hospital association could act as a business associate of its member hospitals and could combine data provided to it to assist the hospitals in evaluating their relative performance in areas such as quality, efficiency and other patient care issues. As discussed below, however, the business associate contracts of each of the hospitals would have to permit the activity, and the protected health information of one hospital could not be disclosed to another hospital unless the disclosure is otherwise permitted by the rule.

The definition also states that a business associate may be a covered entity, and that business associate excludes a person who is part of the covered entity's workforce.

We also clarify in the final rule that a business association arises with

respect to a covered entity when a person performs functions or activities on behalf of, or provides the specified services to or for, an organized health care health care arrangement in which the covered entity participates. This change recognizes that where covered entities participate in certain joint arrangements for the financing or delivery of health care, they often contract with persons to perform functions or to provide services for the joint arrangement. This change is consistent with changes made in the final rule to the definition of health care operations, which permits covered entities to use or disclose protected health information not only for their own health care operations, but also for the operations of an organized health care arrangement in which the covered entity participates. By making these changes, we avoid the confusion that could arise in trying to determine whether a function or activity is being provided on behalf of (or if a specified service is being provided to or for) a covered entity or on behalf of or for a joint enterprise involving the covered entity. The change clarifies that in either instance the person performing the function or activity (or providing the specified service) is a business associate.

We also add language to the final rule that clarifies that the mere fact that two covered entities participate in an organized health care arrangement does not make either of the covered entities a business associate of the other covered entity. The fact that the entities participate in joint health care operations or other joint activities, or pursue common goals through a joint activity, does not mean that one party is performing a function or activity on behalf of the other party (or is providing a specified services to or for the other party).

In general under this provision, actions relating to the protected health information of an individual undertaken by a business associate are considered, for the purposes of this rule, to be actions of the covered entity, although the covered entity is subject to sanctions under this rule only if it has knowledge of the wrongful activity and fails to take the required actions to address the wrongdoing. For example, if a business associate maintains the medical records or manages the claims system of a covered entity, the covered entity is considered to have protected health information and the covered entity must ensure that individuals who are the subject of the information can have access to it pursuant to § 164.524.

The business associate relationship does not describe all relationships between covered entities and other persons or organizations. While we permit uses or disclosures of protected health information for a variety of purposes, business associate contracts or other arrangements are only required for those cases in which the covered entity is disclosing information to someone or some organization that will use the information on behalf of the covered entity, when the other person will be creating or obtaining protected health information on behalf of the covered entity, or when the business associate is providing the specified services to the covered entity and the provision of those services involves the disclosure of protected health information by the covered entity to the business associate. For example, when a health care provider discloses protected health information to health plans for payment purposes, no business associate relationship is established. While the covered provider may have an agreement to accept discounted fees as reimbursement for services provided to health plan members, neither entity is acting on behalf of or providing a service to the other.

Similarly, where a physician or other provider has staff privileges at an institution, neither party to the relationship is a business associate based solely on the staff privileges because neither party is providing functions or activities on behalf of the other. However, if a party provides services to or for the other, such as where a hospital provides billing services for physicians with staff privileges, a business associate relationship may arise with respect to those services. Likewise, where a group health plan purchases insurance or coverage from a health insurance issuer or HMO, the provision of insurance by the health insurance issuer or HMO to the group health plan does not make the issuer a business associate. In such case, the activities of the health insurance issuer or HMO are on their own behalf and not on the behalf of the group health plan. We note that where a group health plan contracts with a health insurance issuer or HMO to perform functions or activities or to provide services that are in addition to or not directly related to the provision of insurance, the health insurance issuer or HMO may be a business associate with respect to those additional functions, activities or services. We also note that covered entities are permitted to disclose protected health information to oversight agencies that act to provide oversight of federal programs and the health care system. These oversight agencies are not performing services for or on behalf of the covered entities and so are not business associates of the covered entities. Therefore HCFA, the federal agency that administers Medicare, is not required to enter into a business associate contract in order to disclose protected health information to the Department's Office of Inspector General.

We do not require a covered entity to enter into a business associate contract with a person or organization that acts merely as a conduit for protected health information (*e.g.,* the US Postal Service, certain private couriers and their electronic equivalents). A conduit transports information but does not access it other than on a random or infrequent basis as may be necessary for the performance of the transportation service, or as required by law. Since no disclosure is intended by the covered entity and the probability of exposure of any particular protected health information to a conduit is very small, we do not consider a conduit to be a business associate of the covered entity.

We do not consider a financial institution to be acting on behalf of a covered entity, and therefore no business associate contract is required, when it processes consumer-conducted financial transactions by debit, credit or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care. A typical consumer-conducted payment transaction is when a consumer pays for health care or health insurance premiums using a check or credit card. In these cases the identity of the consumer is always included and some health information (e.g., diagnosis or procedure) may be implied through the name of the health care provider or health plan being paid. Covered entities that initiate such payment activities must meet the minimum necessary disclosure requirements described in the preamble to § 164.514.

Covered Entity

We provided this definition in the NPRM for convenience of reference and proposed it to mean the entities to which part C of title XI of the Act applies. These are the entities described in section 1172(a)(1): Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction referred

to in section 1173(a)(1) of the Act (a ''standard transaction'').

We note that health care providers who do not submit HIPAA transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on their behalf. A provider could not circumvent these requirements by assigning the task to its business associate since the business associate would be considered to be acting on behalf of the provider. See the definition of ''business associate.''

Where a public agency is required or authorized by law to administer a health plan jointly with another entity, we consider each agency to be a covered entity with respect to the health plan functions it performs. Unlike private sector health plans, public plans are often required by or expressly authorized by law to jointly administer health programs that meet the definition of ''health plan'' under this regulation. In some instances the public entity is required or authorized to administer the program with another public agency. In other instances, the public entity is required or authorized to administer the program with a private entity. In either circumstance, we note that joint administration does not meet the definition of ''business associate'' in § 164.501. Examples of joint administration include state and federal administration of the Medicaid and SCHIP program, or joint administration of a Medicare+Choice plan by the Health Care Financing Administration and the issuer offering the plan.

Health Care

We proposed to define ''health care'' to mean the provision of care, services, or supplies to a patient and to include any: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counseling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body; (2) sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; or (3) procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

The final rule revises both the NPRM definition and the definition as provided in the Transactions Rule, to now mean ''care, services, or supplies related to the health of an individual. Health care includes the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

We delete the term ''providing'' from the definition to delineate more clearly the relationship between ''treatment,'' as the term is defined in § 164.501, and ''health care.'' Other key revisions include adding the term ''assessment'' in subparagraph (1) and deleting proposed subparagraph (3) from the rule. Therefore the procurement or banking of organs, blood (including autologous blood), sperm, eyes or any other tissue or human product is not considered to be health care under this rule and the organizations that perform such activities would not be considered health care providers when conducting these functions. As described in § 164.512(h), covered entities are permitted to disclose protected health information without individual authorization, consent, or agreement (see below for explanation of authorizations, consents, and agreements) as necessary to facilitate cadaveric donation.

Health Care Clearinghouse

In the NPRM, we defined ''health care clearinghouse'' as a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. The entity receives health care transactions from health care providers or other entities, translates the data from a given format into one acceptable to the intended payor or payors, and forwards the processed transaction to appropriate payors and clearinghouses. Billing services, repricing companies, community health management information systems, community health information systems, and ''value-added'' networks and switches would have been considered to be health care clearinghouses for purposes of this part, if they perform the functions of health care clearinghouses as described in the preceding sentences.

In the final regulation, we modify the definition of health care clearinghouse to reflect changes in the definition published in the Transactions Rule. The definition in the final rule is:

Health care clearinghouse means a public or private entity, including billing services, repricing companies, community health management information systems or community health information systems, and ''value-added'' networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

We note here that the term health care clearinghouse may have other meanings and connotations in other contexts, but the regulation defines it specifically, and an entity is considered a health care clearinghouse only to the extent that it meets the criteria in this definition. Telecommunications entities that provide connectivity or mechanisms to convey information, such as telephone companies and Internet Service Providers, are not health care clearinghouses as defined in the rule unless they actually carry out the functions outlined in our definition. Value added networks and switches are not health care clearinghouses unless they carry out the functions outlined in the definition. The examples of entities in our proposed definition we continue to consider to be health care clearinghouses, as well as any other entities that meet that definition, to the extent that they perform the functions in the definition.

In order to fall within this definition of clearinghouse, the covered entity must perform the clearinghouse function on health information received from some other entity. A department or component of a health plan or health care provider that transforms nonstandard information into standard data elements or standard transactions (or vice versa) is not a clearinghouse for purposes of this rule, unless it also performs these functions for another entity. As described in more detail in § 164.504(d), we allow affiliates to perform clearinghouse functions for each other without triggering the definition of ''clearinghouse'' if the conditions in § 164.504(d) are met.

Health Care Provider

We proposed to define health care provider to mean a provider of services as defined in section 1861(u) of the Act, a provider of medical or health services as defined in section 1861(s) of the Act, and any other person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business.

In the final rule, we delete the term ''services and supplies,'' in order to eliminate redundancy within the definition. The definition also reflects the addition of the applicable U.S.C. citations (42 U.S.C. 1395x(u) and 42 U.S.C. 1395x(s), respectively) for the referenced provisions of the Act that were promulgated in the Transactions Rule.

To assist the reader, we also provide here excerpts from the relevant sections of the Act. (Refer to the U.S.C. sections cited above for complete definitions in sections 1861(u) and 1861(s).) Section 1861(u) of the Act defines a ''provider of services,'' to include, for example,

a hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or, for purposes of section 1814(g) (42 U.S.C. 1395f(g)) and section 1835(e) (42 U.S.C. 1395n(e)), a fund.'' Section 1861(s) of the Act defines the term, ''medical and other health services,'' and includes a list of covered items or services, as illustrated by the following excerpt:

(s) Medical and other health services. The term ''medical and other health services'' means any of the following items or services:

(1) Physicians' services;

(2) (A) services and supplies * * * furnished as an incident to a physician's professional service, or kinds which are commonly furnished in physicians' offices and are commonly either rendered without charge or included in the physicians' bills;

(B) hospital services * * * incident to physicians' services rendered to outpatients and partial hospitalization services incident to such services;

(C) diagnostic services which are—

(i) furnished to an individual as an outpatient by a hospital or by others under arrangements with them made by a hospital, and

(ii) ordinarily furnished by such hospital (or by others under such arrangements) to its outpatients for the purpose of diagnostic study;

(D) outpatient physical therapy services and outpatient occupational therapy services;

(E) rural health clinic services and federally qualified health center services;

(F) home dialysis supplies and equipment, self-care home dialysis support services, and institutional dialysis services and supplies;

(G) antigens * * * prepared by a physician * * * for a particular patient, including antigens so prepared which are forwarded to another qualified person * * * for administration to such patient, * * * by or under the supervision of another such physician;

(H)(i) services furnished pursuant to a contract under section 1876 (42 U.S.C. 1395mm) to a member of an eligible organization by a physician assistant or by a nurse practitioner * * * and such services and supplies furnished as an incident to his service to such a member * * * and

(ii) services furnished pursuant to a risk-sharing contract under section 1876(g) (42 U.S.C. 1395mm(g)) to a member of an eligible organization by a clinical psychologist * * * or by a clinical social worker * * * (and) furnished as an incident to such clinical psychologist's services or clinical social worker's services * * *;

(I) blood clotting factors, for hemophilia patients * * *;

(J) prescription drugs used in immunosuppressive therapy furnished, to an individual who receives an organ transplant for which payment is made under this title (42 U.S.C. 1395 et seq.), but only in the case of (certain) drugs furnished * * *

(K)(i) services which would be physicians' services if furnished by a physician * * * and which are performed by a physician assistant * * *; and

(ii) services which would be physicians' services if furnished by a physician * * * and which are performed by a nurse * * *;

(L) certified nurse-midwife services;

(M) qualified psychologist services;

(N) clinical social worker services * * *;

(O) erythropoietin for dialysis patients * * *;

(P) prostate cancer screening tests * * *;

(Q) an oral drug (which is approved by the Federal Food and Drug Administration) prescribed for use as an anti-cancer chemotherapeutic agent for a given indication, and containing an active ingredient (or ingredients) * * *;

(R) colorectal cancer screening tests * * *;

(S) diabetes outpatient self-management training services * * *; and

(T) an oral drug (which is approved by the federal Food and Drug Administration) prescribed for use as an acute anti-emetic used as part of an anti-cancer chemotherapeutic regimen * * *

(3) diagnostic X-ray tests * * * furnished in a place of residence used as the patient's home * * * ;

(4) X-ray, radium, and radioactive isotope therapy, including materials and services of technicians;

(5) surgical dressings, and splints, casts, and other devices used for reduction of fractures and dislocations;

(6) durable medical equipment;

(7) ambulance service where the use of other methods of transportation is contraindicated by the individual's condition * * * ;

(8) prosthetic devices (other than dental) which replace all or part of an internal body organ (including colostomy bags and supplies directly related to colostomy care), * * * and including one pair of conventional eyeglasses or contact lenses furnished subsequent to each cataract surgery * * * [;]

(9) leg, arm, back, and neck braces, and artificial legs, arms, and eyes, including replacements if required * * * ;

(10) (A) pneumococcal vaccine and its administration * * *; and

(B) hepatitis B vaccine and its administration * * *, and

(11) services of a certified registered nurse anesthetist * * *;

(12) * * * extra-depth shoes with inserts or custom molded shoes with inserts for an individual with diabetes, if * * *;

(13) screening mammography * * *;

(14) screening pap smear and screening pelvic exam; and

(15) bone mass measurement * * *. (etc.)

Health Plan

We proposed to define ''health plan'' essentially as section 1171(5) of the Act defines it. Section 1171 of the Act refers to several definitions in section 2791 of the Public Health Service Act, 42 U.S.C. 300gg–91, as added by Public Law 104–191.

As defined in section 1171(5), a ''health plan'' is an individual plan or group health plan that provides, or pays the cost of, medical care. We proposed that this definition include, but not be limited to the 15 types of plans (*e.g.,* group health plan, health insurance issuer, health maintenance organization) listed in the statute, as well as any combination of them. Such term would have included, when applied to public benefit programs, the component of the government agency that administers the program. Church plans and government plans would have been included to the extent that they fall into one or more of the listed categories.

In the proposed rule, ''health plan'' included the following, singly or in combination:

(1) A group health plan, defined as an employee welfare benefit plan (as currently defined in section 3(1) of the Employee Retirement Income and Security Act of 1974, 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg–91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance or otherwise, that:

(i) Has 50 or more participants; or

(ii) Is administered by an entity other than the employer that established and maintains the plan.

(2) A health insurance issuer, defined as an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a state and is subject to state or other law that regulates insurance.

(3) A health maintenance organization, defined as a federally qualified health maintenance organization, an organization recognized as a health maintenance organization under state law, or a similar organization regulated for solvency under state law in the same manner and to the same extent as such a health maintenance organization.

(4) Part A or Part B of the Medicare program under title XVIII of the Act.

(5) The Medicaid program under title XIX of the Act.

(6) A Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss).

(7) A long-term care policy, including a nursing home fixed-indemnity policy.

(8) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(9) The health care program for active military personnel under title 10 of the United States Code.

(10) The veterans health care program under 38 U.S.C. chapter 17.

(11) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in 10 U.S.C. 1072(4).

(12) The Indian Health Service program under the Indian Health Care Improvement Act (25 U.S.C. 1601, *et seq.*).

(13) The Federal Employees Health Benefits Program under 5 U.S.C. chapter 89.

(14) An approved state child health plan for child health assistance that meets the requirements of section 2103 of the Act.

(15) A Medicare Plus Choice organization as defined in 42 CFR 422.2, with a contract under 42 CFR part 422, subpart K.

In addition to the 15 specific categories, we proposed that the list include any other individual plan or group health plan, or combination thereof, that provides or pays for the cost of medical care. The Secretary would determine which plans that meet these criteria would to be considered health plans for the purposes of this rule.

Consistent with the other titles of HIPAA, our proposed definition did not include certain types of insurance entities, such as workers' compensation and automobile insurance carriers, other property and casualty insurers, and certain forms of limited benefits coverage, even when such arrangements provide coverage for health care services.

In the final rule, we add two provisions to clarify the types of policies or programs that we do not consider to be a health plan. First, the rule excepts any policy, plan or program to the extent that it provides, or pays for the cost of, excepted benefits, as defined in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1). We note that, while coverage for on-site medical clinics is excluded from definition of ''health plans,'' such clinics may meet the definition of ''health care provider'' and persons who work in the clinic may also meet the definition of health care provider.'' Second, many commenters were confused by the statutory inclusion as a health plan of any ''other individual or group plan that provides or pays the cost of medical care;'' they questioned how the provision applied to many government programs. We therefore clarify that while many government programs (other than the programs specified in the statute) provide or pay the cost of medical care, we do not consider them to be individual or group plans and therefore, do not consider them to be health plans. Government funded programs that do not have as their principal purpose the provision of, or payment for, the cost of health care but which do incidentally provide such services are not health plans (for example, programs such as the Special Supplemental Nutrition Program for Women, Infants and Children (WIC) and the Food Stamp Program, which provide or pay for nutritional services, are not considered to be health plans). Government funded programs that have as their principal purpose the provision of health care, either directly or by grant, are also not considered to be health plans. Examples include the Ryan White Comprehensive AIDS Resources Emergency Act, government funded health centers and immunization programs. We note that some of these may meet the rule's definition of health care provider.

We note that in certain instances eligibility for or enrollment in a health plan that is a government program providing public benefits, such as Medicaid or SCHIP, is determined by an agency other than the agency that administers the program, or individually identifiable health information used to determine enrollment or eligibility in such a health plan is collected by an agency other than the agency that administers the health plan. In these cases, we do not consider an agency that is not otherwise a covered entity, such as a local welfare agency, to be a covered entity because it determines eligibility or enrollment or collects enrollment information as authorized by law. We also do not consider the agency to be a business associate when conducting these functions, as we describe further in the business associate discussion above.

The definition in the final rule also reflects the following changes promulgated in the Transactions Rule:

(1) Exclusion of nursing home fixed-indemnity policies;

(2) Addition of the word ''issuer'' to Medicare supplemental policy, and long-term care policy;

(3) Addition or revision of the relevant statutory cites where appropriate;

(4) Deletion of the term ''or assisted'' when referring to government programs;

(5) Replacement of the word ''organization'' with ''program'' when referring to Medicare + Choice;

(6) Deletion of the term ''health'' when referring to a group plan in subparagraph (xvi);

(7) Extraction of the definitions of ''group health plan,'' ''health insurance issuer,'' and ''health maintenance organization'' into Part 160 as distinct definitions;

(8) In the definition of ''group health plan,'' deletion of the term ''currently'' from the reference to the statutory cite of ERISA, addition of the relevant statutory cite for the term ''participant,'' and addition of the term ''reimbursement;''

(9) In the definition of ''health insurance issuer,'' addition of the relevant statutory cite, deletion of the term ''or other law'' after ''state law,'' addition of health maintenance organizations for consistency with the statute, and clarification that the term does not include a group health plan; and

(10) In the definition of ''health maintenance organization,'' addition of the relevant statutory cite.

Finally, we add to this definition a high risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals. High risk pools are designed mainly to provide health insurance coverage for individuals who, due to health status or pre-existing conditions, cannot obtain insurance through the individual market or who can do so only at very high premiums. Some states use their high risk pool as an alternative mechanism under section 2744 of HIPAA. We do not reference the definition of ''qualified high risk pool'' in HIPAA because that definition includes the requirements for a state to use its risk pool as its alternative mechanism under HIPAA. Some states may have high risk pools, but do not use them as their alternative mechanism and therefore may not meet the definition in HIPAA. We want to make clear that state high risk pools are covered entities under this rule whether or not they meet the definition of a qualified high risk pool under section 2744. High risk pools, as described in this rule, do not include any program established under state law solely to provide excepted benefits. For example, a state program established to provide workers' compensation coverage is not

considered to be a high risk pool under the rule.

Implementation Specification

This definition was adopted in the Transactions Rule and is minimally revised here. We add the words ''requirements or'' before the word ''instructions.'' The word ''instructions'' is appropriate in the context of the implementation specifications adopted in the Transactions Rule, which are generally a series of instructions as to how to use particular electronic forms. However, that word is not apropos in the context of the rules below. In the rules below, the implementation specifications are specific requirements for how to comply with a given standard. The change to this definition thus ties in to this regulatory framework.

Standard

This definition was adopted in the Transactions Rule and we have modified it to make it clearer. We also add language reflecting section 264 of the statute, to clarify that the standards adopted by this rule meet this definition.

State

We modify the definition of state as adopted in the Transactions Rule to clarify that this term refers to any of the several states.

Transaction

We change the term ''exchange'' to the term ''transmission'' in the definition of Transaction to clarify that these transactions may be one-way communications.

Workforce

We proposed in the NPRM to define workforce to mean employees, volunteers, trainees, and other persons under the direct control of a covered entity, including persons providing labor on an unpaid basis.

The definition in the final rule reflects one revision established in the Transactions Rule, which replaces the term ''including persons providing labor on an unpaid basis'' with the term ''whether or not they are paid by the covered entity.'' In addition, we clarify that if the assigned work station of persons under contract is on the covered entity's premises and such persons perform a substantial proportion of their activities at that location, the covered entity may choose to treat them either as business associates or as part of the workforce, as explained in the discussion of the definition of business associate. If there is no business associate contract, we assume the person is a member of the covered entity's workforce. We note that independent contractors may or may not be workforce members. However, for compliance purposes we will assume that such personnel are members of the workforce if no business associate contract exists.

Part 160—Subpart B—Preemption of State Laws

Statutory Background

Section 1178 of the Act establishes a ''general rule'' that state law provisions that are contrary to the provisions or requirements of part C of title XI or the standards or implementation specifications adopted or established thereunder are preempted by the federal requirements. The statute provides three exceptions to this general rule: (1) In section 1178(a)(2)(A)(i), for state laws that the Secretary determines are necessary to prevent fraud and abuse, ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery, and other purposes; (2) in section 1178(a)(2)(A)(ii), for state laws that address controlled substances; and (3) in section 1178(a)(2)(B), for state laws relating to the privacy of individually identifiable health information that as provided for by the related provision of section 264(c)(2) of HIPAA, are contrary to and more stringent than the federal requirements. Section 1178 also carves out, in sections 1178(b) and 1178(c), certain areas of state authority that are not limited or invalidated by the provisions of part C of title XI: these areas relate to public health and state regulation of health plans.

The NPRM proposed a new Subpart B of the proposed part 160. The new Subpart B, which would apply to all standards, implementation specifications, and requirements adopted under HIPAA, would consist of four sections. Proposed § 160.201 provided that the provisions of Subpart B applied to exception determinations and advisory opinions issued by the Secretary under section 1178. Proposed § 160.202 set out proposed definitions for four terms: (1) ''Contrary,'' (2) ''more stringent,'' (3) ''relates to the privacy of individually identifiable health information,'' and (4) ''state law.'' The definition of ''contrary'' was drawn from case law concerning preemption. A seven-part set of specific criteria, drawn from fair information principles, was proposed for the definition of ''more stringent.'' The definition of ''relates to the privacy of individually identifiable health information'' was also based on case law. The definition of ''state law'' was drawn from the statutory definition of this term elsewhere in HIPAA. We note that state action having the force and effect of law may include common law. We eliminate the term ''decision'' from the proposed rule because it is redundant.

Proposed § 160.203 proposed a general rule reflecting the statutory general rule and exceptions that generally mirrored the statutory language of the exceptions. The one substantive addition to the statutory exception language was with respect to the statutory exception, ''for other purposes.'' The following language was added: ''for other purposes related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system.''

Proposed § 160.204 proposed two processes, one for the making of exception determinations, relating to determinations under section 1178(a)(2)(A) of the Act, the other for the rendering of advisory opinions, with respect to section 1178(a)(2)(B) of the Act. The processes proposed were similar in the following respects: (1) Only the state could request an exception determination or advisory opinion, as applicable; (2) both required the request to contain the same information, except that a request for an exception determination also had to set out the length of time the requested exception would be in effect, if less than three years; (3) both sets of requirements provided that requests had to be submitted to the Secretary as required by the Secretary, and until the Secretary's determination was made, the federal standard, requirement or implementation specification remained in effect; (4) both sets of requirements provided that the Secretary's decision would be effective intrastate only; (5) both sets of requirements provided that any change to either the federal or state basis for the Secretary's decision would require a new request, and the federal standard, implementation specification, or requirement would remain in effect until the Secretary acted favorably on the new request; (6) both sets of requirements provided that the Secretary could seek changes to the federal rules or urge states or other organizations to seek changes; and (7) both sets of requirements provided for annual publication of Secretarial decisions. In addition, the process for exception determinations provided for a maximum effective period of three years for such determinations.

The following changes have been made to subpart B in the final rules. First, § 160.201 now expressly

implements section 1178. Second, the definition of ''more stringent'' has been changed by eliminating the criterion relating to penalties and by framing the criterion under paragraph (1) more generally. Also, we have clarified that the term ''individual'' means the person who is the subject of the individually identifiable health information, since the term ''individual'' is defined this way only in subpart E of part 164, not in part 160. Third, the definition of ''state law'' has been changed by substituting the words ''statute, constitutional provision'' for the word ''law,'' the words ''common law'' for the word ''decision,'' and adding the words ''force and'' before the word ''effect'' in the proposed definition. Fourth, in § 160.203, several criteria relating to the statutory grounds for exception determinations have been further spelled out: (1) The words '' related to the provision of or payment for health care'' have been added to the exception for fraud and abuse; (2) the words ''to the extent expressly authorized by statute or regulation'' have been added to the exception for state regulation of health plans; (3) the words ''of serving a compelling need related to public health, safety, or welfare, and, where a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, where the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served'' have been added to the general exception ''for other purposes''; and (4) the statutory provision regarding controlled substances has been elaborated on as follows: ''Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substance, as defined at 21 U.S.C. 802, or which is deemed a controlled substance by state law.''

The most extensive changes have been made to proposed § 160.204. The provision for advisory opinions has been eliminated. Section 160.204 now sets out only a process for requesting exception determinations. In most respects, this process is the same as proposed. However, the proposed restriction of the effect of exception determinations to wholly intrastate transactions has been eliminated. Section 160.204(a) has been modified to allow any person, not just a state, to submit a request for an exception determination, and clarifies that requests from states may be made by the state's chief elected official or his or her designee. Proposed § 160.204(a)(3) stated that if it is determined that the federal standard, requirement, or implementation specification in question meets the exception criteria as well as or better than the state law for which the exception is requested, the request will be denied; this language has been deleted. Thus, the criterion for granting or denying an exception request is whether the applicable exception criterion or criteria are met.

A new § 160.205 is also adopted, replacing part of what was proposed at proposed § 160.204. The new § 160.205 sets out the rules relating to the effectiveness of exception determinations. Exception determinations are effective until either the underlying federal or state laws change or the exception is revoked, by the Secretary, based on a determination that the grounds supporting the exception no longer exist. The proposed maximum of three years has been eliminated.

Relationship to Other Federal Laws

Covered entities subject to these rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act. Thus, covered entities will need to determine how the privacy regulation will affect their ability to comply with these other federal laws.

Many commenters raised questions about how different federal statutes and regulations intersect with the privacy regulation. While we address specific concerns in the response to comments later in the preamble, in this section, we explore some of the general interaction issues. These summaries do not identify all possible conflicts or overlaps of the privacy regulation and other federal laws, but should provide general guidance for complying with both the privacy regulation and other federal laws. The summaries also provide examples of how covered entities can analyze other federal laws when specific questions arise. HHS may consult with other agencies concerning the interpretation of other federal laws as necessary.

Implied Repeal Analysis

When faced with the need to determine how different federal laws interact with one another, we turn to the judiciary's approach. Courts apply the implied repeal analysis to resolve tensions that appear to exist between two or more statutes. While the implication of a regulation-on-regulation conflict is unclear, courts agree that administrative rules and regulations that do not conflict with express statutory provisions have the force and effect of law. Thus, we believe courts would apply the standard rules of interpretation that apply to statutes to address questions of interpretation with regard to regulatory conflicts.

When faced with two potentially conflicting statutes, courts attempt to construe them so that both are given effect. If this construction is not possible, courts will look for express language in the later statute, or an intent in its legislative history, indicating that Congress intended the later statute to repeal the earlier one. If there is no expressed intent to repeal the earlier statute, courts will characterize the statutes as either general or specific. Ordinarily, later, general statutes will not repeal the special provisions of an earlier, specific statute. In some cases, when a later, general statute creates an irreconcilable conflict or is manifestly inconsistent with the earlier, specific statute in a manner that indicates a clear and manifest Congressional intent to repeal the earlier statute, courts will find that the later statute repeals the earlier statute by implication. In these cases, the latest legislative action may prevail and repeal the prior law, but only to the extent of the conflict.

There should be few instances in which conflicts exist between a statute or regulation and the rules below. For example, if a statute permits a covered entity to disclose protected health information and the rules below permit such a disclosure, no conflict arises; the covered entity could comply with both and choose whether or not to disclose the information. In instances in which a potential conflict appears, we would attempt to resolve it so that both laws applied. For example, if a statute or regulation permits dissemination of protected health information, but the rules below prohibit the use or disclosure without an authorization, we believe a covered entity would be able to comply with both because it could obtain an authorization under § 164.508 before disseminating the information under the other law.

Many apparent conflicts will not be true conflicts. For example, if a conflict

appears to exist because a previous statute or regulation requires a specific use or disclosure of protected health information that the rules below appear to prohibit, the use or disclosure pursuant to that statute or regulation would not be a violation of the privacy regulation because § 164.512(a) permits covered entities to use or disclose protected health information as required by law.

If a statute or regulation prohibits dissemination of protected health information, but the privacy regulation requires that an individual have access to that information, the earlier, more specific statute would apply. The interaction between the Clinical Laboratory Improvement Amendments regulation is an example of this type of conflict. From our review of several federal laws, it appears that Congress did not intend for the privacy regulation to overrule existing statutory requirements in these instances.

Examples of Interaction

We have summarized how certain federal laws interact with the privacy regulation to provide specific guidance in areas deserving special attention and to serve as examples of the analysis involved. In the Response to Comment section, we have provided our responses to specific questions raised during the comment period.

The Privacy Act

The Privacy Act of 1974, 5 U.S.C. 552a, prohibits disclosures of records contained in a system of records maintained by a federal agency (or its contractors) without the written request or consent of the individual to whom the record pertains. This general rule is subject to various statutory exceptions. In addition to the disclosures explicitly permitted in the statute, the Privacy Act permits agencies to disclose information for other purposes compatible with the purpose for which the information was collected by identifying the disclosure as a ''routine use'' and publishing notice of it in the **Federal Register**. The Act applies to all federal agencies and certain federal contractors who operate Privacy Act systems of records on behalf of federal agencies.

Some federal agencies and contractors of federal agencies that are covered entities under the privacy rules are subject to the Privacy Act. These entities must comply with all applicable federal statutes and regulations. For example, if the privacy regulation permits a disclosure, but the disclosure is not permitted under the Privacy Act, the federal agency may not make the disclosure. If, however, the Privacy Act allows a federal agency the discretion to make a routine use disclosure, but the privacy regulation prohibits the disclosure, the federal agency will have to apply its discretion in a way that complies with the regulation. This means not making the particular disclosure.

The Freedom of Information Act

FOIA, 5 U.S.C. 552, provides for public disclosure, upon the request of any person, of many types of information in the possession of the federal government, subject to nine exemptions and three exclusions. For example, Exemption 6 permits federal agencies to withhold ''personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.'' 5 U.S.C. 552(b)(6).

Uses and disclosures required by FOIA come within § 164.512(a) of the privacy regulation that permits uses or disclosures required by law if the uses or disclosures meet the relevant requirements of the law. Thus, a federal agency must determine whether it may apply an exemption or exclusion to redact the protected health information when responding to a FOIA request. When a FOIA request asks for documents that include protected health information, we believe the agency, when appropriate, must apply Exemption 6 to preclude the release of medical files or otherwise redact identifying details before disclosing the remaining information.

We offer the following analysis for federal agencies and federal contractors who operate Privacy Act systems of records on behalf of federal agencies and must comply with FOIA and the privacy regulation. If presented with a FOIA request that would result in the disclosure of protected health information, a federal agency must first determine if FOIA requires the disclosure or if an exemption or exclusion would be appropriate. We believe that generally a disclosure of protected health information, when requested under FOIA, would come within FOIA Exemption 6. We recognize, however, that the application of this exemption to information about deceased individuals requires a different analysis than that applicable to living individuals because, as a general rule, under the Privacy Act, privacy rights are extinguished at death. However, under FOIA, it is entirely appropriate to consider the privacy interests of a decedent's survivors under Exemption 6. See Department of Justice FOIA Guide 2000, Exemption 6: Privacy Considerations. Covered entities subject to FOIA must evaluate each disclosure on a case-by-case basis, as they do now under current FOIA procedures.

Federal Substance Abuse Confidentiality Requirements

The federal confidentiality of substance abuse patient records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR part 2, establish confidentiality requirements for patient records that are maintained in connection with the performance of any federally-assisted specialized alcohol or drug abuse program. Substance abuse programs are generally programs or personnel that provide alcohol or drug abuse treatment, diagnosis, or referral for treatment. The term ''federally-assisted'' is broadly defined and includes federally conducted or funded programs, federally licensed or certified programs, and programs that are tax exempt. Certain exceptions apply to information held by the Veterans Administration and the Armed Forces.

There are a number of health care providers that are subject to both these rules and the substance abuse statute and regulations. In most cases, a conflict will not exist between these rules. These privacy rules permit a health care provider to disclose information in a number of situations that are not permitted under the substance abuse regulation. For example, disclosures allowed, without patient authorization, under the privacy rule for law enforcement, judicial and administrative proceedings, public health, health oversight, directory assistance, and as required by other laws would generally be prohibited under the substance abuse statute and regulation. However, because these disclosures are permissive and not mandatory, there is no conflict. An entity would not be in violation of the privacy rules for failing to make these disclosures.

Similarly, provisions in the substance abuse regulation provide for permissive disclosures in case of medical emergencies, to the FDA, for research activities, for audit and evaluation activities, and in response to certain court orders. Because these are permissive disclosures, programs subject to both the privacy rules and the substance abuse rule are able to comply with both rules even if the privacy rules restrict these types of disclosures. In addition, the privacy rules generally require that an individual be given access to his or her own health information. Under the substance abuse

regulation, programs may provide such access, so there is no conflict.

The substance abuse regulation requires notice to patients of the substance abuse confidentiality requirements and provides for written consent for disclosure. While the privacy rules have requirements that are somewhat different, the program may use notice and authorization forms that include all the elements required by both regulations. The substance abuse rule provides a sample notice and a sample authorization form and states that the use of these forms would be sufficient. While these forms do not satisfy all of the requirements of the privacy regulation, there is no conflict because the substance abuse regulation does not mandate the use of these forms.

Employee Retirement Income Security Act of 1974

ERISA was enacted in 1974 to regulate pension and welfare employee benefit plans established by private sector employers, unions, or both, to provide benefits to their workers and dependents. Under ERISA, plans that provide ''through the purchase of insurance or otherwise * * * medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, [or] death'' are defined as employee welfare benefit plans. 29 U.S.C. 1002(1). In 1996, HIPAA amended ERISA to require portability, nondiscrimination, and renewability of health benefits provided by group health plans and group health insurance issuers. Numerous, although not all, ERISA plans are covered under the rules proposed below as ''health plans.''

Section 514(a) of ERISA, 29 U.S.C. 1144(a), preempts all state laws that ''relate to'' any employee benefit plan. However, section 514(b) of ERISA, 29 U.S.C. 1144(b)(2)(A), expressly saves from preemption state laws that regulate insurance. Section 514(b)(2)(B) of ERISA, 29 U.S.C. 1144(b)(2)(B), provides that an ERISA plan is deemed not to be an insurer for the purpose of regulating the plan under the state insurance laws. Thus, under the deemer clause, states may not treat ERISA plans as insurers subject to direct regulation by state law. Finally, section 514(d) of ERISA, 29 U.S.C. 1144(d), provides that ERISA does not ''alter, amend, modify, invalidate, impair, or supersede any law of the United States.''

We considered whether the preemption provision of section 264(c)(2) of HIPAA would give effect to state laws that would otherwise be preempted by section 514(a) of ERISA. As discussed above, our reading of the statutes together is that the effect of section 264(c)(2) is only to leave in place state privacy protections that would otherwise apply and that are more stringent than the federal privacy protections.

Many health plans covered by the privacy regulation are also subject to ERISA requirements. Our discussions and consultations have not uncovered any particular ERISA requirements that would conflict with the rules.

The Family Educational Rights and Privacy Act

FERPA, as amended, 20 U.S.C. 1232g, provides parents of students and eligible students (students who are 18 or older) with privacy protections and rights for the records of students maintained by federally funded educational agencies or institutions or persons acting for these agencies or institutions. We have excluded education records covered by FERPA, including those education records designated as education records under Parts B, C, and D of the Individuals with Disabilities Education Act Amendments of 1997, from the definition of protected health information. For example, individually identifiable health information of students under the age of 18 created by a nurse in a primary or secondary school that receives federal funds and that is subject to FERPA is an education record, but not protected health information. Therefore, the privacy regulation does not apply. We followed this course because Congress specifically addressed how information in education records should be protected in FERPA.

We have also excluded certain records, those described at 20 U.S.C. 1232g(a)(4)(B)(iv), from the definition of protected health information because FERPA also provided a specific structure for the maintenance of these records. These are records (1) of students who are 18 years or older or are attending post-secondary educational institutions, (2) maintained by a physician, psychiatrist, psychologist, or recognized professional or paraprofessional acting or assisting in that capacity, (3) that are made, maintained, or used only in connection with the provision of treatment to the student, and (4) that are not available to anyone, except a physician or appropriate professional reviewing the record as designated by the student. Because FERPA excludes these records from its protections only to the extent they are not available to anyone other than persons providing treatment to students, any use or disclosure of the record for other purposes, including providing access to the individual student who is the subject of the information, would turn the record into an education record. As education records, they would be subject to the protections of FERPA.

These exclusions are not applicable to all schools, however. If a school does not receive federal funds, it is not an educational agency or institution as defined by FERPA. Therefore, its records that contain individually identifiable health information are not education records. These records may be protected health information. The educational institution or agency that employs a school nurse is subject to our regulation as a health care provider if the school nurse or the school engages in a HIPAA transaction.

While we strongly believe every individual should have the same level of privacy protection for his/her individually identifiable health information, Congress did not provide us with authority to disturb the scheme it had devised for records maintained by educational institutions and agencies under FERPA. We do not believe Congress intended to amend or preempt FERPA when it enacted HIPAA.

With regard to the records described at 20 U.S.C. 1232g(a)(4)(b)(iv), we considered requiring health care providers engaged in HIPAA transactions to comply with the privacy regulation up to the point these records were used or disclosed for purposes other than treatment. At that point, the records would be converted from protected health information into education records. This conversion would occur any time a student sought to exercise his/her access rights. The provider, then, would need to treat the record in accordance with FERPA's requirements and be relieved from its obligations under the privacy regulation. We chose not to adopt this approach because it would be unduly burdensome to require providers to comply with two different, yet similar, sets of regulations and inconsistent with the policy in FERPA that these records be exempt from regulation to the extent the records were used only to treat the student.

Gramm-Leach-Bliley

In 1999, Congress passed Gramm-Leach-Bliley (GLB), Pub. L. 106–102, which included provisions, section 501 *et seq.*, that limit the ability of financial institutions to disclose ''nonpublic personal information'' about consumers to non-affiliated third parties and require financial institutions to provide customers with their privacy policies and practices with respect to nonpublic

personal information. In addition, Congress required seven agencies with jurisdiction over financial institutions to promulgate regulations as necessary to implement these provisions. GLB and its accompanying regulations define ''financial institutions'' as including institutions engaged in the financial activities of bank holding companies, which may include the business of insuring. See 15 U.S.C. 6809(3); 12 U.S.C. 1843(k). However, Congress did not provide the designated federal agencies with the authority to regulate health insurers. Instead, it provided states with an incentive to adopt and have their state insurance authorities enforce these rules. See 15 U.S.C. 6805. If a state were to adopt laws consistent with GLB, health insurers would have to determine how to comply with both sets of rules.

Thus, GLB has caused concern and confusion among health plans that are subject to our privacy regulation. Although Congress remained silent as to its understanding of the interaction of GLB and HIPAA's privacy provisions, the Federal Trade Commission and other agencies implementing the GLB privacy provisions noted in the preamble to their GLB regulations that they ''would consult with HHS to avoid the imposition of duplicative or inconsistent requirements.'' 65 Fed. Reg. 33646, 33648 (2000). Additionally, the FTC also noted that ''persons engaged in providing insurance'' would be within the enforcement jurisdiction of state insurance authorities and not within the jurisdiction of the FTC. *Id.*

Because the FTC has clearly stated that it will not enforce the GLB privacy provisions against persons engaged in providing insurance, health plans will not be subject to dual federal agency jurisdiction for information that is both nonpublic personal information and protected health information. If states choose to adopt GLB-like laws or regulations, which may or may not track the federal rules completely, health plans would need to evaluate these laws under the preemption analysis described in subpart B of Part 160.

Federally Funded Health Programs

These rules will affect various federal programs, some of which may have requirements that are, or appear to be, inconsistent with the requirements of these regulations. These programs include those operated directly by the federal government (such as health programs for military personnel and veterans) as well as programs in which health services or benefits are provided by the private sector or by state or local governments, but which are governed by various federal laws (such as Medicare, Medicaid, and ERISA).

Congress explicitly included some of these programs in HIPAA, subjecting them directly to the privacy regulation. Section 1171 of the Act defines the term ''health plan'' to include the following federally conducted, regulated, or funded programs: Group plans under ERISA that either have 50 or more participants or are administered by an entity other than the employer who established and maintains the plan; federally qualified health maintenance organizations; Medicare; Medicaid; Medicare supplemental policies; the health care program for active military personnel; the health care program for veterans; the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); the Indian health service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*; and the Federal Employees Health Benefits Program. There also are many other federally conducted, regulated, or funded programs in which individually identifiable health information is created or maintained, but which do not come within the statutory definition of ''health plan.'' While these latter types of federally conducted, regulated, or assisted programs are not explicitly covered by part C of title XI in the same way that the programs listed in the statutory definition of ''health plan'' are covered, the statute may nonetheless apply to transactions and other activities conducted under such programs. This is likely to be the case when the federal entity or federally regulated or funded entity provides health services; the requirements of part C may apply to such an entity as a ''health care provider.'' Thus, the issue of how different federal requirements apply is likely to arise in numerous contexts.

There are a number of authorities under the Public Health Service Act and other legislation that contain explicit confidentiality requirements, either in the enabling legislation or in the implementing regulations. Many of these are so general that there would appear to be no problem of inconsistency, in that nothing in those laws or regulations would appear to restrict the provider's ability to comply with the privacy regulation's requirements.

There may, however, be authorities under which either the requirements of the enabling legislation or of the program regulations would impose requirements that differ from these rules.

For example, regulations applicable to the substance abuse block grant program funded under section 1943(b) of the Public Health Service Act require compliance with 42 CFR part 2, and, thus, raise the issues identified above in the substance abuse confidentiality regulations discussion. There are a number of federal programs which, either by statute or by regulation, restrict the disclosure of patient information to, with minor exceptions, disclosures ''required by law.'' See, for example, the program of projects for prevention and control of sexually transmitted diseases funded under section 318(e)(5) of the Public Health Service Act (42 CFR 51b.404); the regulations implementing the community health center program funded under section 330 of the Public Health Service Act (42 CFR 51c.110); the regulations implementing the program of grants for family planning services under title X of the Public Health Service Act (42 CFR 59.15); the regulations implementing the program of grants for black lung clinics funded under 30 U.S.C. 437(a) (42 CFR 55a.104); the regulations implementing the program of maternal and child health projects funded under section 501 of the Act (42 CFR 51a.6); the regulations implementing the program of medical examinations of coal miners (42 CFR 37.80(a)). These legal requirements would restrict the grantees or other entities providing services under the programs involved from making many of the disclosures that §§ 164.510 or 164.512 would permit. In some cases, permissive disclosures for treatment, payment, or health care operations would also be limited. Because §§ 164.510 and 164.512 are merely permissive, there would not be a conflict between the program requirements, because it would be possible to comply with both. However, entities subject to both sets of requirements would not have the total range of discretion that they would have if they were subject only to this regulation.

Food, Drug, and Cosmetic Act

The Food, Drug, and Cosmetic Act, 21 U.S.C. 301, *et seq.*, and its accompanying regulations outline the responsibilities of the Food and Drug Administration with regard to monitoring the safety and effectiveness of drugs and devices. Part of the agency's responsibility is to obtain reports about adverse events, track medical devices, and engage in other types of post marketing surveillance. Because many of these reports contain protected health information, the information within them may come within the purview of the privacy rules.

Although some of these reports are required by the Food, Drug, and Cosmetic Act or its accompanying regulations, other types of reporting are voluntary. We believe that these reports, while not mandated, play a critical role in ensuring that individuals receive safe and effective drugs and devices. Therefore, in § 164.512(b)(1)(iii), we have provided that covered entities may disclose protected health information to a person subject to the jurisdiction of the Food and Drug Administration for specified purposes, such as reporting adverse events, tracking medical devices, or engaging in other post marketing surveillance. We describe the scope and conditions of such disclosures in more detail in § 164.512(b).

Clinical Laboratory Improvement Amendments

CLIA, 42 U.S.C. 263a, and the accompanying regulations, 42 CFR part 493, require clinical laboratories to comply with standards regarding the testing of human specimens. This law requires clinical laboratories to disclose test results or reports only to authorized persons, as defined by state law. If a state does not define the term, the federal law defines it as the person who orders the test.

We realize that the person ordering the test is most likely a health care provider and not the individual who is the subject of the protected health information included within the result or report. Under this requirement, therefore, a clinical laboratory may be prohibited by law from providing the individual who is the subject of the test result or report with access to this information.

Although we believe individuals should be able to have access to their individually identifiable health information, we recognize that in the specific area of clinical laboratory testing and reporting, the Health Care Financing Administration, through regulation, has provided that access may be more limited. To accommodate this requirement, we have provided at § 164.524(1)(iii) that covered entities maintaining protected health information that is subject to the CLIA requirements do not have to provide individuals with a right of access to or a right to inspect and obtain a copy of this information if the disclosure of the information to the individual would be prohibited by CLIA.

Not all clinical laboratories, however, will be exempted from providing individuals with these rights. If a clinical laboratory operates in a state in which the term ''authorized person'' is defined to include the individual, the clinical laboratory would have to provide the individual with these rights. Similarly, if the individual was the person who ordered the test and an authorized person included such a person, the laboratory would be required to provide the individual with these rights.

Additionally, CLIA regulations exempt the components or functions of ''research laboratories that test human specimens but do not report patient specific results for the diagnosis, prevention or treatment of any disease or impairment of, or the assessment of the health of individual patients'' from the CLIA regulatory scheme. 42 CFR 493.3(a)(2). If subject to the access requirements of this regulation, such entities would be forced to meet the requirements of CLIA from which they are currently exempt. To eliminate this additional regulatory burden, we have also excluded covered entities that are exempt from CLIA under that rule from the access requirement of this regulation.

Although we are concerned about the lack of immediate access by the individual, we believe that, in most cases, individuals who receive clinical tests will be able to receive their test results or reports through the health care provider who ordered the test for them. The provider will receive the information from the clinical laboratory. Assuming that the provider is a covered entity, the individual will have the right of access and right to inspect and copy this protected health information through his or her provider.

Other Mandatory Federal or State Laws

Many federal laws require covered entities to provide specific information to specific entities in specific circumstances. If a federal law requires a covered entity to disclose a specific type of information, the covered entity would not need an authorization under § 164.508 to make the disclosure because the final rule permits covered entities to make disclosures that are required by law under § 164.512(a). Other laws, such as the Social Security Act (including its Medicare and Medicaid provisions), the Family and Medical Leave Act, the Public Health Service Act, Department of Transportation regulations, the Environmental Protection Act and its accompanying regulations, the National Labor Relations Act, the Federal Aviation Administration, and the Federal Highway Administration rules, may also contain provisions that require covered entities or others to use or disclose protected health information for specific purposes.

When a covered entity is faced with a question as to whether the privacy regulation would prohibit the disclosure of protected health information that it seeks to disclose pursuant to a federal law, the covered entity should determine if the disclosure is required by that law. In other words, it must determine if the disclosure is mandatory rather than merely permissible. If it is mandatory, a covered entity may disclose the protected health information pursuant to § 164.512(a), which permits covered entities to disclose protected health information without an authorization when the disclosure is required by law. If the disclosure is not required (but only permitted) by the federal law, the covered entity must determine if the disclosure comes within one of the other permissible disclosures. If the disclosure does not come within one of the provisions for permissible disclosures, the covered entity must obtain an authorization from the individual who is the subject of the information or de-identify the information before disclosing it.

If another federal law prohibits a covered entity from using or disclosing information that is also protected health information, but the privacy regulation permits the use or disclosure, a covered entity will need to comply with the other federal law and not use or disclose the information.

Federal Disability Nondiscrimination Laws

The federal laws barring discrimination on the basis of disability protect the confidentiality of certain medical information. The information protected by these laws falls within the larger definition of ''health information'' under this privacy regulation. The two primary disability nondiscrimination laws are the Americans with Disabilities Act (ADA), 42 U.S.C. 12101 *et seq.*, and the Rehabilitation Act of 1973, as amended, 29 U.S.C. 701 *et seq.*, although other laws barring discrimination on the basis of disability (such as the nondiscrimination provisions of the Workforce Investment Act of 1988, 29 U.S.C. 2938) may also apply. Federal disability nondiscrimination laws cover two general categories of entities relevant to this discussion: employers and entities that receive federal financial assistance.

Employers are not covered entities under the privacy regulation. Many employers, however, are subject to the federal disability nondiscrimination laws and, therefore, must protect the

confidentiality of all medical information concerning their applicants and employees.

The employment provisions of the ADA, 42 U.S.C. 12111 *et seq.*, expressly cover employers of 15 or more employees, employment agencies, labor organizations, and joint labor-management committees. Since 1992, employment discrimination complaints arising under sections 501, 503, and 504 of the Rehabilitation Act also have been subject to the ADA's employment nondiscrimination standards. See ''Rehabilitation Act Amendments,'' Pub. L. No. 102–569, 106 Stat. 4344. Employers subject to ADA nondiscrimination standards have confidentiality obligations regarding applicant and employee medical information. Employers must treat such medical information, including medical information from voluntary health or wellness programs and any medical information that is voluntarily disclosed as a confidential medical record, subject to limited exceptions.

Transmission of health information by an employer to a covered entity, such as a group health plan, is governed by the ADA confidentiality restrictions. The ADA, however, has been interpreted to permit an employer to use medical information for insurance purposes. See 29 CFR part 1630 App. at § 1630.14(b) (describing such use with reference to 29 CFR 1630.16(f), which in turn explains that the ADA regulation ''is not intended to disrupt the current regulatory structure for self-insured employers * * * or current industry practices in sales, underwriting, pricing, administrative and other services, claims and similar insurance related activities based on classification of risks as regulated by the states''). See also, ''Enforcement Guidance on Disability-Related Inquiries and Medical Examinations of Employees under the Americans with Disabilities Act,'' 4, n.10 (July 26, 2000), FEP Manual (BNA) (''Enforcement Guidance on Employees''). See generally, ''ADA Enforcement Guidance on Preemployment Disability-Related Questions and Medical Examinations'' (October 10, 1995), 8 FEP Manual (BNA) 405:7191 (1995) (also available at *http://www.eeoc.gov*). Thus, use of medical information for insurance purposes may include transmission of health information to a covered entity.

If an employer-sponsored group health plan is closely linked to an employer, the group health plan may be subject to ADA confidentiality restrictions, as well as this privacy regulation. *See Carparts Distribution Center, Inc.* v. *Automotive Wholesaler's Association of New England, Inc.,* 37 F.3d 12 (1st Cir. 1994)(setting forth three bases for ADA Title I jurisdiction over an employer-provided medical reimbursement plan, in a discrimination challenge to the plan's HIV/AIDS cap). Transmission of applicant or employee health information by the employer's management to the group health plan may be permitted under the ADA standards as the use of medical information for insurance purposes. Similarly, disclosure of such medical information by the group health plan, under the limited circumstances permitted by this privacy regulation, may involve use of the information for insurance purposes as broadly described in the ADA discussion above.

Entities that receive federal financial assistance, which may also be covered entities under the privacy regulation, are subject to section 504 of the Rehabilitation Act (29 U.S.C. 794) and its implementing regulations. Each federal agency has promulgated such regulations that apply to entities that receive financial assistance from that agency (''recipients''). These regulations may limit the disclosure of medical information about persons who apply to or participate in a federal financially assisted program or activity. For example, the Department of Labor's section 504 regulation (found at 29 CFR part 32), consistent with the ADA standards, requires recipients that conduct employment-related programs, including employment training programs, to maintain confidentiality regarding any information about the medical condition or history of applicants to or participants in the program or activity. Such information must be kept separate from other information about the applicant or participant and may be provided to certain specified individuals and entities, but only under certain limited circumstances described in the regulation. See 29 CFR 32.15(d). Apart from those circumstances, the information must be afforded the same confidential treatment as medical records, *id.* Also, recipients of federal financial assistance from the Department of Health and Human Services, such as hospitals, are subject to the ADA's employment nondiscrimination standards. They must, accordingly, maintain confidentiality regarding the medical condition or history of applicants for employment and employees.

The statutes and implementing regulations under which the federal financial assistance is provided may contain additional provisions regulating collection and disclosure of medical, health, and disability-related information. See, *e.g.,* section 188 of the Workforce Investment Act of 1988 (29 U.S.C. 2938) and 29 CFR 37.3(b). Thus, covered entities that are subject to this privacy regulation, may also be subject to the restrictions in these laws as well.

U.S. Safe Harbor Privacy Principles (European Union Directive on Data Protection)

The E.U. Directive became effective in October 1998 and prohibits European Union Countries from permitting the transfer of personal data to another country without ensuring that an ''adequate level of protection,'' as determined by the European Commission, exists in the other country or pursuant to one of the Directive's derogations of this rule, such as pursuant to unambiguous consent or to fulfill a contract with the individual. In July 2000, the European Commission concluded that the U.S. Safe Harbor Privacy Principles [1] constituted ''adequate protection.'' Adherence to the Principles is voluntary. Organizations wishing to engage in the exchange of personal data with E.U. countries may assert compliance with the Principles as one means of obtaining data from E.U. countries.

The Department of Commerce, which negotiated these Principles with the European Commission, has provided guidance for U.S. organizations seeking to adhere to the guidelines and comply with U.S. law. We believe this guidance addresses the concerns covered entities seeking to transfer personal data from E.U. countries may have. When ''U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law.'' An organization does not need to comply with the Principles if a conflicting U.S. law ''explicitly authorizes'' the particular conduct. The organization's non-compliance is ''limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorization.'' However, if only a difference exists such that an ''option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.'' Questions regarding compliance and interpretation will be decided based on U.S. law. See Department of Commerce, Memorandum on Damages for Breaches

[1] The Principles are: (1) Notice; (2) Choice (*i.e.,* consent); (3) Onward Transfer (i.e., subsequent disclosures); (4) Security; (5) Data Integrity; (6) Access; and (7) Enforcement. Department of Commerce, Safe Harbor Principles, July 21, 2000 (''Principles''). They do not apply to manually processed data.

of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law 5 (July 17, 2000); Department of Commerce, Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000, 65 FR 45666 (2000). The Principles and our privacy regulation are based on common principles of fair information practices. We believe they are essentially consistent and that an organization complying with our privacy regulation can fairly and correctly self-certify that it complies with the Principles. If a true conflict arises between the privacy regulation and the Principles, the Department of Commerce's guidance provides that an entity must comply with the U.S. law.

Part 160—Subpart C—Compliance and Enforcement

Proposed § 164.522 included five paragraphs addressing activities related to the Secretary's enforcement of the rule. These provisions were based on procedures and requirements in various civil rights regulations. Proposed § 164.522(a) provided that the Secretary would, to the extent practicable, seek the cooperation of covered entities in obtaining compliance, and could provide technical assistance to covered entities to help them comply voluntarily. Proposed § 164.522(b) provided that individuals could file complaints with the Secretary. However, where the complaint related to the alleged failure of a covered entity to amend or correct protected health information as proposed in the rule, the Secretary would not make certain determinations such as whether protected health information was accurate or complete. This paragraph also listed the requirements for filing complaints and indicated that the Secretary may investigate such complaints and what might be reviewed as part of such investigation.

Under proposed § 164.522(c), the Secretary would be able to conduct compliance reviews. Proposed § 164.522(d) described the responsibilities that covered entities keep records and reports as prescribed by the Secretary, cooperate with compliance reviews, permit the Secretary to have access to their facilities, books, records, and other sources of information during normal business hours, and seek records held by other persons. This paragraph also stated that the Secretary would maintain the confidentiality of protected health information she collected and prohibit covered entities from taking retaliatory action against individuals for filing complaints or for other activities. Proposed § 164.522(e) provided that the Secretary would inform the covered entity and the individual complainant if an investigation or review indicated a failure to comply and would seek to resolve the matter informally if possible. If the matter could not be resolved informally, the Secretary would be able to issue written findings, be required to inform the covered entity and the complainant, and be able to pursue civil enforcement action or make a criminal referral. The Secretary would also be required to inform the covered entity and the individual complainant if no violation was found.

We make the following changes and additions to proposed § 164.522 in the final rule. First, we have moved this section to part 160, as a new subpart C, ''Compliance and Enforcement.'' Second, we add new sections that explain the applicability of these provisions and incorporate certain definitions. Accordingly, we change the proposed references to violations to ''this subpart'' to violations of ''the applicable requirements of part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.'' Third, the final rule at § 160.306(a) provides that any person, not just an ''individual'' (the person who is the subject of the individually identifiable health information) may file a complaint with the Secretary. Other references in this subpart to an individual have been changed accordingly. Fourth, we delete the proposed § 164.522(a) language that indicated that the Secretary would not determine whether information was accurate or complete, or whether errors or omissions might have an adverse effect on the individual. While the policy is not changed in that the Secretary will not make such determinations, we believe the language is unnecessary and may suggest that we would make all other types of determinations, such as all determinations in which the regulation defers to the professional judgment of the covered entity. Fifth, § 160.306(b)(3) requires that complaints be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown. Sixth, § 160.310(b) requires cooperation with investigations as well as compliance reviews. Seventh, § 160.310 (c)(1) provides that the Secretary must be provided access to a covered entity's facilities, books, records, accounts, and other sources of information, including protected health information, at any time and without notice where exigent circumstances exist, such as where documents might be hidden or destroyed. Eighth, the provision proposed at § 164.522(d) that would prohibit covered entities from taking retaliatory action against individuals for filing a complaint with the Secretary or for certain other actions has been changed and moved to § 164.530. Ninth, § 160. 312(a)(2) deletes the reference in the proposed rule to using violation findings as a basis for initiating action to secure penalties. This deletion is not a substantive change. This language was removed because penalties will be addressed in the enforcement regulation. As in the NPRM, the Secretary may promulgate alternative procedures for complaints relating to national security. For example, to protect classified information, we may promulgate rules that would allow an intelligence community agency to create a separate body within that agency to receive complaints.

The Department plans to issue an Enforcement Rule that applies to all of the regulations that the Department issues under the Administrative Simplification provisions of HIPAA. This regulation will address the imposition of civil monetary penalties and the referral of criminal cases where there has been a violation of this rule. Penalties are provided for under section 262 of HIPAA. The Enforcement Rule would also address the topics covered by Subpart C below. It is expected that this Enforcement Rule would replace Subpart C.

Part 164—Subpart A—General Provisions

Section 164.102—Statutory Basis

In the NPRM, we provided that the provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation standards under part C of title XI of the Act and section 264 of Public Law 104–191. The final rule adopts this language.

Section 164.104—Applicability

In the NPRM, we provided that except as otherwise provided, the provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care providers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of the Act. The final rule adopts this language.

Section 164.106—Relationship to Other Parts

The final rule adds a new provision stating that in complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter. This language references Subchapter C in this regulation, Administrative Data Standards and Related Requirements; Part 160, General Administrative Requirements; and Part 162, Administrative Requirements. Part 160 includes requirements such as keeping records and submitting compliance reports to the Secretary and cooperating with the Secretary's complaint investigations and compliance reviews. Part 162 includes requirements such as requiring a covered entity that conducts an electronic transaction, adopted under this part, with another covered entity to conduct the transaction as a standard transaction as adopted by the Secretary.

Part 164—Subpart B–D—Reserved

Part 164—Subpart E—Privacy

Section 164.500—Applicability

The discussion below describes the entities and the information that are subject to the final regulation.

Many of the provisions of the regulation are presented as ''standards.'' Generally, the standards indicate what must be accomplished under the regulation and implementation specifications describe how the standards must be achieved.

Covered Entities

We proposed in the NPRM to apply the standards in the regulation to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions referred to in section 1173(a)(1) of the Act. The proposal referred to these entities as ''covered entities.''

We have revised § 164.500 to clarify the applicability of the rule to health care clearinghouses. As we stated in the preamble to the NPRM, we believe that in most instances health care clearinghouses will receive protected health information as a business associate to another covered entity. This understanding was confirmed by the comments and by our fact finding. Clearinghouses rarely have direct contact with individuals, and usually will not be in a position to create protected health information or to receive it directly from them. Unlike health plans and providers, clearinghouses usually convey and repackage information and do not add materially to the substance of protected health information of an individual.

The revised language provides that clearinghouses are not subject to certain requirements in the rule when acting as business associates of other covered entities. As revised, a clearinghouse acting as a business associate is subject only to the provisions of this section, to the definitions, to the general rules for uses and disclosures of protected health information (subject to limitations), to the provision relating to health care components, to the provisions relating to uses and disclosures for which consent, individual authorization or an opportunity to agree or object is not required (subject to limitations), to the transition requirements and to the compliance date. With respect to the uses and disclosures authorized under § 164.502 or § 164.512, a clearinghouse acting as a business associate is not authorized by the rule to make any use or disclosure not permitted by its business associate contract. Clearinghouses acting as business associates are not subject to the other requirements of this rule, which include the provisions relating to procedural requirements, requirements for obtaining consent, individual authorization or agreement, provision of a notice, individual rights to request privacy protection, access and amend information and receive an accounting of disclosures and the administrative requirements.

We note that, even as business associates, clearinghouses remain covered entities. Clearinghouses, like other covered entities, are responsible under this regulation for abiding by the terms of business associate contracts. For example, while the provisions regarding individuals' access to and right to request corrections to protected health information about them apply only to health plans and covered health care providers, clearinghouses may have some responsibility for providing such access under their business associate contracts. A clearinghouse (or any other covered entity) that violates the terms of a business associate contract also is in direct violation of this rule and, as a covered entity, is subject to compliance and enforcement action.

We clarify that a covered entity is only subject to these rules to the extent that they possess protected health information. Moreover, these rules only apply with regard to protected health information. For example, if a covered entity does not disclose or receive from its business associate any protected health information and no protected health information is created or received by its business associate on behalf of the covered entity, then the business associate requirements of this rule do not apply.

We clarify that the Department of Defense or any other federal agency and any non-governmental organization acting on its behalf, is not subject to this rule when it provides health care in another country to foreign national beneficiaries. The Secretary believes that this exemption is warranted because application of the rule could have the unintended effect of impeding or frustrating the conduct of such activities, such as interfering with the ability of military command authorities to obtain protected health information on prisoners of war, refugees, or detainees for whom they are responsible under international law. See the preamble to the definition of ''individual'' for further discussion.

Covered Information

We proposed in the NPRM to apply the requirements of the rule to individually identifiable health information that is or has been electronically transmitted or maintained by a covered entity. The provisions would have applied to the information itself, referred to as protected health information in the rule, and not to the particular records in which the information is contained. We proposed that once information was maintained or transmitted electronically by a covered entity, the protections would follow the information in whatever form, including paper records, in which it exists while held by a covered entity. The proposal would not have applied to information that was never electronically maintained or transmitted by a covered entity.

In the final rule, we extend the scope of protections to all individually identifiable health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity. This includes individually identifiable health information in paper records that never has been electronically stored or transmitted. (See § 164.501, definition of ''protected health information,'' for further discussion.)

Section 164.501—Definitions

Correctional Institution

The proposed rule did not define the term correctional institution. The final rule defines correctional institution as any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States,

a state, a territory, a political subdivision of a state or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. This language was necessary to explain the privacy rights and protections of inmates in this regulation.

Covered Functions

We add a new term, ''covered functions,'' as a shorthand way of expressing and referring to the functions that the entities covered by section 1172(a) of the Act perform. Section 1171 defines the terms ''health plan'', ''health care provider'', and ''health care clearinghouse'' in functional terms. Thus, a ''health plan'' is an individual or group plan ''that provides, or pays the cost of, medical care * * *'', a ''health care provider'' ''furnish[es] health care services or supplies,'' and a ''health care clearinghouse'' is an entity ''that processes or facilitates the processing of * * * data elements of health information * * *''. Covered functions, therefore, are the activities that any such entity engages in that are directly related to operating as a health plan, health care provider, or health care clearinghouse; that is, they are the functions that make it a health plan, health care provider, or health care clearinghouse.

The term ''covered functions'' is not intended to include various support functions, such as computer support, payroll and other office support, and similar support functions, although we recognize that these support functions must occur in order for the entity to carry out its health care functions. Because such support functions are often also performed for parts of an organization that are not doing functions directly related to the health care functions and may involve access to and/or use of protected health information, the rules below describe requirements for ensuring that workforce members who perform these support functions do not impermissibly use or disclose protected health information. See § 164.504.

Data Aggregation

The NPRM did not include a definition of data aggregation. In the final rule, data aggregation is defined, with respect to protected health information received by a business associate in its capacity as the business associate of a covered entity, as the combining of such protected health information by the business associate with protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit the creation of data for analyses that relate to the health care operations of the respective covered entities. The definition is included in the final rule to help describe how business associates can assist covered entities to perform health care operations that involve comparative analysis of protected health information from otherwise unaffiliated covered entities. Data aggregation is a service that gives rise to a business associate relationship if the performance of the service involves disclosure of protected health information by the covered entity to the business associate.

Designated Record Set

In the proposed rule, we defined designated record set as ''a group of records under the control of a covered entity from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual and which is used by the covered entity to make decisions about the individual.'' We defined a ''record'' as ''any item, collection, or grouping of protected health information maintained, collected, used, or disseminated by a covered entity.''

In the final rule, we modify the definition of designated record set to specify certain records maintained by or for a covered entity that are always part of a covered entity's designated record sets and to include other records that are used to make decisions about individuals. We do not use the means of retrieval of a record as a defining criteria.

For health plans, designated record sets include, at a minimum, the enrollment, payment, claims adjudication, and case or medical management record systems of the plan. For covered health care providers, designated record sets include, at a minimum, the medical record and billing record about individuals maintained by or for the provider. In addition to these records, designated record sets include any other group of records that are used, in whole or in part, by or for a covered entity to make decisions about individuals. We note that records that otherwise meet the definition of designated record set and which are held by a business associate of the covered entity are part of the covered entity's designated record sets. Although we do not specify particular types of records that are always included in the designated record sets of clearinghouses when they are not acting as business associates, this definition includes a group of records that such a clearinghouse uses, in whole or in part, to make decisions about individuals.

For the most part we retain, with slight modifications, the definition of ''record,'' defining it as any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated.

Direct Treatment Relationship

This term was not included in the proposed rule. Direct treatment relationship means a relationship between a health care provider and an individual that is not an indirect treatment relationship (see definition of indirect treatment relationship, below). For example, outpatient pharmacists and Web-based providers generally have direct treatment relationships with patients. Outpatient pharmacists fill prescriptions written by other providers, but they furnish the prescription and advice about the prescription directly to the patient, not through another treating provider. Web-based providers generally deliver health care independently, without the orders of another provider.

A provider may have direct treatment relationships with some patients and indirect treatment relationships with others. In some provisions of the final rule, providers with indirect treatment relationships are excepted from requirements that apply to other providers. See § 164.506 regarding consent for uses and disclosures of protected health information for treatment, payment, and health care operations, and § 164.520 regarding notice of information practices. These exceptions apply only with respect to the individuals with whom the provider has an indirect treatment relationship.

Disclosure

We proposed to define ''disclosure'' to mean the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. The final rule is unchanged. We note that the transfer of protected health information from a covered entity to a business associate is a disclosure for purposes of this regulation.

Health Care Operations

The preamble to the proposed rule explained that in order for treatment and payment to occur, protected health

information must be used within entities and shared with business partners. In the proposed rule we provided a definition for ''health care operations'' to clarify the activities we considered to be ''compatible with and directly related to'' treatment and payment and for which protected health information could be used or disclosed without individual authorization. These activities included conducting quality assessment and improvement activities, reviewing the competence or qualifications and accrediting/licensing of health care professionals and plans, evaluating health care professional and health plan performance, training future health care professionals, insurance activities relating to the renewal of a contract for insurance, conducting or arranging for medical review and auditing services, and compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding. Recognizing the dynamic nature of the health care industry, we acknowledged that the specified categories may need to be modified as the industry evolves.

The preamble discussion of the proposed general rules listed certain activities that would not be considered health care operations because they were sufficiently unrelated to treatment and payment to warrant requiring an individual to authorize such use or disclosure. Those activities included: marketing of health and non-health items and services; disclosure of protected health information for sale, rent or barter; use of protected health information by a non-health related division of an entity; disclosure of protected health information for eligibility, enrollment, underwriting, or risk rating determinations prior to an individuals' enrollment in a health plan; disclosure to an employer for employment determinations; and fundraising.

In the final rule, we do not change the general approach of defining health care operations: health care operations are the listed activities undertaken by the covered entity that maintains the protected health information (*i.e.,* one covered entity may not disclose protected health information for the operations of a second covered entity); a covered entity may use any protected health information it maintains for its operations (*e.g.,* a plan may use protected health information about former enrollees as well as current enrollees); we expand the proposed list to reflect many changes requested by commenters.

We modify the proposal that health care operations represent activities ''in support of'' treatment and payment functions. Instead, in the final rule, health care operations are the enumerated activities to the extent that the activities are related to the covered entity's functions as a health care provider, health plan or health care clearinghouse, *i.e.,* the entity's ''covered functions.'' We make this change to clarify that health care operations includes general administrative and business functions necessary for the covered entity to remain a viable business. While it is possible to draw a connection between all the enumerated activities and ''treatment and payment,'' for some general business activities (*e.g.,* audits for financial disclosure statements) that connection may be tenuous. The proposed concept also did not include the operations of those health care clearinghouses that may be covered by this rule outside their status as business associate to a covered entity. We expand the definition to include disclosures for the enumerated activities of organized health care arrangements in which the covered entity participates. See also the definition of organized health care arrangements, below.

In addition, we make the following changes and additions to the enumerated subparagraphs:

(1) We add language to clarify that the primary purpose of the studies encompassed by ''quality assessment and improvement activities'' must not be to obtain generalizable knowledge. A study with such a purpose would meet the rule's definition of research, and use or disclosure of protected health information would have to meet the requirements of §§ 164.508 or 164.512(i). Thus, studies may be conducted as a health care operation if development of generalizable knowledge is not the primary goal. However, if the study changes and the covered entity intends the results to be generalizable, the change should be documented by the covered entity as proof that, when initiated, the primary purpose was health care operations.

We add population-based activities related to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions that do not entail direct patient care. Many commenters recommended adding the term ''disease management'' to health care operations. We were unable, however, to find a generally accepted definition of the term. Rather than rely on this label, we include many of the functions often included in discussions of disease management in this definition or in the definition of treatment. This topic is discussed further in the comment responses below.

(2) We have deleted ''undergraduate and graduate'' as a qualifier for ''students,'' to make the term more general and inclusive. We add the term ''practitioners.'' We expand the purposes encompassed to include situations in which health care providers are working to improve their skills. The rule also adds the training of non-health care professionals.

(3) The rule expands the range of insurance related activities to include those related to the creation, renewal or replacement of a contract for health insurance or health benefits, as well as ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss and excess of loss insurance). For these activities, we also eliminate the proposed requirement that these uses and disclosures apply only to protected health information about individuals already enrolled in a health plan. Under this provision, a group health plan that wants to replace its insurance carrier may disclose certain protected health information to insurance issuers in order to obtain bids on new coverage, and an insurance carrier interested in bidding on new business may use protected health information obtained from the potential new client to develop the product and pricing it will offer. For circumstances in which no new contract is issued, we add a provision in § 164.514(g) restricting the recipient health plan from using or disclosing protected health information obtained for this purpose, other than as required by law. Uses and disclosures in these cases come within the definition of ''health care operations,'' provided that the requirements of § 164.514(g) are met, if applicable. See § 164.504(f) for requirements for such disclosures by group health plans, as well as specific restrictions on the information that may be disclosed to plan sponsors for such purposes. We note that a covered health care provider must obtain an authorization under § 164.508 in order to disclose protected health information about an individual for purposes of pre-enrollment underwriting; the underwriting is not an ''operation'' of the provider and that disclosure is not otherwise permitted by a provision of this rule.

(4) We delete reference to the ''compiling and analyzing information in anticipation of or for use in a civil or criminal legal proceeding'' and replace it with a broader reference to

conducting or arranging for ''legal services.''

We add two new categories of activities:

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.

(6) Business management activities and general administrative functions, such as management activities relating to implementation of and compliance with the requirements of this subchapter, fundraising for the benefit of the covered entity to the extent permitted without authorization under § 164.514(f), and marketing of certain services to individuals served by the covered entity, to the extent permitted without authorization under § 164.514(e) (see discussion in the preamble to that section, below). For example, under this category we permit uses or disclosures of protected health information to determine from whom an authorization should be obtained, for example to generate a mailing list of individuals who would receive an authorization request.

We add to the definition of health care operations disclosure of protected health information for due diligence to a covered entity that is a potential successor in interest. This provision includes disclosures pursuant to the sale of a covered entity's business as a going concern, mergers, acquisitions, consolidations, and other similar types of corporate restructuring between covered entities, including a division of a covered entity, and to an entity that is not a covered entity but will become a covered entity if the transfer or sale is completed. Other types of sales of assets, or disclosures to organizations that are not and would not become covered entities, are not included in the definition of health care operations and could only occur if the covered entity obtained valid authorization for such disclosure in accordance with § 164.508, or if the disclosure is otherwise permitted under this rule.

We also add to health care operations disclosure of protected health information for resolution of internal grievances. These uses and disclosures include disclosure to an employee and/or employee representative, for example when the employee needs protected health information to demonstrate that the employer's allegations of improper conduct are untrue. We note that such employees and employee representatives are not providing services to or for the covered entity, and, therefore, no business associate contract is required. Also included are resolution of disputes from patients or enrollees regarding the quality of care and similar matters.

We also add use for customer service, including the provision of data and statistical analyses for policyholders, plan sponsors, or other customers, as long as the protected health information is not disclosed to such persons. We recognize that part of the general management of a covered entity is customer service. We clarify that customer service may include the use of protected health information to provide data and statistical analyses. For example, a plan sponsor may want to understand why its costs are rising faster than average, or why utilization in one plant location is different than in another location. An association that sponsors an insurance plan for its members may want information on the relative costs of its plan in different areas. Some plan sponsors may want more detailed analyses that attempt to identify health problems in a work site. We note that when a plan sponsor has several different group health plans, or when such plans provide insurance or coverage through more than one health insurance issuer or HMO, the covered entities may jointly engage in this type of analysis as a health care operation of the organized health care arrangement.

This activity qualifies as a health care operation only if it does not result in the disclosure of protected health information to the customer. The results of the analyses must be presented in a way that does not disclose protected health information. A disclosure of protected health information to the customer as a health care operation under this provision violates this rule. This provision is not intended to permit covered entities to circumvent other provisions in this rule, including requirements relating to disclosures of protected health information to plan sponsors or the requirements relating to research. See § 164.504(f) and § 164.512(i).

We use the term customer to provide flexibility to covered entities. We do not intend the term to apply to persons with whom the covered entity has no other business; this provision is intended to permit covered entities to provide service to their existing customer base.

We note that this definition, either alone or in conjunction with the definition of ''organized health care arrangement,'' allows an entity such as an integrated staff model HMO, whether legally integrated or whether a group of associated entities, that hold themselves out as an organized arrangement to share protected health information under § 164.506. In these cases, the sharing of protected health information will be either for the operations of the disclosing entity or for the organized health care arrangement in which the entity is participating.

Whether a disclosure is allowable for health care operations under this provision is determined separately from whether a business associate contract is required. These provisions of the rule operate independently. Disclosures for health care operations may be made to an entity that is neither a covered entity nor a business associate of the covered entity. For example, a covered academic medical center may disclose certain protected health information to community health care providers who participate in one of its continuing medical education programs, whether or not such providers are covered health care providers under this rule. A provider attending a continuing education program is not thereby performing services for the covered entity sponsoring the program and, thus, is not a business associate for that purpose. Similarly, health plans may disclose for due diligence purposes to another entity that may or may not be a covered entity or a business associate.

Health Oversight Agency

The proposed rule would have defined ''health oversight agency'' as ''an agency, person, or entity, including the employees or agents thereof, (1) That is: (i) A public agency; or (ii) A person or entity acting under grant of authority from or contract with a public agency; and (2) Which performs or oversees the performance of any audit; investigation; inspection; licensure or discipline; civil, criminal, or administrative proceeding or action; or other activity necessary for appropriate oversight of the health care system, of government benefit programs for which health information is relevant to beneficiary eligibility, or of government regulatory programs for which health information is necessary for determining compliance with program standards.'' The proposed rule also described the functions of health oversight agencies in the proposed health oversight section (§ 164.510(c)) by repeating much of this definition.

In the final rule, we modify the definition of health oversight agency by eliminating from the definition the language in proposed § 164.510(c) (now § 164.512(d)). In addition, the final rule clarifies this definition by specifying that a ''health oversight agency'' is an agency or authority of the United States,

a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or grantees, that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

The preamble to the proposed rule listed the following as examples of health oversight agencies that conduct oversight activities relating to the health care system: state insurance commissions, state health professional licensure agencies, Offices of Inspectors General of federal agencies, the Department of Justice, state Medicaid fraud control units, Defense Criminal Investigative Services, the Pension and Welfare Benefit Administration, the HHS Office for Civil Rights, and the FDA. The proposed rule listed the Social Security Administration and the Department of Education as examples of health oversight agencies that conduct oversight of government benefit programs for which health information is relevant to beneficiary eligibility. The proposed rule listed the Occupational Health and Safety Administration and the Environmental Protection Agency as examples of oversight agencies that conduct oversight of government regulatory programs for which health information is necessary for determining compliance with program standards.

In the final rule, we include the following as additional examples of health oversight activities: (1) The U.S. Department of Justice's civil rights enforcement activities, and in particular, enforcement of the Civil Rights of Institutionalized Persons Act (42 U.S.C. 1997–1997j) and the Americans with Disabilities Act (42 U.S.C. 12101 *et seq.*), as well as the EEOC's civil rights enforcement activities under titles I and V of the ADA; (2) the FDA's oversight of food, drugs, biologics, devices, and other products pursuant to the Food, Drug, and Cosmetic Act (21 U.S.C. 301 *et seq.*) and the Public Health Service Act (42 U.S.C. 201 *et seq.*); and (3) data analysis —performed by a public agency or by a person or entity acting under grant of authority from or under contract with a public agency —to detect health care fraud.

''Overseeing the health care system,'' which is included in the definition of health oversight, encompasses activities such as: oversight of health care plans; oversight of health benefit plans; oversight of health care providers; oversight of health care and health care delivery; oversight activities that involve resolution of consumer complaints; oversight of pharmaceuticals, medical products and devices, and dietary supplements; and a health oversight agency's analysis of trends in health care costs, quality, health care delivery, access to care, and health insurance coverage for health oversight purposes.

We recognize that health oversight agencies, such as the U.S. Department of Labor's Pension and Welfare Benefits Administration, may perform more than one type of health oversight. For example, agencies may sometimes perform audits and investigations and at other times conduct general oversight of health benefit plans. Such entities are considered health oversight agencies under the rule for any and all of the health oversight functions that they perform.

The definition of health oversight agency does not include private organizations, such as private-sector accrediting groups. Accreditation organizations are performing health care operations functions on behalf of health plans and covered health care providers. Accordingly, in order to obtain protected health information without individuals' authorizations, accrediting groups must enter into business associate agreements with health plans and covered health care providers for these purposes. Similarly, private entities, such as coding committees, that help government agencies that are health plans make coding and payment decisions are performing health care payment functions on behalf the government agencies and, therefore, must enter into business associate agreements in order to receive protected health information from the covered entity (absent individuals' authorization for such disclosure).

Indirect Treatment Relationship

This term was not included in the proposed rule. An ''indirect treatment relationship'' is a relationship between a health care provider and an individual in which the provider delivers health care to the individual based on the orders of another health care provider and the health care services, products, diagnoses, or results are typically furnished to the patient through another provider, rather than directly. For example, radiologists and pathologists generally have indirect treatment relationships with patients because they deliver diagnostic services based on the orders of other providers and the results of those services are furnished to the patient through the direct treating provider. This definition is necessary to clarify the relationships between providers and individuals in the regulation. For example, see the consent discussion at § 164.506.

Individual

We proposed to define ''individual'' to mean the person who is the subject of the protected health information. We proposed that the term include, with respect to the signing of authorizations and other rights (such as access, copying, and correction), the following types of legal representatives:

(1) With respect to adults and emancipated minors, legal representatives (such as court-appointed guardians or persons with a power of attorney), to the extent to which applicable law permits such legal representatives to exercise the person's rights in such contexts.

(2) With respect to unemancipated minors, a parent, guardian, or person acting in loco parentis, provided that when a minor lawfully obtains a health care service without the consent of or notification to a parent, guardian, or other person acting in *loco parentis,* the minor shall have the exclusive right to exercise the rights of an individual with respect to the protected health information relating to such care.

(3) With respect to deceased persons, an executor, administrator, or other person authorized under applicable law to act on behalf of the decedent's estate.

In addition, we proposed to exclude from the definition:

(1) Foreign military and diplomatic personnel and their dependents who receive health care provided by or paid for by the Department of Defense or other federal agency or by an entity acting on its behalf, pursuant to a country-to-country agreement or federal statute.

(2) Overseas foreign national beneficiaries of health care provided by the Department of Defense or other federal agency or by a non-governmental organization acting on its behalf.

In the final rule, we eliminate from the definition of ''individual'' the provisions designating a legal representative as the ''individual'' for purposes of exercising certain rights with regard to protected health information. Instead, we include in the final rule a separate standard for ''personal representatives.'' A covered entity must treat a personal representative of an individual as the individual except under specified circumstances. See discussion in

§ 164.502(g) regarding personal representatives.

In addition, we eliminate from the definition of ''individual'' the above exclusions for foreign military and diplomatic personnel and overseas foreign national beneficiaries. We address the special circumstances for use and disclosure of protected health information about individuals who are foreign military personnel in § 164.512(k). We address overseas foreign national beneficiaries in § 164.500, ''Applicability.'' The protected health information of individuals who are foreign diplomatic personnel and their dependents are not subject to special treatment under the final rule.

Individually identifiable health information about one individual may exist in the health records of another individual; health information about one individual may include health information about a second person. For example, a patient's medical record may contain information about the medical conditions of the patient's parents, children, and spouse, as well as their names and contact information. For the purpose of this rule, if information about a second person is included within the protected health information of an individual, the second person is not the person who is the subject of the protected health information. The second person is not the ''individual'' with regard to that protected health information, and under this rule thus does not have the individual's rights (*e.g.,* access and amendment) with regard to that information.

Individually Identifiable Health Information

We proposed to define ''individually identifiable health information'' to mean information that is a subset of health information, including demographic information collected from an individual, and that:

(1) Is created by or received from a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

(i) Which identifies the individual, or

(ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

In the final rule, we change ''created by or received from a health care provider * * *'' to ''created or received by a health care provider * * * ''in order to conform to the statute. We otherwise retain the definition of ''individually identifiable health information'' without change in the final rule.

Inmate

The proposed rule did not define the term inmate. In the final rule, it is defined as a person incarcerated in or otherwise confined to a correctional institution. The addition of this definition is necessary to explain the privacy rights and protections of inmates in this regulation.

Law Enforcement Official

The proposed rule would have defined a ''law enforcement official'' as ''an official of an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to conduct: (1) An investigation or official proceeding inquiring into a violation of, or failure to comply with, any law; or (2) a criminal, civil, or administrative proceeding arising from a violation of, or failure to comply with, any law.''

The final rule modifies this definition slightly. The definition in the final rule recognizes that law enforcement officials are empowered to prosecute cases as well as to conduct investigations and civil, criminal, or administrative proceedings. In addition, the definition in the final rule reflects the fact that when investigations begin, often it is not clear that law has been violated. Thus, the final rule describes law enforcement investigations and official proceedings as inquiring into a potential violation of law. In addition, it describes law enforcement-related civil, criminal, or administrative proceedings as arising from alleged violation of law.

Marketing

The proposed rule did not include a definition of ''marketing.'' The proposed rule generally required that a covered entity would need an authorization from an individual to use or disclose protected health information for marketing.

In the final rule we define marketing as a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. The definition does not limit the type or means of communication that are considered marketing.

The definition of marketing contains three exceptions. If a covered entity receives direct or indirect remuneration from a third party for making a written communication otherwise described in an exception, then the communication is not excluded from the definition of marketing. The activities we except from the definition of marketing are encompassed by the definitions of treatment, payment, and health care operations. Covered entities may therefore use and disclose protected health information for these excepted activities without authorization under § 164.508 and pursuant to any applicable consent obtained under § 164.506.

The first exception applies to communications made by a covered entity for the purpose of describing the entities participating in a provider network or health plan network. It also applies to communications made by a covered entity for the purpose of describing if and the extent to which a product or service, or payment for a product or service, is provided by the covered entity or included in a benefit plan. This exception permits covered entities to use or disclose protected health information when discussing topics such as the benefits and services available under a health plan, the payment that may be made for a product or service, which providers offer a particular product or service, and whether a provider is part of a network or whether (and what amount of) payment will be provided with respect to the services of particular providers. This exception expresses our intent not to interfere with communications made to individuals about their health benefits.

The second exception applies to communications tailored to the circumstances of a particular individual, made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual. This exception leaves health care providers free to use or disclose protected health information as part of a discussion of its products and services, or the products and services of others, and to prescribe, recommend, or sell such products or services, as part of the treatment of an individual. This exception includes activities such as referrals, prescriptions, recommendations, and other communications that address how a product or service may relate to the individual's health. This exception expresses our intent not to interfere with communications made to individuals about their treatment.

The third exception applies to communications tailored to the

circumstances of a particular individual and made by a health care provider or health plan to an individual in the course of managing the treatment of that individual or for the purpose of directing or recommending to that individual alternative treatments, therapies, providers, or settings of care. As with the previous exception, this exception permits covered entities to discuss freely their products and services and the products and services of third parties, in the course of managing an individual's care or providing or discussing treatment alternatives with an individual, even when such activities involve the use or disclose protected health information.

Section 164.514 contains provisions governing use or disclosure of protected health information in marketing communications, including a description of certain marketing communications that may use or include protected health information but that may be made by a covered entity without individual authorization. The definition of health care operations includes those marketing communications that may be made without an authorization pursuant to § 164.514. Covered entities may therefore use and disclose protected health information for these activities pursuant to any applicable consent obtained under § 164.506, or, if they are not required to obtain a consent under § 164.506, without one.

Organized Health Care Arrangement

This term was not used in the proposed rule. We define the term in order to describe certain arrangements in which participants need to share protected health information about their patients to manage and benefit the common enterprise. To allow uses and disclosures of protected health information for these arrangements, we also add language to the definition of ''health care operations.'' See discussion of that term above.

We include five arrangements within the definition of organized health care arrangement. The arrangements involve clinical or operational integration among legally separate covered entities in which it is often necessary to share protected health information for the joint management and operations of the arrangement. They may range in legal structure, but a key component of these arrangements is that individuals who obtain services from them have an expectation that these arrangements are integrated and that they jointly manage their operations. We include within the definition a clinically integrated care setting in which individuals typically receive health care from more than one health care provider. Perhaps the most common example of this type of organized health care arrangement is the hospital setting, where a hospital and a physician with staff privileges at the hospital together provide treatment to the individual. Participants in such clinically integrated settings need to be able to share health information freely not only for treatment purposes, but also to improve their joint operations. For example, any physician with staff privileges at a hospital must be able to participate in the hospital's morbidity and mortality reviews, even when the particular physician's patients are not being discussed. Nurses and other hospital personnel must also be able to participate. These activities benefit the common enterprise, even when the benefits to a particular participant are not evident. While protected health information may be freely shared among providers for treatment purposes under other provisions of this rule, some of these joint activities also support the health care operations of one or more participants in the joint arrangement. Thus, special rules are needed to ensure that this rule does not interfere with legitimate information sharing among the participants in these arrangements.

We also include within the definition an organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement, and in which the joint activities of the participating covered entities include at least one of the following: utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or payment activities, if the financial risk for delivering health care is shared in whole or in part by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk. A common example of this type of organized health care arrangement is an independent practice association formed by a large number of physicians. They may advertise themselves as a common enterprise (*e.g.,* Acme IPA), whether or not they are under common ownership or control, whether or not they practice together in an integrated clinical setting, and whether or not they share financial risk.

If such a group engages jointly in one or more of the listed activities, the participating covered entities will need to share protected health information to undertake such activities and to improve their joint operations. In this example, the physician participants in the IPA may share financial risk through common withhold pools with health plans or similar arrangements. The IPA participants who manage the financial arrangements need protected health information about all the participants' patients in order to manage the arrangement. (The participants may also hire a third party to manage their financial arrangements.) If the participants in the IPA engage in joint quality assurance or utilization review activities, they will need to share protected health information about their patients much as participants in an integrated clinical setting would. Many joint activities that require the sharing of protected health information benefit the common enterprise, even when the benefits to a particular participant are not evident.

We include three relationships related to group health plans as organized health care arrangements. First, we include a group health plan and an issuer or HMO with respect to the group health plan within the definition, but only with respect to the protected health information of the issuer or HMO that relates to individuals who are or have been participants or beneficiaries in the group health plan. We recognize that many group health plans are funded partially or fully through insurance, and that in some cases the group health plan and issuer or HMO need to coordinate operations to properly serve the enrollees. Second, we include a group health plan and one or more other group health plans each of which are maintained by the same plan sponsor. We recognize that in some instances plan sponsors provide health benefits through a combination of group health plans, and that they may need to coordinate the operations of such plans to better serve the participants and beneficiaries of the plans. Third, we include a combination of group health plans maintained by the same plan sponsor and the health insurance issuers and HMOs with respect to such plans, but again only with respect to the protected health information of such issuers and HMOs that relates to

individuals who are or have been enrolled in such group health plans. We recognize that is some instances a plan sponsor may provide benefits through more than one group health plan, and that such plans may fund the benefits through one or more issuers or HMOs. Again, coordinating health care operations among these entities may be necessary to serve the participants and beneficiaries in the group health plans. We note that the necessary coordination may necessarily involve the business associates of the covered entities and may involve the participation of the plan sponsor to the extent that it is providing plan administration functions and subject to the limits in § 164.504.

Payment

We proposed the term payment to mean:

(1) The activities undertaken by or on behalf of a covered entity that is:

(i) A health plan, or by a business partner on behalf of a health plan, to obtain premiums or to determine or fulfill its responsibility for coverage under the health plan and for provision of benefits under the health plan; or

(ii) A health care provider or health plan, or a business partner on behalf of such provider or plan, to obtain reimbursement for the provision of health care.

(2) Activities that constitute payment include:

(i) Determinations of coverage, adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, and medical data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and

(v) Utilization review activities, including precertification and preauthorization of services.

In the final rule, we maintain the general approach of defining of payment: payment activities are described generally in the first clause of the definition, and specific examples are given in the second clause. Payment activities relate to the covered entity that maintains the protected health information (*i.e.,* one covered entity may not disclose protected health information for the payment activities of a second covered entity). A covered entity may use or disclose only the protected health information about the individual to whom care was rendered, for its payment activities (*e.g.,* a provider may disclose protected health information only about the patient to whom care was rendered in order to obtain payment for that care, or only the protected health information about persons enrolled in the particular health plan that seeks to audit the provider's records). We expand the proposed list to reflect many changes requested by commenters.

We add eligibility determinations as an activity included in the definition of payment. We expand coverage determinations to include the coordination of benefits and the determination of a specific individual's cost sharing amounts. The rule deletes activities related to the improvement of methods of paying or coverage policies from this definition and instead includes them in the definition of health care operations. We add to the definition ''collection activities.'' We replace ''medical data processing'' activities with health care data processing related to billing, claims management, and collection activities. We add activities for the purpose of obtaining payment under a contract for reinsurance (including stop-loss and excess of loss insurance). Utilization review activities now include concurrent and retrospective review of services.

In addition, we modify this definition to clarify that the activities described in section 1179 of the Act are included in the definition of ''payment.'' We add new subclause (vi) allowing covered entities to disclose to consumer reporting agencies an individual's name, address, date of birth, social security number and payment history, account number, as well as the name and address of the individual's health care provider and/or health plan, as appropriate. Covered entities may make disclosure of this protected health information to consumer reporting agencies for purposes related to collection of premiums or reimbursement. This allows reporting not just of missed payments and overdue debt but also of subsequent positive payment experience (*e.g.,* to expunge the debt). We consider such positive payment experience to be ''related to'' collection of premiums or reimbursement.

The remaining activities described in section 1179 are included in other language in this definition. For example, ''authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care'' are covered by paragraph (2)(iii) of the definition, which allows use and disclosure of protected health information for ''billing, claims management, collection activities and related health care data processing.'' ''Claims management'' also includes auditing payments, investigating and resolving payment disputes and responding to customer inquiries regarding payments. Disclosure of protected health information for compliance with civil or criminal subpoenas, or with other applicable laws, are covered under § 164.512 of this regulation. (See discussion above regarding the interaction between 1179 and this regulation.)

We modify the proposed regulation text to clarify that payment includes activities undertaken to reimburse health care providers for treatment provided to individuals.

Covered entities may disclose protected health information for payment purposes to any other entity, regardless of whether it is a covered entity. For example, a health care provider may disclose protected health information to a financial institution in order to cash a check or to a health care clearinghouse to initiate electronic transactions. However, if a covered entity engages another entity, such as a billing service or a financial institution, to conduct payment activities on its behalf, the other entity may meet the definition of ''business associate'' under this rule. For example, an entity is acting as a business associate when it is operating the accounts receivable system on behalf of a health care provider.

Similarly, payment includes disclosure of protected health information by a health care provider to an insurer that is not a ''health plan'' as defined in this rule, to obtain payment. For example, protected health information may be disclosed to obtain reimbursement from a disability insurance carrier. We do not interpret the definition of ''payment'' to include activities that involve the disclosure of protected health information by a covered entity, including a covered health care provider, to a plan sponsor for the purpose of obtaining payment under a group health plan maintained by such plan sponsor, or for the purpose of obtaining payment from a health insurance issuer or HMO with respect to a group health plan maintained by such plan sponsor, unless the plan sponsor is performing plan administration pursuant to § 164.504(f).

The Transactions Rule adopts standards for electronic health care transactions, including two for processing payments. We adopted the ASC X12N 835 transaction standard for ''Health Care Payment and Remittance

Advice'' transactions between health plans and health care providers, and the ASC X12N 820 standard for ''Health Plan Premium Payments'' transactions between entities that arrange for the provision of health care or provide health care coverage payments and health plans. Under these two transactions, information to effect funds transfer is transmitted in a part of the transaction separable from the part containing any individually identifiable health information.

We note that a covered entity may conduct the electronic funds transfer portion of the two payment standard transactions with a financial institution without restriction, because it contains no protected health information. The protected health information contained in the electronic remittance advice or the premium payment enrollee data portions of the transactions is not necessary either to conduct the funds transfer or to forward the transactions. Therefore, a covered entity may not disclose the protected health information to a financial institution for these purposes. A covered entity may transmit the portions of the transactions containing protected health information through a financial institution if the protected health information is encrypted so it can be read only by the intended recipient. In such cases no protected health information is disclosed and the financial institution is acting solely as a conduit for the individually identifiable data.

Plan Sponsor

In the final rule we add a definition of ''plan sponsor.'' We define plan sponsor by referencing the definition of the term provided in (3)(16)(B) of the Employee Retirement Income Security Act (ERISA). The plan sponsor is the employer or employee organization, or both, that establishes and maintains an employee benefit plan. In the case of a plan established by two or more employers, it is the association, committee, joint board of trustees, or other similar group or representative of the parties that establish and maintain the employee benefit plan. This term includes church health plans and government health plans. Group health plans may disclose protected health information to plan sponsors who conduct payment and health care operations activities on behalf of the group health plan if the requirements for group health plans in § 164.504 are met.

The preamble to the Transactions Rule noted that plan sponsors of group health plans are not covered entities and, therefore, are not required to use the standards established in that regulation to perform electronic transactions, including enrollment and disenrollment transactions. We do not change that policy through this rule. Plan sponsors that perform enrollment functions are doing so on behalf of the participants and beneficiaries of the group health plan and not on behalf of the group health plan itself. For purposes of this rule, plan sponsors are not subject to the requirements of § 164.504 regarding group health plans when conducting enrollment activities.

Protected Health Information

We proposed to define ''protected health information'' to mean individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form. For purposes of this definition, we proposed to define ''electronically transmitted'' as including information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response, and ''faxback'' systems. We proposed that this definition not include ''paper-to-paper'' faxes, or person-to-person telephone calls, video teleconferencing, or messages left on voice-mail.

Further, ''electronically maintained'' was proposed to mean information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

The proposal's definition explicitly excluded:

(1) Individually identifiable health information that is part of an ''education record'' governed by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g.

(2) Individually identifiable health information of inmates of correctional facilities and detainees in detention facilities.

In this final rule we expand the definition of protected health information to encompass all individually identifiable health information transmitted or maintained by a covered entity, regardless of form. Specifically, we delete the conditions for individually identifiable health information to be ''electronically maintained'' or ''electronically transmitted'' and the corresponding definitions of those terms. Instead, the final rule defines protected health information to be individually identifiable health information that is:

(1) Transmitted by electronic media;

(2) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or

(3) Transmitted or maintained in any other form or medium.

We refer to electronic media, as defined in § 162.103, which means the mode of electronic transmission. It includes the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

The definition of protected health information is set out in this form to emphasize the severability of this provision. As discussed below, we believe we have ample legal authority to cover all individually identifiable health information transmitted or maintained by covered entities. We have structured the definition this way so that, if a court were to disagree with our view of our authority in this area, the rule would still be operational, albeit with respect to a more limited universe of information.

Other provisions of the rules below may also be severable, depending on their scope and operation. For example, if the rule itself provides a fallback, as it does with respect to the various discretionary uses and disclosures permitted under § 164.512, the provisions would be severable under case law.

The definition in the final rule retains the exception relating to individually identifiable health information in ''education records'' governed by FERPA. We also exclude the records described in 20 U.S.C. 1232g(a)(4)(B)(iv). These are records of students held by post-secondary educational institutions or of students 18 years of age or older, used exclusively for health care treatment and which have not been disclosed to anyone other than a health care provider at the student's request. (See discussion of FERPA above.)

We have removed the exception for individually identifiable health information of inmates of correctional facilities and detainees in detention facilities. Individually identifiable health information about inmates is protected health information under the final rule, and special rules for use and disclosure of the protected health

information about inmates and their ability to exercise the rights granted in this rule are described below.

Psychotherapy Notes

Section 164.508(a)(3)(iv)(A) of the proposed rule defined psychotherapy notes as notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. The proposed definition excluded medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis and progress. Furthermore, we stated in the preamble of the proposed rule that psychotherapy notes would have to be maintained separately from the medical record.

In this final rule, we retain the definition of psychotherapy notes that we had proposed, but add to the regulation text the requirement that, to meet the definition of psychotherapy notes, the information must be separated from the rest of the individual's medical record.

Public Health Authority

The proposed rule would have defined ''public health authority'' as ''an agency or authority of the United States, a state, a territory, or an Indian tribe that is responsible for public health matters as part of its official mandate.''

The final rule changes this definition slightly to clarify that a ''public health authority'' also includes a person or entity acting under a grant of authority from or contract with a public health agency. Therefore, the final rule defines this term as an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required By Law

In the preamble to the NPRM, we did not include a definition of ''required by law.'' We discussed what it meant for an action to be considered to be ''required'' or ''mandated'' by law and included several examples of activities that would be considered as required by law for the purposes of the proposed rule, including a valid Inspector General subpoena, grand jury subpoena, civil investigative demand, or a statute or regulation requiring production of information justifying a claim would constitute a disclosure required by law.

In the final rule we include a new definition, move the preamble clarifications to the regulatory text and add several items to the illustrative list. For purposes of this regulation, ''required by law'' means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Among the examples listed in definition are Medicare conditions of participation with respect to health care providers participating in that program, court-ordered warrants, and subpoenas issued by a court. We note that disclosures ''required by law'' include disclosures of protected health information required by this regulation in § 164.502(a)(2). It does not include contracts between private parties or similar voluntary arrangements. This list is illustrative only and is not intended in any way to limit the scope of this paragraph or other paragraphs in § 164.512 that permit uses or disclosures to the extent required by other laws. We note that nothing in this rule compels a covered entity to make a use or disclosure required by the legal demands or prescriptions listed in this clarification or by any other law or legal process, and a covered entity remains free to challenge the validity of such laws and processes.

Research

We proposed to define ''research'' as it is defined in the Federal Policy for the Protection of Human Subjects, at 45 CFR part 46, subpart A (referred to elsewhere in this rule as ''Common Rule''), and in addition, elaborated on the meaning of the term ''generalizable knowledge.'' In § 164.504 of the proposed rule we defined research as ''* * * a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. 'Generalizable knowledge' is knowledge related to health that can be applied to populations outside of the population served by the covered entity.''

The final rule eliminates the further elaboration of ''generalizable knowledge.'' Therefore, the rule defines ''research'' as the term is defined in the Common Rule: a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.

Research Information Unrelated to Treatment

We delete this definition and the associated requirements from the final rule. Refer to § 164.508(f) for new requirements regarding authorizations for research that includes treatment of the individual.

Treatment

The proposed rule defined ''treatment'' as the provision of health care by, or the coordination of health care (including health care management of the individual through risk assessment, case management, and disease management) among, health care providers; the referral of a patient from one provider to another; or the coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual. The preamble noted that the definition was intended to relate only to services provided to an individual and not to an entire enrolled population.

In the final rule, we do not change the general approach to defining treatment: treatment means the listed activities undertaken by any health care provider, not just a covered health care provider. A plan can disclose protected health information to any health care provider to assist the provider's treatment activities; and a health care provider may use protected health information about an individual to treat another individual. A health care provider may use any protected health information it maintains for treatment purposes (*e.g.,* a provider may use protected health information about former patients as well as current patients). We modify the proposed list of treatment activities to reflect changes requested by commenters.

Specifically, we modify the proposed definition of ''treatment'' to include the management of health care and related services. Under the definition, the provision, coordination, or management of health care or related services may be undertaken by one or more health care providers. ''Treatment'' includes coordination or management by a health care provider with a third party and consultation between health care providers. The term also includes referral by a health care provider of a patient to another health care provider.

Treatment refers to activities undertaken on behalf of a single patient, not a population. Activities are considered treatment only if delivered

by a health care provider or a health care provider working with another party. Activities of health plans are not considered to be treatment. Many services, such as a refill reminder communication or nursing assistance provided through a telephone service, are considered treatment activities if performed by or on behalf of a health care provider, such as a pharmacist, but are regarded as health care operations if done on behalf of a different type of entity, such as a health plan.

We delete specific reference to risk assessment, case management, and disease management. Activities often referred to as risk assessment, disease and case management are treatment activities only to the extent that they are services provided to a particular patient by a health care provider; population based analyses or records review for the purposes of treatment protocol development or modification are health care operations, not treatment activities. If a covered entity is licensed as both a health plan and a health care provider, a single activity could be considered to be both treatment and health care operations; for compliance purposes we would consider the purpose of the activity. Given the integration of the health care system we believe that further classification of activities into either treatment or health care operations would not be helpful. See the definition of health care operations for additional discussion.

Use

We proposed to define ''use'' to mean the employment, application, utilization, examination, or analysis of information within an entity that holds the information. In the final rule, we clarify that use refers to the use of individually identifiable health information. We replace the term ''holds'' with the term ''maintains.'' These changes are for clarity only, and are not intended to effect any substantive change.

Section 164.502—General Rules for Uses and Disclosures of Protected Health Information

Section 164.502(a)—Use and Disclosure for Treatment, Payment and Health Care Operations

As a general rule, we proposed in the NPRM to prohibit covered entities from using or disclosing protected health information except as authorized by the individual who is the subject of such information or as explicitly permitted by the rule. The proposed rule explicitly would have permitted covered entities to use or disclose an individual's protected health information without authorization for treatment, payment, and health care operations. The proposal would not have restricted to whom disclosures could be made for the purposes of treatment, payment, or operations. The proposal would have allowed disclosure of the protected health information of one individual for the treatment or payment of another, as appropriate. We also proposed to prohibit covered entities from seeking individual authorization for uses and disclosures for treatment, payment, and health care operations unless required by state or other applicable law.

We proposed two exceptions to this general rule which prohibited covered entities from using or disclosing research information unrelated to treatment or psychotherapy notes for treatment, payment, or health care operations purposes unless a specific authorization was obtained from the subject of the information. In addition, we proposed that a covered entity be prohibited from conditioning treatment, enrollment in a health plan or payment decisions on a requirement that the individual provide a specific authorization for the disclosure of these two types of information (see proposed § 164.508(a)(3)(iii)).

We also proposed to permit covered entities to use or disclose an individual's protected health information for specified public and public policy-related purposes, including public health, research, health oversight, law enforcement, and use by coroners. In addition, the proposal would have permitted covered entities to use and disclose protected health information when required to do so by other law or pursuant to an authorization from the individual allowing them to use or disclose the information for purposes other than treatment, payment or health care operations.

We proposed to require covered entities to disclose protected health information for only two purposes: to permit individuals to inspect and copy protected health information about themselves and for enforcement of the rule.

We proposed not to require covered entities to vary the level of protection accorded to protected health information based on the sensitivity of such information. In addition, we proposed to require that each affected entity assess its own needs and devise, implement, and maintain appropriate privacy policies, procedures, and documentation to address its business requirements.

In the final rule, the general standard remains that covered entities may use or disclose protected health information only as permitted or required by this rule. However, we make significant changes to the conditions under which uses and disclosures are permitted.

We revise the application of the general standard to require covered health care providers who have a direct treatment relationship with an individual to obtain a general ''consent'' from the individual in order to use or disclose protected health information about the individual for treatment, payment and health care operations (for details on who must obtain such consents and the requirements they must meet, see § 164.506). These consents are intended to accommodate both the covered provider's need to use or disclose protected health information for treatment, payment, and health care operations, and also the individual's interest in understanding and acquiescing to such uses and disclosures. In general, other covered entities are permitted to use and disclose protected health information to carry out treatment, payment, or health care operations (as defined in this rule) without obtaining such consent, as in the proposed rule. Covered entities must, as under the proposed rule, obtain the individual's ''authorization'' in order to use or disclose psychotherapy notes for most purposes: see § 164.508(a)(2) for exceptions to this rule. We delete the proposed special treatment of ''research information unrelated to treatment.''

We revise the application of the general standard to require all covered entities to obtain the individual's verbal ''agreement'' before using or disclosing protected health information for facility directories, to persons assisting in the individual's care, and for other purposes described in § 164.510. Unlike ''consent'' and ''authorization,'' verbal agreement may be informal and implied from the circumstances (for details on who must obtain such agreements and the requirements they must meet, see § 164.510). Verbal agreements are intended to accommodate situations where it is neither appropriate to remove from the individual the ability to control the protected health information nor appropriate to require formal, written permission to share such information. For the most part, these provisions reflect current practices.

As under the proposed rule, we permit covered entities to use or disclose protected health information without the individual's consent, authorization or agreement for specified

public policy purposes, in compliance with the requirements in § 164.512.

We permit covered entities to disclose protected health information to the individual who is the subject of that information without any condition. We note that this may include disclosures to ''personal representatives'' of individuals as provided by § 164.502(g).

We permit a covered entity to use or disclose protected health information for other lawful purposes if the entity obtains a written ''authorization'' from the individual, consistent with the provisions of § 164.508. Unlike ''consents,'' these ''authorizations'' are specific and detailed. (For details on who must obtain such authorizations and the requirements they must meet, see § 164.508.) They are intended to provide the individuals with concrete information about, and control over, the uses and disclosures of protected health information about themselves.

The final rule retains the provision that requires a covered entity to disclose protected health information only in two instances: When individuals request access to information about themselves, and when disclosures are compelled by the Secretary for compliance and enforcement purposes.

Finally, § 164.502(a)(1) also requires covered entities to use or disclose protected health information in compliance with the other provisions of § 164.502, for example, consistent with the minimum necessary standard, to create de-identified information, or to a personal representative of an individual. These provisions are described below.

We note that a covered entity may use or disclose protected health information as permitted by and in accordance with a provision of this rule, regardless of whether that use or disclosure fails to meet the requirements for use or disclosure under another provision of this rule.

Section 164.502(b)—Minimum Necessary Uses and Disclosures

The proposed rule required a covered entity to make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose of the use or disclosure (proposed § 164.506(b)). This final rule significantly modifies the proposed requirements for implementing the minimum necessary standard. In the final rule, § 164.502(b) contains the basic standard and § 164.514 describes the requirements for implementing the standard. Therefore we discuss all aspects of the minimum necessary standard and specific requirements below in the discussion of § 164.514(d).

Section 164.502(c)—Uses and Disclosures Under a Restriction Agreement

The proposed rule would have required that covered health care providers permit individuals to request restrictions of uses and disclosures of protected health information and would have prohibited covered providers from using or disclosing protected health information in violation of any agreed-to restriction.

The final rule retains an individual's right to request restrictions on uses or disclosures for treatment, payment or health care operations and prohibits a covered entity from using or disclosing protected health information in a way that is inconsistent with an agreed upon restriction between the covered entity and the individual, but makes some changes to this right. Most significantly, under the final rule individuals have the right to request restrictions of all covered entities. This standard is set forth in § 164.522. Details about the changes to the standard are explained in the preamble discussion to § 164.522.

Section 164.502(d)—Creation of De-identified Information

In proposed § 164.506(d) of the NPRM, we proposed to permit use of protected health information for the purpose of creating de-identified information and we provided detailed mechanisms for doing so.

In § 164.502(d) of the final rule, we permit a covered entity to use protected health information to create de-identified information, whether or not the de-identified information is to be used by the covered entity. We clarify that de-identified information created in accordance with our procedures (which have been moved to § 164.514(a)) is not subject to the requirements of these privacy rules unless it is re-identified. Disclosure of a key or mechanism that could be used to re-identify such information is also defined to be disclosure of protected health information. See the preamble to § 164.514(a) for further discussion.

Section 164.502(e)—Business Associates

In the proposed rule, other than for purposes of consultation or referral for treatment, we would have allowed a covered entity to disclose protected health information to a business partner only pursuant to a written contract that would, among other specified provisions, limit the business partner's uses and disclosures of protected health information to those permitted by the contract, and would impose certain security, inspection and reporting requirements on the business partner. We proposed to define the term ''business partner'' to mean, with respect to a covered entity, a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity.

In the final rule, we change the term ''business partner'' to ''business associate'' and in the definition clarify the full range of circumstances in which a person is acting as a business associate of a covered entity. (See definition of ''business associate'' in § 160.103.) These changes mean that § 164.502(e) requires a business associate contract (or other arrangement, as applicable) not only when the covered entity discloses protected health information to a business associate, but also when the business associate creates or receives protected health information on behalf of the covered entity.

In the final rule, we modify the proposed standard and implementation specifications for business associates in a number of significant ways. These modifications are explained in the preamble discussion of § 164.504(e).

Section 164.502(f)—Deceased Individuals

We proposed to extend privacy protections to the protected health information of a deceased individual for two years following the date of death. During the two-year time frame, we proposed in the definition of ''individual'' that the right to control the deceased individual's protected health information would be held by an executor or administrator, or other person (*e.g.*, next of kin) authorized under applicable law to act on behalf of the decedent's estate. The only proposed exception to this standard allowed for uses and disclosures of a decedent's protected health information for research purposes without the authorization of a legal representative and without the Institutional Review Board (IRB) or privacy board approval required (in proposed § 164.510(j)) for most other uses and disclosures for research.

In the final rule (§ 164.502(f)), we modify the standard to extend protection of protected health information about deceased individuals for as long as the covered entity maintains the information. We retain the exception for uses and disclosures for research purposes, now part of § 164.512(i), but also require that the

covered entity take certain verification measures prior to release of the decedent's protected health information for such purposes (see §§ 164.514(h) and 164.512(i)(1)(iii)).

We remove from the definition of ''individual'' the provision related to deceased persons. Instead, we create a standard for ''personal representatives'' (§ 164.502(g), see discussion below) that requires a covered entity to treat a personal representative of an individual as the individual in certain circumstances, *i.e.*, allows the representative to exercise the rights of the individual. With respect to deceased individuals, the final rule describes when a covered entity must allow a person who otherwise is permitted under applicable law to act with respect to the interest of the decedent or on behalf of the decedent's estate, to make decisions regarding the decedent's protected health information.

The final rule also adds a provision to § 164.512(g), that permits covered entities to disclose protected health information to a funeral director, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. Such disclosures are permitted both after death and in reasonable anticipation of death.

Section 164.502(g)—Personal Representatives

In the proposed rule we defined ''individual'' to include certain persons who were authorized to act on behalf of the person who is the subject of the protected health information. For adults and emancipated minors, the NPRM provided that ''individual'' includes a legal representative to the extent to which applicable law permits such legal representative to exercise the individual's rights in such contexts. With respect to unemancipated minors, we proposed that the definition of ''individual'' include a parent, guardian, or person acting *in loco parentis*, (hereinafter referred to as ''parent'') except when an unemancipated minor obtained health care services without the consent of, or notification to, a parent. Under the proposed rule, if a minor obtained health care services under these conditions, the minor would have had the exclusive rights of an individual with respect to the protected health information related to such health care services.

In the final rule, the definition of ''individual'' is limited to the subject of the protected health information, which includes unemancipated minors and other individuals who may lack capacity to act on their own behalf. We remove from the definition of ''individual'' the provisions regarding legal representatives. The circumstances in which a representative must be treated as an individual for purposes of this rule are addressed in a separate standard titled ''personal representatives.'' (§ 164.502(g)). The standard regarding personal representatives incorporates some changes to the proposed provisions regarding legal representatives. In general, under the final regulation, the ''personal representatives'' provisions are directed at the more formal representatives, while § 164.510(b) addresses situations in which persons are informally acting on behalf of an individual.

With respect to adults or emancipated minors, we clarify that a covered entity must treat a person as a personal representative of an individual if such person is, under applicable law, authorized to act on behalf of the individual in making decisions related to health care. This includes a court-appointed guardian and a person with a power of attorney, as set forth in the NPRM, but may also include other persons. The authority of a personal representative under this rule is limited: the representative must be treated as the individual only to the extent that protected health information is relevant to the matters on which the personal representative is authorized to represent the individual. For example, if a person's authority to make health care decisions for an individual is limited to decisions regarding treatment for cancer, such person is a personal representative and must be treated as the individual with respect to protected health information related to the cancer treatment of the individual. Such a person is not the personal representative of the individual with respect to all protected health information about the individual, and therefore, a covered entity may not disclose protected health information that is not relevant to the cancer treatment to the person, unless otherwise permitted under the rule. We intend this provision to apply to persons empowered under state or other law to make health related decisions for an individual, whether or not the instrument or law granting such authority specifically addresses health information.

In addition, we clarify that with respect to an unemancipated minor, if under applicable law a parent may act on behalf of an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this rule with respect to protected health information relevant to such personal representation, with three exceptions. Under the general rule, in most circumstances the minor would not have the capacity to act as the individual, and the parent would be able to exercise rights and authorities on behalf of the minor. Under the exceptions to the rule on personal representatives of unemancipated minors, the minor, and not the parent, would be treated as the individual and able to exercise the rights and authorities of an individual under the rule. These exceptions occur if: (1) The minor consents to a health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative; (2) the minor may lawfully obtain such health care service without the consent of a parent, and the minor, a court, or another person authorized by law consents to such health care service; or (3) a parent assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service. We note that the definition of health care includes services, but we use ''health care service'' in this provision to clarify that the scope of the rights of minors under this rule is limited to the protected health information related to a particular service.

Under this provision, we do not provide a minor with the authority to act under the rule unless the state has given them the ability to obtain health care without consent of a parent, or the parent has assented. In addition, we defer to state law where the state authorizes or prohibits disclosure of protected health information to a parent. See part 160, subpart B, Preemption of State Law. This rule does not affect parental notification laws that permit or require disclosure of protected health information to a parent. However, the rights of a minor under this rule are not otherwise affected by such notification.

In the final rule, the provision regarding personal representatives of deceased individuals has been changed to clarify the provision. The policy has not changed substantively from the NPRM.

Finally, we added a provision in the final rule to permit covered entities to elect not to treat a person as a personal representative in abusive situations. Under this provision, a covered entity need not treat a person as a personal representative of an individual if the covered entity, in the exercise of professional judgment, decides that it is

not in the best interest of the individual to treat the person as the individual's personal representative and the covered entity has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person, or that treating such person as the personal representative could endanger the individual.

Section 164.502(g) requires a covered entity to treat a person that meets the requirements of a personal representative as the individual (with the exceptions described above). We note that disclosure of protected health information to a personal representative is mandatory under this rule only if disclosure to the individual is mandatory. Disclosure to the individual is mandatory only under §§ 164.524 and 164.528. Further, as noted above, the personal representative's rights are limited by the scope of its authority under other law. Thus, this provision does not constitute a general grant of authority to personal representatives.

We make disclosure to personal representatives mandatory to ensure that an individual's rights under §§ 164.524 and 164.528 are preserved even when individuals are incapacitated or otherwise unable to act for themselves to the same degree as other individuals. If the covered entity were to have the discretion to recognize a personal representative as the individual, there could be situations in which no one could invoke an individual's rights under these sections.

We continue to allow covered entities to use their discretion to disclose certain protected health information to family members, relatives, close friends, and other persons assisting in the care of an individual, in accordance with § 164.510(b). We recognize that many health care decisions take place on an informal basis, and we permit disclosures in certain circumstance to permit this practice to continue. Health care providers may continue to use their discretion to address these informal situations.

Section 164.502(h)—Confidential Communications

In the NPRM, we did not directly address the issue of whether an individual could request that a covered entity restrict the manner in which it communicated with the individual. The NPRM did provide individuals with the right to request that health care providers restrict uses and disclosures of protected health information for treatment, payment and health operations, but providers were not required to agree to such a restriction.

In the final rule, we require covered providers to accommodate reasonable requests by patients about how the covered provider communicates with the individual. For example, an individual who does not want his or her family members to know about a certain treatment may request that the provider communicate with the individual at his or her place of employment, or to send communications to a designated address. Covered providers must accommodate the request unless it is unreasonable. Similarly, the final rule permits individuals to request that health plans communicate with them by alternative means, and the health plan must accommodate such a request if it is reasonable and the individual states that disclosure of the information could endanger the individual. The specific provisions relating to confidential communications are in § 164.522.

Section 164.502(i)—Uses and Disclosures Consistent with Notice

We proposed to prohibit covered entities from using or disclosing protected health information in a manner inconsistent with their notice of information practices. We retain this provision in the final rule. See § 164.520 regarding notice content and distribution requirements.

Section 164.502(j)—Disclosures by Whistleblowers and Workforce Member Crime Victims

Disclosures by Whistleblowers

In § 164.518(c)(4) of the NPRM we addressed the issue of whistleblowers by proposing that a covered entity not be held in violation of this rule because a member of its workforce or a person associated with a business associate of the covered entity used or disclosed protected health information that such person believed was evidence of a civil or criminal violation, and any disclosure was: (1) Made to relevant oversight agencies or law enforcement or (2) made to an attorney to allow the attorney to determine whether a violation of criminal or civil law had occurred or to assess the remedies or actions at law that may be available to the person disclosing the information.

We included an extensive discussion on how whistleblower actions can further the public interest, including reference to the need in some circumstances to utilize protected health information for this purpose as well as reference to the *qui tam* provisions of the Federal False Claims Act.

In the final rule we retitle the provision and include it in § 164.502 to reflect the fact that these disclosures are not made by the covered entity and therefore this material does not belong in the section on safeguarding information against disclosure.

We retain the basic concept in the NPRM of providing protection to a covered entity for the good faith whistleblower action of a member of its workforce or a business associate. We clarify that a whistleblower disclosure by an employee, subcontractor, or other person associated with a business associate is considered a whistleblower disclosure of the business associate under this provision. However, in the final rule, we modify the scope of circumstances under which a covered entity is protected in whistleblower situations. A covered entity is not in violation of the requirements of this rule when a member of its workforce or a business associate of the covered entity discloses protected health information to: (i) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity; (ii) an appropriate health care accreditation organization; or (iii) an attorney, for the purpose of determining his or her legal options with respect to whistleblowing. We delete disclosures to a law enforcement official.

We expand the scope of this section to cover disclosures of protected health information to an oversight or accreditation organization for the purpose of reporting breaches of professional standards or problems with quality of care. The covered entity will not be in violation of this rule, provided that the disclosing individual believes in good faith that the covered entity has engaged in conduct which is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by the covered entity potentially endanger one or more patients, workers or the public. Since these provisions only relate to whistleblower actions in relation to the covered entity, disclosure of protected health information to expose malfeasant conduct by another person, such as knowledge gained during the course of treatment about an individual's illicit drug use, would not be protected activity.

We clarify that this section only applies to protection of a covered entity, based on the whistleblower action of a member of its workforce or business associates. Since the HIPAA legislation only applies to covered entities, not their workforces, it is beyond the scope of this rule to directly regulate the

whistleblower actions of members of a covered entity's workforce.

In the NPRM, we had proposed to require covered entities to apply sanctions to members of its workforce who improperly disclose protected health information. In this final rule, we retain this requirement in § 164.530(e)(1) but modify the proposed provision on sanctions to clarify that the sanctions required under this rule do not apply to workforce members of a covered entity for whistleblower disclosures.

Disclosures by Workforce Members Who Are Crime Victims

The proposed rule did not address disclosures by workforce members who are victims of a crime. In the final rule, we clarify that a covered entity is not in violation of the rule when a workforce member of a covered entity who is the victim of a crime discloses protected health information to law enforcement officials about the suspected perpetrator of the crime. We limit the amount of protected health information that may be disclosed to the limited information for identification and location described in § 164.512(f)(2).

We note that this provision is similar to the provision in § 164.512(f)(5), which permits a covered entity to disclose protected health information to law enforcement that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity. This provision differs in that it permits the disclosure even if the crime occurred somewhere other than on the premises of the covered entity. For example, if a hospital employee is the victim of an attack outside of the hospital, but spots the perpetrator sometime later when the perpetrator seeks medical care at the hospital, the workforce member who was attacked may notify law enforcement of the perpetrator's location and other identifying information. We do not permit, however, the disclosure of protected health information other than that described in § 164.512(f)(2).

Section 164.504—Uses and Disclosures—Organizational Requirements—Component Entities, Affiliated Entities, Business Associates and Group Health Plans

Section 164.504(a)–(c)—Health Care Component (Component Entities)

In the preamble to the proposed rule we introduced the concept of a ''component entity'' to differentiate the health care unit of a larger organization from the larger organization. In the proposal we noted that some organizations that are primarily involved in non-health care activities do provide health care services or operate health plans or health care clearinghouses. Examples included a school with an on-site health clinic and an employer that self administers a sponsored health plan. In such cases, the proposal said that the health care component of the entity would be considered the covered entity, and any release of information from that component to another office or person in the organization would be a regulated disclosure. We would have required such entities to create barriers to prevent protected health information from being used or disclosed for activities not authorized or permitted under the proposal.

We discuss group health plans and their relationships with plan sponsors below under ''Requirements for Group Health Plans.''

In the final rule we address the issue of differentiating health plan, covered health care provider and health care clearinghouse activities from other functions carried out by a single legal entity in paragraphs (a)–(c) of § 164.504. We have created a new term, ''hybrid entity'', to describe the situation where a health plan, health care provider, or health care clearinghouse is part of a larger legal entity; under the definition, a ''hybrid entity'' is ''a single legal entity that is a covered entity and whose covered functions are not its primary functions.'' The term ''covered functions'' is discussed above under § 164.501. By ''single legal entity'' we mean a legal entity, such as a corporation or partnership, that cannot be further differentiated into units with their own legal identities. For example, for purposes of this rule a multinational corporation composed of multiple subsidiary companies would not be a single legal entity, but a small manufacturing firm and its health clinic, if not separately incorporated, could be a single legal entity.

The health care component rules are designed for the situation in which the health care functions of the legal entity are not its dominant mission. Because some part of the legal entity meets the definition of a health plan or other covered entity, the legal entity as a whole could be required to comply with the rules below. However, in such a situation, it makes sense not to require the entire entity to comply with the requirements of the rules below, when most of its activities may have little or nothing to do with the provision of health care; rather, as a practical matter, it makes sense for such an entity to focus its compliance efforts on the component that is actually performing the health care functions. On the other hand, where most of what the covered entity does consist of covered functions, it makes sense to require the entity as a whole to comply with the rules. The provisions at §§ 164.504(a)–(c) provide that for a hybrid entity, the rules apply only to the part of the entity that is the health care component. At the same time, the lack of corporate boundaries increases the risk that protected health information will be used in a manner that would not otherwise be permitted by these rules. Thus, we require that the covered entity erect firewalls to protect against the improper use or disclosure within or by the organization. See § 164.504(c)(2).

The term ''primary functions'' in the definition of ''hybrid entity'' is not meant to operate with mathematical precision. Rather, we intend that a more common sense evaluation take place: Is most of what the covered entity does related to its health care functions? If so, then the whole entity should be covered. Entities with different insurance lines, if not separately incorporated, present a particular issue with respect to this analysis. Because the definition of ''health plan'' excludes many types of insurance products (in the exclusion under paragraph (2)(i) of the definition), we would consider an entity that has one or more of these lines of insurance in addition to its health insurance lines to come within the definition of ''hybrid entity,'' because the other lines of business constitute substantial parts of the total business operation and are required to be separate from the health plan(s) part of the business.

An issue that arises in the hybrid entity situation is what records are covered in the case of an office of the hybrid entity that performs support functions for both the health care component of the entity and for the rest of the entity. For example, this situation could arise in the context of a company with an onsite clinic (which we will assume is a covered health care provider), where the company's business office maintains both clinic records and the company's personnel records. Under the definition of the term ''health care component,'' the business office is part of the health care component (in this hypothetical, the clinic) ''to the extent that'' it is performing covered functions on behalf of the clinic involving the use or disclosure of protected health information that it receives from, creates or maintains for the clinic. Part of the business office, therefore, is part of the

health care component, and part of the business office is outside the health care component. This means that the non-health care component part of the business office is not covered by the rules below. Under our hypothetical, then, the business office would not be required to handle its personnel records in accordance with the rules below. The hybrid entity would be required to establish firewalls with respect to these record systems, to ensure that the clinic records were handled in accordance with the rules.

With respect to excepted benefits, the rules below operate as follows. (Excepted benefits include accident, disability income, liability, workers' compensation and automobile medical payment insurance.) Excepted benefit programs are excluded from the health care component (or components) through the definition of ''health plan.'' If a particular organizational unit performs both excepted benefits functions and covered functions, the activities associated with the excepted benefits program may not be part of the health care component. For example, an accountant who works for a covered entity with both a health plan and a life insurer would have his or her accounting functions performed for the health plan as part of the component, but not the life insurance accounting function. See § 164.504(c)(2)(iii). We require this segregation of excepted benefits because HIPAA does not cover such programs, policies and plans, and we do not permit any use or disclosure of protected health information for the purposes of operating or performing the functions of the excepted benefits without authorization from the individual, except as otherwise permitted in this rule.

In § 164.504(c)(2) we require covered entities with a health care component to establish safeguard policies and procedures to prevent any access to protected health information by its other organizational units that would not be otherwise permitted by this rule. We note that section 1173(d)(1)(B) of HIPAA requires policies and procedures to isolate the activities of a health care clearinghouse from a ''larger organization'' to prevent unauthorized access by the larger organization. This safeguard provision is consistent with the statutory requirement and extends to any covered entity that performs ''non-covered entity functions'' or operates or conducts functions of more than one type of covered entity.

Because, as noted, the covered entity in the hybrid entity situation is the legal entity itself, we state explicitly what is implicitly the case, that the covered entity (legal entity) remains responsible for compliance vis-a-vis subpart C of part 160. See § 164.504(c)(3)(i). We do this simply to make these responsibilities clear and to avoid confusion on this point. Also, in the hybrid entity situation the covered entity/legal entity has control over the entire workforce, not just the workforce of the health care component. Thus, the covered entity is in a position to implement policies and procedures to ensure that the part of its workforce that is doing mixed or non-covered functions does not impermissibly use or disclose protected health information. Its responsibility to do so is clarified in § 164.504(c)(3)(ii).

Section 164.504(d)—Affiliated Entities

Some legally distinct covered entities may share common administration of organizationally differentiated but similar activities (for example, a hospital chain). In § 164.504(d) we permit legally distinct covered entities that share common ownership or control to designate themselves, or their health care components, together to be a single covered entity. Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Such organizations may promulgate a single shared notice of information practices and a consent form. For example, a corporation with hospitals in twenty states may designate itself as a covered entity and, therefore, able to merge information for joint marketplace analyses. The requirements that apply to a covered entity also apply to an affiliated covered entity. For example, under the minimum necessary provisions, a hospital in one state could not share protected health information about a particular patient with another hospital if such a use is not necessary for treatment, payment or health care operations. The covered entities that together make up the affiliated covered entity are separately subject to liability under this rule. The safeguarding requirements for affiliated covered entities track the requirements that apply to health care components.

Section 164.504(e)—Business Associates

In the NPRM, we proposed to require a contract between a covered entity and a business associate, except for disclosures of protected health information by a covered entity that is a health care provider to another health care provider for the purposes of consultation or referral. A covered entity would have been in violation of this rule if the covered entity knew or reasonably should have known of a material breach of the contract by a business associate and it failed to take reasonable steps to cure the breach or terminate the contract. We proposed in the preamble that when a covered entity acted as a business associate to another covered entity, the covered entity that was acting as business associate also would have been responsible for any violations of the regulation.

We also proposed that covered health care providers receiving protected health information for consultation or referral purposes would still have been subject to this rule, and could not have used or disclosed such protected health information for a purpose other than the purpose for which it was received (*i.e.,* the consultation or referral). Further, we noted that providers making disclosures for consultations or referrals should be careful to inform the receiving provider of any special limitations or conditions to which the disclosing provider had agreed to impose (*e.g.,* the disclosing provider had provided notice to its patients that it would not make disclosures for research).

We proposed that business associates would not have been permitted to use or disclose protected health information in ways that would not have been permitted of the covered entity itself under these rules, and covered entities would have been required to take reasonable steps to ensure that protected health information disclosed to a business associate remained protected.

In the NPRM (proposed § 164.506(e)(2)) we would have required that the contractual agreement between a covered entity and a business associate be in writing and contain provisions that would:

- Prohibit the business associate from further using or disclosing the protected health information for any purpose other than the purpose stated in the contract.
- Prohibit the business associate from further using or disclosing the protected health information in a manner that would violate the requirements of this proposed rule if it were done by the covered entity.
- Require the business associate to maintain safeguards as necessary to ensure that the protected health information is not used or disclosed except as provided by the contract.
- Require the business associate to report to the covered entity any use or disclosure of the protected health information of which the business

associate becomes aware that is not provided for in the contract.

- Require the business associate to ensure that any subcontractors or agents to whom it provides protected health information received from the covered entity will agree to the same restrictions and conditions that apply to the business associate with respect to such information.
- Require the business associate to provide access to non-duplicative protected health information to the subject of that information, in accordance with proposed § 164.514(a).
- Require the business associate to make available its internal practices, books and records relating to the use and disclosure of protected health information received from the covered entity to the Secretary for the purposes of enforcing the provisions of this rule.
- Require the business associate, at termination of the contract, to return or destroy all protected health information received from the covered entity that the business associate still maintains in any form to the covered entity and prohibit the business associate from retaining such protected health information in any form.
- Require the business associate to incorporate any amendments or corrections to protected health information when notified by the covered entity that the information is inaccurate or incomplete.
- State that individuals who are the subject of the protected health information disclosed are intended to be third party beneficiaries of the contract.
- Authorize the covered entity to terminate the contract, if the covered entity determines that the business associate has violated a material term of the contract.

We also stated in the preamble to the NPRM that the contract could have included any additional arrangements that did not violate the provisions of this regulation.

We explained in the preamble to the NPRM that a business associate (including business associates that are covered entities) that had contracts with more than one covered entity would have had no authority to combine, aggregate or otherwise use for a single purpose protected health information obtained from more than one covered entity unless doing so would have been a lawful use or disclosure for each of the covered entities that supplied the protected health information that is being combined, aggregated or used. In addition, the business associate would have had to have been authorized through the contract or arrangement with each covered entity that supplied the protected health information to combine or aggregate the information. A covered entity would not have been permitted to obtain protected health information through a business associate that it could not otherwise obtain itself.

In the final rule we retain the overall approach proposed: covered entities may disclose protected health information to persons that meet the rule's definition of business associate, or hire such persons to obtain or create protected health information for them, only if covered entities obtain specified satisfactory assurances from the business associate that it will appropriately handle the information; the regulation specifies the elements of such satisfactory assurances; covered entities have responsibilities when such specified satisfactory assurances are violated by the business associate. We retain the requirement that specified satisfactory assurances must be obtained if a covered entity's business associate is also a covered entity. We note that a master business associate contract or MOU that otherwise meets the requirements regarding specified satisfactory assurances meets the requirements with respect to all the signatories.

A covered entity may disclose protected health information to a business associate, consistent with the other requirements of the final rule, as necessary to permit the business associate to perform functions and activities for or on behalf of the covered entity, or to provide the services specified in the business associate definition to or for the covered entity. As discussed below, a business associate may only use the protected health information it receives in its capacity as a business associate to a covered entity as permitted by its contract or agreement with the covered entity.

We do not attempt to directly regulate business associates, but pursuant to our authority to regulate covered entities we place restrictions on the flow of information from covered entities to non-covered entities. We add a provision to clarify that a violation of a business associate agreement by a covered entity that is a business associate of another covered entity constitutes a violation of this rule.

In the final rule, we make significant changes to the requirements regarding business associates. As explained below in more detail: we make significant changes to the content of the required contractual satisfactory assurances; we include exceptions for arrangements that would otherwise meet the definition of business associate; we make special provisions for government agencies that by law cannot enter into contracts with one another or that operate under other legal requirements incompatible with some aspects of the required contractual satisfactory assurances; we provide a new mechanism for covered entities to hire a third party to aggregate data.

The final rule provides several exception to the business associate requirements, where a business associate relationship would otherwise exist. We substantially expand the exception for disclosure of protected health information for treatment. Rather than allowing disclosures without business associate assurances only for the purpose of consultation or referral, in the final rule we allow covered entities to make any disclosure of protected health information for treatment purposes to a health care provider without a business associate arrangement. This provision includes all activities that fall under the definition of treatment.

We do not require a business associate contract for a group health plan to make disclosures to the plan sponsor, to the extent that the health plan meets the applicable requirements of § 164.504(f).

We also include an exception for certain jointly administered government programs providing public benefits. Where a health plan that is a government program provides public benefits, such as SCHIP and Medicaid, and where eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or where the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and the joint activities are authorized by law, no business associate contract is required with respect to the collection and sharing of individually identifiable health information for the performance of the authorized functions by the health plan and the agency other than the agency administering the health plan. We note that the phrase ''government programs providing public benefits'' refers to programs offering benefits to specified members of the public and not to programs that offer benefits only to employees or retirees of government agencies.

We note that we do not consider a financial institution to be acting on behalf of a covered entity, and therefore no business associate contract is required, when it processes consumer-conducted financial transactions by debit, credit or other payment card,

clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care. A typical consumer-conducted payment transaction is when a consumer pays for health care or health insurance premiums using a check or credit card. In these cases, the identity of the consumer is always included and some health information (*e.g.,* diagnosis or procedure) may be implied through the name of the health care provider or health plan being paid. Covered entities that initiate such payment activities must meet the minimum necessary disclosure requirements described in the preamble to § 164.514.

In the final rule, we reduce the extent to which a covered entity must monitor the actions of its business associate and we make it easier for covered entities to identify the circumstances that will require them to take actions to correct a business associate's material violation of the contract, in the following ways. We delete the proposed language requiring covered entities to ''take reasonable steps to ensure'' that each business associate complies with the rule's requirements. Additionally, we now require covered entities to take reasonable steps to cure a breach or terminate the contract for business associate behaviors only if they know of a material violation by a business associate. In implementing this standard, we will view a covered entity that has substantial and credible evidence of a violation as knowing of such violation. While this standard relieves the covered entity of the need to actively monitor its business associates, a covered entity nonetheless is expected to investigate when they receive complaints or other information that contain substantial and credible evidence of violations by a business associate, and it must act upon any knowledge of such violation that it possesses. We note that a whistleblowing disclosure by a business associate of a covered entity that meets the requirements of § 164.502(j)(1) does not put the covered entity in violation of this rule, and the covered entity has no duty to correct or cure, or to terminate the relationship.

We also qualify the requirement for terminating contracts with non-compliant business associates. The final rule still requires that the business associate contract authorize the covered entity to terminate the contract, if the covered entity determines that the business associate has violated a material term of the contract, and it requires the covered entity to terminate the contract if steps to cure such a material breach fail. The rule now stipulates, however, that if the covered entity is unable to cure a material breach of the business associate's obligation under the contract, it is expected to terminate the contract, when feasible. This qualification has been added to accommodate circumstances where terminating the contract would be unreasonably burdensome on the covered entity, such as when there are no viable alternatives to continuing a contract with that particular business associate. It does not mean, for instance, that the covered entity can choose to continue the contract with a non-compliant business associate merely because it is more convenient or less costly than contracts with other potential business associates. We also require that if a covered entity determines that it is not feasible to terminate a non-compliant business associate, the covered entity must notify the Secretary.

We retain all of the requirements for a business associate contract that were listed in proposed § 164.506(e)(2), with some modifications. See § 164.504(e)(2).

We retain the requirement that the business associate contract must provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law. We do not mean by this requirement that the business associate contract must specify each and every use and disclosure of protected health information permitted to the business associate. Rather, the contract must state the purposes for which the business associate may use and disclose protected health information, and must indicate generally the reasons and types of persons to whom the business associate may make further disclosures. For example, attorneys often need to provide information to potential witnesses, opposing counsel, and others in the course of their representation of a client. The business associate contract pursuant to which protected health information is provided to its attorney may include a general statement permitting the attorney to disclose protected health information to these types of people, within the scope of its representation of the covered entity.

We retain the requirement that a business associate contract may not authorize a business associate to use or further disclose protected health information in a manner that would violate the requirements of this subpart if done by the covered entity, but we add two exceptions. First, we permit a covered entity to authorize a business associate to use and disclose protected health information it receives in its capacity as a business associate for its proper management and administration and to carry out its legal responsibilities. The contract must limit further disclosures of the protected health information for these purposes to those that are required by law and to those for which the business associate obtains reasonable assurances that the protected health information will be held confidentially and that it will be notified by the person to whom it discloses the protected health information of any breaches of confidentiality.

Second, we permit a covered entity to authorize the business associate to provide data aggregation services to the covered entity. As discussed above in § 164.501, data aggregation, with respect to protected health information received by a business associate in its capacity as the business associate of a covered entity, is the combining of such protected health information by the business associate with protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit the creation of data for analyses that relate to the health care operations of the respective covered entities. We added this service to the business associate definition to clarify the ability of covered entities to contract with business associates to undertake quality assurance and comparative analyses that involve the protected health information of more than one contracting covered entity. We except data aggregation from the general requirement that a business associate contract may not authorize a business associate to use or further disclose protected health information in a manner that would violate the requirements of this subpart if done by the covered entity in order to permit the combining or aggregation of protected health information received in its capacity as a business associate of different covered entities when it is performing this service. In many cases, the combining of this information for the respective health care operations of the covered entities is not something that the covered entities could do—a covered entity cannot generally disclose protected health information to another covered entity for the disclosing covered entity's health care operations. However, we permit covered entities that enter into business associate contracts with a business associate for data aggregation to permit the business associate to combine or aggregate the protected health information they

disclose to the business associate for their respective health care operations.

We note that there may be other instances in which a business associate may combine or aggregate protected health information received in its capacity as a business associate of different covered entities, such as when it is performing health care operations on behalf of covered entities that participate in an organized health care arrangement. A business associate that is performing payment functions on behalf of different covered entities also may combine protected health information when it is necessary, such as when the covered entities share financial risk or otherwise jointly bill for services.

In the final rule we clarify that the business associate contract must require the business associate to make available protected health information for amendment and to incorporate such amendments. The business associate contract must also require the business associate to make available the information required to provide an accounting of disclosures. We provide more flexibility to the requirement that all protected health information be returned by the business associate upon termination of the contract. The rule now stipulates that if feasible, the protected health information should be destroyed or returned at the end of a contract. Accordingly, a contract with a business associate must state that if there are reasons that the return or destruction of the information is not feasible and the information must be retained for specific reasons and uses, such as for future audits, privacy protections must continue after the contract ends, for as long as the business associate retains the information. The contract also must state that the uses of information after termination of the contract must be limited to the specific set of uses or disclosures that make it necessary for the business associate to retain the information.

We also remove the requirement that business associate contracts contain a provision stating that individuals whose protected health information is disclosed under the contract are intended third-party beneficiaries of the contract. Third party beneficiary or similar responsibilities may arise under these business associate arrangements by operation of state law; we do not intend in this rule to affect the operation of such state laws.

We modify the requirement that a business associate contract require the business associate to ensure that agents abide by the provisions of the business associate contract. We clarify that agents includes subcontractors, and we note that a business associate contract must make the business associate responsible for ensuring that any person to whom it delegates a function, activity or service which is within its business associate contract with the covered entity agrees to abide by the restrictions and conditions that apply to the business associate under the contract. We note that a business associate will need to consider the purpose for which protected health information is being disclosed in determining whether the recipient must be bound to the restrictions and conditions of the business associate contract. When the disclosure is a delegation of a function, activity or service that the business associate has agreed to perform for a covered entity, the recipient who undertakes such a function steps into the shoes of the business associate and must be bound to the restrictions and conditions. When the disclosure is to a third party who is not performing business associate functions, activities or services for on behalf of the covered entity, but is the type of disclosure that the covered entity itself could make without giving rise to a business associate relationship, the business associate is not required to ensure that the restrictions or conditions of the business associate contract are maintained.

For example, if a business associate acts as the billing agent of a health care provider, and discloses protected health information on behalf of the hospital to health plans, the business associate has no responsibility with respect to further uses or disclosures by the health plan. In the example above, where a covered entity has a business associate contract with a lawyer, and the lawyer discloses protected health information to an expert witness in preparation for litigation, the lawyer again would have no responsibility under this subpart with respect to uses or disclosures by the expert witness, because such witness is not undertaking the functions, activities or services that the business associate lawyer has agreed to perform. However, if a covered entity contracts with a third party administrator to provide claims management, and the administrator delegates management of the pharmacy benefits to a third party, the business associate third party administrator must ensure that the pharmacy manager abides by the restrictions and conditions in the business associate contract between the covered entity and the third party administrator.

We provide in § 164.504(c)(3) several methods other than a business associate contract that will satisfy the requirement for satisfactory assurances under this section. First, when a government agency is a business associate of another government agency that is a covered entity, we permit memorandum of understanding between the agencies to constitute satisfactory assurance for the purposes of this rule, if the memorandum accomplishes each of the objectives of the business associate contract. We recognize that the relationships of government agencies are often organized as a matter of law, and that it is not always feasible for one agency to contract with another for all of the purposes provided for in this section. We also recognize that it may be incorrect to view one government agency as ''acting on behalf of'' the other government agency; under law, each agency may be acting to fulfill a statutory mission. We note that in some instances, it may not be possible for the agencies to include the right to terminate the arrangement because the relationship may be established under law. In such instances, the covered entity government agency would need to fulfill the requirement to report known violations of the memorandum to the Secretary.

Where the covered entity is a government agency, we consider the satisfactory assurances requirement to be satisfied if other law contains requirements applicable to the business associate that accomplish each of the objectives of the business associate contract. We recognize that in some cases, covered entities that are government agencies may be able to impose the requirements of this section directly on the persons acting as their business associates. We also recognize that often one government agency is acting as a business associate of another government agency, and either party may have the legal authority to establish the requirements of this section by regulation. We believe that imposing these requirements directly on business associates provides greater protection than we can otherwise provide under this section, and so we recognize such other laws as sufficient to substitute for a business associate contract.

We also recognize that there may be some circumstances where the relationship between covered entities and business associates is otherwise mandated by law. In the final rule, we provide that where a business associate is required by law to act as a business associate to a covered entity, the covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without

meeting the requirement to have a business associate contract (or, in the case of government agencies, a memorandum of understanding or law pertaining to the business associate) if it makes a good faith attempt the obtain satisfactory assurances required by this section and, if unable to do so, documents the attempt and the reasons that such assurances cannot be obtained. This provision addresses situations where law requires one party to act as the business associate of another party. The fact that the parties have contractual obligations that may be enforceable is not sufficient to meet the required by law test in this provision.

This provision recognizes that in some instances the law requires that a government agency act as a business associate of a covered entity. For example, the United States Department of Justice is required by law to defend tort suits brought against certain covered entities; in such circumstances, however, the United States, and not the individual covered entity, is the client and is potentially liable. In such situations, covered entities must be able to disclose protected health information needed to carry out the representation, but the particular requirements that would otherwise apply to a business associate relationship may not be possible to obtain. Subsection (iii) makes clear that, where the relationship is required by law, the covered entity complies with the rule if it attempts, in good faith, to obtain satisfactory assurances as are required by this paragraph and, if such attempt fails, documents the attempts and the reasons that such assurances cannot be obtained.

The operation of the final rule maintains the construction discussed in the preamble to the NPRM that a business associate (including a business associate that is a covered entity) that has business associate contracts with more than one covered entity generally may not use or disclose the protected health information that it creates or receives in its capacity as a business associate of one covered entity for the purposes of carrying out its responsibilities as a business associate of another covered entity, unless doing so would be a lawful use or disclosure for each of the covered entities and the business associate's contract with each of the covered entities permits the business associate to undertake the activity. For example, a business associate performing a function under health care operations on behalf of an organized health care arrangement would be permitted to combine or aggregate the protected health information obtained from covered entities participating in the arrangement to the extent necessary to carry out the authorized activity and in conformance with its business associate contracts. As described above, a business associate providing data aggregation services to different covered entities also could combine and use the protected health information of the covered entities to assist with their respective health care operations. A covered entity that is undertaking payment activities on behalf of different covered entities also may use or disclose protected health information obtained as a business associate of one covered entity when undertaking such activities as a business associate of another covered entity where the covered entities have authorized the activities and where they are necessary to secure payment for the entities. For example, when a group of providers share financial risk and contract with a business associate to conduct payment activities on their behalf, the business associate may use the protected health information received from the covered entities to assist them in managing their shared risk arrangement.

Finally, we note that the requirements imposed by this provision are intended to extend privacy protection to situations in which a covered entity discloses substantial amounts of protected health information to other persons so that those persons can perform functions or activities on its behalf or deliver specified services to it. A business associate contract basically requires the business associate to maintain the confidentiality of the protected health information that it receives and generally to use and disclose such information for the purposes for which it was provided. This requirement does not interfere with the relationship between a covered entity and business associate, or require the business associate to subordinate its professional judgment to that of a covered entity. Covered entities may rely on the professional judgment of their business associates as to the type and amount of protected health information that is necessary to carry out a permitted activity. The requirements of this provision are aimed at securing the continued confidentiality of protected health information disclosed to third parties that are serving the covered entity's interests.

Section 164.504(f)—Group Health Plans

Covered entities under HIPAA include health care clearinghouses, health care providers and health plans. Specifically included in the definition of ''health plan'' are group health plans (as defined in section 2791(a) of the Public Health Service Act) with 50 or more participants or those of any size that are administered by an entity other than the employer who established and maintains the plan. These group health plans may be fully insured or self-insured. Neither employers nor other group health plan sponsors are defined as covered entities. However, employers and other plan sponsors—particularly those sponsors with self-insured group health plans—may perform certain functions that are integrally related to or similar to the functions of group health plans and, in carrying out these functions, often require access to individual health information held by the group health plan.

Most group health plans are also regulated under the Employee Retirement Income Security Act of 1974 (ERISA). Under ERISA, a group health plan must be a separate legal entity from its plan sponsor. ERISA-covered group health plans usually do not have a corporate presence, in other words, they may not have their own employees and sometimes do not have their own assets (*i.e.,* they may be fully insured or the benefits may be funded through the general assets of the plan sponsor, rather than through a trust). Often, the only tangible evidence of the existence of a group health plan is the contractual agreement that describes the rights and responsibilities of covered participants, including the benefits that are offered and the eligible recipients.

ERISA requires the group health plan to identify a ''named fiduciary,'' a person responsible for ensuring that the plan is operated and administered properly and with ultimate legal responsibility for the plan. If the plan documents under which the group health plan was established and is maintained permit, the named fiduciary may delegate certain responsibilities to trustees and may hire advisors to assist it in carrying out its functions. While generally the named fiduciary is an individual, it may be another entity. The plan sponsor or employees of the plan sponsor are often the named fiduciaries. These structural and operational relationships present a problem in our ability to protect health information from being used inappropriately in employment-related decisions. On the one hand, the group health plan, and any health insurance issuer or HMO providing health insurance or health coverage to the group health plan, are covered entities under the regulation and may only disclose protected health information as authorized under the

regulation or with individual consent. On the other hand, plan sponsors may need access to protected health information to carry out administration functions on behalf of the plan, but under circumstances in which securing individual consent is impractical. We note that we sometimes refer in the rule and preamble to health insurance issuers and HMOs that provide health insurance or health coverage to a group health plan as health insurance issuers or HMOs with respect to a group health plan.

The proposed rule used the health care component approach for employers and other plan sponsors. Under this approach, only the component of an employer or other plan sponsor would be treated as a covered entity. The component of the plan sponsor would have been able to use protected health information for treatment, payment, and health care operations, but not for other purposes, such as discipline, hiring and firing, placement and promotions. We have modified the final rule in a number of ways.

In the final rule, we recognize plan sponsors' legitimate need for health information in certain situations while, at the same time, protecting health information from being used for employment-related functions or for other functions related to other employee benefit plans or other benefits provided by the plan sponsor. We do not attempt to directly regulate employers or other plan sponsors, but pursuant to our authority to regulate health plans, we place restrictions on the flow of information from covered entities to non-covered entities.

The final rule permits group health plans, and allows them to authorize health insurance issuers or HMOs with respect to the group health plan, to disclose protected health information to plan sponsors if the plan sponsors voluntarily agree to use and disclose the information only as permitted or required by the regulation. The information may be used only for plan administration functions performed on behalf of the group health plan which are specified in plan documents. The group health plan is not required to have a business associate contract with the plan sponsor to disclose the protected health information or allow the plan sponsor to create protected health information on its behalf, if the conditions of § 164.504(e) are met.

In order for the group health plan to disclose protected health information to a plan sponsor, the plan documents under which the plan was established and is maintained must be amended to: (1) Describe the permitted uses and disclosures of protected health information; (2) specify that disclosure is permitted only upon receipt of a certification from the plan sponsor that the plan documents have been amended and the plan sponsor has agreed to certain conditions regarding the use and disclosure of protected health information; and (3) provide adequate firewalls to: identify the employees or classes of employees who will have access to protected health information; restrict access solely to the employees identified and only for the functions performed on behalf of the group health plan; and provide a mechanism for resolving issues of noncompliance.

Any employee of the plan sponsor who receives protected health information for payment, health care operations or other matters related to the group health plan must be identified in the plan documents either by name or function. We assume that since individuals employed by the plan sponsor may change frequently, the group health plan would likely describe such individuals in a general manner. Any disclosure to employees or classes of employees not identified in the plan documents is not a permissible disclosure. To the extent a group health plan does have its own employees separate from the plan sponsor's employees, as the workforce of a covered entity (*i.e.* the group health plan), they also are bound by the permitted uses and disclosures of this rule.

The certification that must be given to the group health plan must state that the plan sponsor agrees to: (1) Not use or further disclose protected health information other than as permitted or required by the plan documents or as required by law; (2) ensure that any subcontractors or agents to whom the plan sponsor provides protected health information agree to the same restrictions; (3) not use or disclose the protected health information for employment-related actions; (4) report to the group health plan any use or disclosure that is inconsistent with the plan documents or this regulation; (5) make the protected health information accessible to individuals; (6) allow individuals to amend their information; (7) provide an accounting of its disclosures; (8) make its practices available to the Secretary for determining compliance; (9) return and destroy all protected health information when no longer needed, if feasible; and (10) ensure that the firewalls have been established.

We have included this certification requirement in part, as a way to reduce the burden on health insurance issuers and HMOs. Without a certification, health insurance issuers and HMOs would need to review the plan documents in order to ensure that the amendments have been made before they could disclose protected health information to plan sponsors. The certification, however, is a simple statement that the amendments have been made and that the plan sponsor has agreed to certain restrictions on the use and disclosure of protected health information. The receipt of the certification therefore, is sufficient basis for the health insurance issuer or HMO to disclose protected health information to the plan sponsor.

Many activities included in the definitions of health care operations and payment are commonly referred to as plan administration functions in the ERISA group health plan context. For purposes of this rule, plan administration activities are limited to activities that would meet the definition of payment or health care operations, but do not include functions to modify, amend, or terminate the plan or solicit bids from prospective issuers. Plan administration functions include quality assurance, claims processing, auditing, monitoring, and management of carve-out plans—such as vision and dental. Under the final rule, ''plan administration'' does not include any employment-related functions or functions in connection with any other benefits or benefit plans, and group health plans may not disclose information for such purposes absent an authorization from the individual. For purposes of this rule, enrollment functions performed by the plan sponsor on behalf of its employees are not considered plan administration functions.

Plan sponsors have access to protected health information only to the extent group health plans have access to protected health information and plan sponsors are permitted to use or disclose protected health information only as would be permitted by group health plans. That is, a group health plan may permit a plan sponsor to have access to or to use protected health information only for purposes allowed by the regulation.

As explained above, where a group health plan purchases insurance or coverage from a health insurance issuer or HMO, the provision of insurance or coverage by the health insurance issuer or HMO to the group health plan does not make the health insurance issuer or HMO a business associate. In such case, the activities of the health insurance issuer or HMO are on their own behalf and not on the behalf of the group

health plan. We note that where a group health plan contracts with a health insurance issuer or HMO to perform functions or activities or to provide services that are in addition to or not directly related to the provision of insurance, the health insurance issuer or HMO may be a business associate with respect to those additional functions, activities, or services. In addition, group health plans that provide health benefits only through an insurance contract and do not create, maintain, or receive protected health information (except for summary information described below or information that merely states whether an individual is enrolled in or has been disenrolled from the plan) do not have to meet the notice requirements of § 164.520 or the administrative requirements of § 164.530, except for the documentation requirement in § 164.530(j), because these requirements are satisfied by the issuer or HMO that is providing benefits under the group health plan. A group health plan, however, may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor unless the notice required in 164.520 indicate such disclosure may occur.

The final rule also permits a health plan that is providing insurance to a group health plan to provide summary information to the plan sponsor to permit the plan sponsor to solicit premium bids from other health plans or for the purpose of modifying, amending, or terminating the plan. The rule provides that summary information is information that summarizes claims history, claims expenses, or types of claims experienced by individuals for whom the plan sponsor has provided health benefits under a group health plan, provided that specified identifiers are not included. Summary information may be disclosed under this provision even if it does not meet the definition of de-identified information. As part of the notice requirements in § 164.520, health plans must inform individuals that they may disclose protected health information to plan sponsors. The provision to allow summaries of claims experience to be disclosed to plan sponsors that purchase insurance will allow them to shop for replacement coverage, and get meaningful bids from prospective issuers. It also permits a plan sponsor to get summary information as part of its consideration of whether or not to change the benefits that are offered or employees or whether or not to terminate a group health plan.

We note that a plan sponsor may perform enrollment functions on behalf of its employees without meeting the conditions above and without using the standard transactions described in the Transactions Rule.

Section 164.504(g)—Multiple Covered Function Entities

Although not addressed in the proposed rule, this final rule also recognizes that a covered entity may as a single legal entity, affiliated entity, or other arrangement combine the functions or operations of health care providers, health plans and health care clearinghouses (for example, integrated health plans and health care delivery systems may function as both health plans and health care providers). The rule permits such covered entities to use or disclose the protected health information of its patients or members for all covered entity functions, consistent with the other requirements of this rule. The health care component must meet the requirements of this rule that apply to a particular type of covered entity when it is functioning as that entity; *e.g.,* when a health care component is operating as a health care provider it must meet the requirements of this rule applicable to a health care provider. However, such covered entities may not use or disclose the protected health information of an individual who is not involved in a particular covered entity function for that function, and such information must be segregated from any joint information systems. For example, an HMO may integrate data about health plan members and clinic services to members, but a health care system may not share information about a patient in its hospital with its health plan if the patient is not a member of the health plan.

Section 164.506—Uses and Disclosures for Treatment, Payment, and Health Care Operations

Introduction: ''Consent'' versus ''Authorization''

In the proposed rule, we used the term ''authorization'' to describe the individual's written permission for a covered entity to use and disclose protected health information, regardless of the purpose of the use or disclosure. Authorization would have been required for all uses and disclosures that were not otherwise permitted or required under the NPRM.

We proposed to permit covered entities, subject to limited exceptions for psychotherapy notes and research information unrelated to treatment, to use and disclose protected health information to carry out treatment, payment, and health care operations without authorization. See proposed § 164.506(a)(1).

We also proposed to prohibit covered entities from requiring individuals to sign authorizations for uses and disclosures of protected health information for treatment, payment, and health care operations, unless required by other applicable law. See proposed § 164.508(a)(iv). We instead proposed requiring covered entities to produce a notice describing their information practices, including practices with respect to uses and disclosures to carry out treatment, payment, and health care operations.

In the final rule, we retain the requirement for covered entities to obtain the individual's written permission (an ''authorization'') for uses and disclosures of protected health information that are not otherwise permitted or required under the rule. However, under the final rule, we add a second type of written permission for use or disclosure of protected health information: a ''consent'' for uses and disclosures to carry out treatment, payment, and health care operations. In the final rule, we permit, and in some cases require, covered entities to obtain the individual's written permission for the covered entity to use or disclose protected health information other than psychotherapy notes to carry out treatment, payment, and health care operations. We refer to this written permission as a ''consent.''

The ''consent'' and the ''authorization'' do not overlap. The requirement to obtain a ''consent'' applies in different circumstances than the requirement to obtain an authorization. In content, a consent and an authorization differ substantially from one another.

As described in detail below, a ''consent'' allows use and disclosure of protected health information only for treatment, payment, and health care operations. It is written in general terms and refers the individual to the covered entity's notice for further information about the covered entity's privacy practices. It allows use and disclosure of protected health information by the covered entity seeking the consent, not by other persons. Most persons who obtain a consent will be health care providers; health plans and health care clearinghouses may also seek a consent. The consent requirements appear in § 164.506 and are described in this section of the preamble.

With a few exceptions, an ''authorization'' allows use and disclosure of protected health information for purposes other than treatment, payment, and health care

operations. In order to make uses and disclosures that are not covered by the consent requirements and not otherwise permitted or required under the final rule, covered entities must obtain the individual's ''authorization.'' An ''authorization'' must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. In some instances, a covered entity may not refuse to treat or cover individuals based on the fact that they refuse to sign an authorization. See § 164.508 and the corresponding preamble discussion regarding authorization requirements.

Section 164.506(a)—Consent Requirements

We make significant changes in the final rule with respect to uses and disclosures of protected health information to carry out treatment, payment, and health care operations. We do not prohibit covered entities from seeking an individual's written permission for use or disclosure of protected health information to carry out treatment, payment, or health care operations.

Except as described below, we instead require covered health care providers to obtain the individual's consent prior to using or disclosing protected health information to carry out treatment, payment, or health care operations. If the covered provider does not obtain the individual's consent, the provider is prohibited from using or disclosing protected health information about the individual for purposes of treating the individual, obtaining payment for health care delivered to the individual, or for the provider's health care operations. See § 164.506(a)(1).

We except two types of health care providers from this consent requirement. First, covered health care providers that have an indirect treatment relationship with an individual are not required to obtain the individual's consent prior to using or disclosing protected health information about the individual to carry out treatment, payment, and health care operations. An ''indirect treatment relationship'' is defined in § 164.501 and described in the corresponding preamble. These providers may use and disclose protected health information as otherwise permitted under the rule and consistent with their notice of privacy practices (see § 164.520 regarding notice requirements and § 164.502(i) regarding requirements to adhere to the notice). For example, a covered provider that provides consultation services to another provider without seeing the patient would have an indirect treatment relationship with that patient and would not be required to obtain the patient's consent to use protected health information about the patient for the consultation. These covered providers are, however, permitted to obtain consent, as described below.

Second, covered health care providers that create or receive protected health information in the course of providing health care to inmates of a correctional institution are not required to obtain the inmate's consent prior to using or disclosing protected health information about the inmate to carry out treatment, payment, and health care operations. See § 164.501 and the corresponding preamble discussion regarding the definitions of ''correctional institution'' and ''inmate.'' These providers may use and disclose protected health information as otherwise permitted under the rule. These providers are permitted, however, to obtain consent, as described below.

In addition, we permit covered health care providers to use and disclose protected health information, without consent, to carry out treatment, payment, and health care operations, if the protected health information was created or received in certain treatment situations. In the treatment situations described in § 164.506(a)(3) and immediately below, the covered health care provider must attempt to obtain the individual's consent. If the covered provider is unable to obtain consent, but documents the attempt and the reason consent was not obtained, the covered provider may, without consent, use and disclose the protected health information resulting from the treatment as otherwise permitted under the rule. All other protected health information about that individual that the covered health care provider creates or receives, however, is subject to the consent requirements.

This exception to the consent requirement applies to protected health information created or received in any of three treatment situations. First, the exception applies to protected health information created or received in emergency treatment situations. In these situations, covered providers must attempt to obtain the consent as soon as reasonably practicable after the delivery of the emergency treatment. Second, the exception applies to protected health information created or received in situations where the covered health care provider is required by law to treat the individual (for example, certain publicly funded providers) and the covered health care provider attempts to obtain such consent. Third, the exception applies to protected health information created or received in treatment situations where there are substantial barriers to communicating with the individual and, in the exercise of professional judgment, the covered provider clearly infers from the circumstances the individual's consent to receive treatment. For example, there may be situations in which a mentally incapacitated individual seeks treatment from a health care provider but is unable to provide informed consent to undergo such treatment and does not have a personal representative available to provide such consent on the individual's behalf. If the covered provider, in her professional judgment, believes she can legally provide treatment to that individual, we also permit the provider to use and disclose protected health information resulting from the treatment without the individual's consent. We intend covered health care providers that legally provide treatment without the individual's consent to that treatment to be able to use and disclose protected health information resulting from that treatment to carry out treatment, payment, or health care operations without obtaining the individual's consent for such use or disclosure. We do not intend to impose unreasonable barriers to individuals' ability to receive, and health care providers' ability to provide, health care.

Under § 164.506(a)(4), covered health care providers that have an indirect treatment relationship with an individual, as well as health plans and health care clearinghouses, may elect to seek consent for their own uses and disclosures to carry out treatment, payment, and health care operations. If such a covered entity seeks consent for these purposes, the consent must meet the minimum requirements described below.

If a covered health care provider with an indirect treatment relationship, a health plan, or a health care clearinghouse does not seek consent, the covered entity may use or disclose protected health information to carry out treatment, payment, and health care operations as otherwise permitted under the rule and consistent with its notice of privacy practices (see § 164.520 regarding notice requirements and § 164.502(i) regarding requirements to adhere to the notice).

If a covered health care provider with an indirect treatment relationship, a health plan, or a health care clearinghouse does ask an individual to sign a consent, and the individual does not do so, the covered entity is