

BACKGROUND INFORMATION FOR COMMITTEE MEMBERS **(Written by Laura Levit)**

Overview of HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was passed on August 21, 1996. HIPAA was intended to make healthcare delivery more efficient, and to increase the number of Americans with health insurance coverage. These objectives were achieved through three main provisions of the Act: 1) the portability provisions, 2) the tax provisions and 3) the administrative simplification provisions.

Portability and Tax Provisions

Prior to the passage of HIPAA, many people were afraid to switch jobs or change employers out of fear that a preexisting medical condition would disqualify them from receiving health insurance coverage from a new employer. The portability provisions of HIPAA addressed this concern, and decreased the possibility that an individual would lose health care coverage when changing to a new employer's health plan. The portability provisions also change the rules of insurance to make it easier for individuals to purchase health insurance independent from their employer. This was intended to increase the number of unemployed or self-employed individuals with health insurance.

Similar to the goals of the portability provisions of HIPAA, the tax provisions of HIPAA were also intended to make it easier for individuals to maintain health insurance. The tax provisions achieved this goal by modifying existing tax laws to make health insurance more affordable. HIPAA does not regulate the price of health insurance. Rather, it relies on tax breaks and other tax incentives to reduce health care costs (Chaikind, Hearne et al. 2005).

Administrative Simplification Provisions

The administrative simplification provisions of HIPAA instructed the Secretary of the Department of Health and Human Services (HHS) to issue several regulations concerning the use of the electronic transmission of health information. These sections of HIPAA were included in the final version of HIPAA because of the lobbying efforts of health plans. Health plans went to congress requesting that federal legislation be developed in this area. The use of electronic health information was expanding in the early 1990's, and the health care industry was unable to standardize the process and use of electronic health information without federal action.¹ As a result, the administrative simplification provisions were created by Congress at the request of the health care industry to streamline the use of electronic health information within the health care system.

Among the sets of regulations mandated by the administrative simplification provisions of HIPAA are the security standards. HIPAA instructed the Secretary of HHS to develop nationwide security standards and safeguards for the use of electronic health care information. The resulting HHS regulations spell out specific administrative,

¹ Personal Communication, Marcy Wilder, Partner, Hogan and Hartson, March 17, 2007.

technical, and physical security procedures that health plans and providers must incorporate into their operations to prevent unauthorized access, use and disclosure of protected health information (Centers_for_Medicare_and_Medicaid_Services 2005). HHS published the final HIPAA Security Rule in the Federal Register on February 20, 2003. Health plans and providers were required to be in compliance with these measures by April 21, 2005.

In addition to requiring the Secretary of HHS to develop standards for the security of electronic health information, the administrative simplification provisions of HIPAA also directed the Secretary to develop standards for unique health identifiers for patients, employers, health plans, and providers. Unique health identifiers are national numbers that are used to identify the individual or organization in standard health transactions. The Centers for Medicare and Medicaid Services (CMS) has issued standards for the unique health identifiers for employers and providers, and unique health identifiers for health plans are under development. However, Congress has prevented CMS from implementing a standard for the unique health identifier for patients, by inserting language into the annual appropriations bill every year since HIPAA was enacted (Chaikind, Hearne et al. 2005)

Finally, the administrative simplification provisions of HIPAA provided for the creation of privacy standards for the protection of personally identifiable medical information. As mentioned above, the administrative simplification provisions were incorporated into HIPAA for the purpose of standardizing the use of electronic health information. Privacy protections were only a secondary concern. However, congress recognized that advances in electronic technology could erode the privacy of health information, and included the privacy provision in HIPAA (Institute_of_Medicine 2006). According to the American Health Information Management Association an average of 150 people have access to a patient's medical records during the course of a typical hospitalization. Many of these people have legitimate reasons to access medical records, however, prior to the privacy provision in HIPAA there was no regulation on who could access medical records, what information could be accessed, and how the information found in medical records could be used in the health care system. In accordance with the administrative simplification provisions, HHS developed the Privacy Rule, which set out detailed rules regarding the types of uses and disclosures of individually identifiable medical information that are permitted by the health care industry. The Office for Civil Rights is the HHS agency responsible for enforcing the Privacy Rule.

The remainder of this paper will focus on the Privacy Rule, and how this regulation affects health research. First, the paper will start with a discussion of the development of privacy as a legal right, including information on why protecting informational privacy within the health care arena is important, and public opinions regarding the need for privacy protections of individually identifiable medical records. Second, the next sections of this paper will provide a detailed overview of the legislative history of HIPAA, and how the Privacy Rule has been interpreted and applied to health research. Third, there will be an explanation on how the Privacy Rule interacts with other federal rules regulating human subject research, and an examination of the rule's relationship to state privacy laws.

Fourth, there will be a brief update on the enforcement and number of violations to the Privacy Rule since its implementation. Fifth, the paper will give a detailed

summary of the recommendations provided to HHS on perceived problems associated with the Privacy Rule's regulation of research. This will include comments from the National Committee on Vital and Health Statistics, the Association of American Medical Colleges, and the Secretary's Advisory Committee on Human Research Protections. Finally, this paper will conclude with a discussion on the creation of a nationwide health information network, and the new types of privacy issues and concerns that the implementation of this technology will produce.

Background on Privacy Rights

Definition of Privacy

In order to understand the HIPAA Privacy Rule and the rights that this set of regulations is designed to protect, it is necessary to have an understanding of how privacy has developed and been defined in the legal context. One legal privacy scholar has defined privacy as “an individual's claim to limit access by others to some aspect of their personal life (Gostin 2008 (unpublished)).”

This broad definition of privacy can be broken down into a number of specific legal claims. Samuel Warren and Louis Brandeis co-authored a law review article in 1890, which created a new legal privacy right. They referred to this privacy interest as “the right to be let alone,” meaning an individual's right not to be viewed, photographed or observed without their knowledge or permission (Warren and Brandeis 1890). A second type of privacy that has been recognized in the law is decisional privacy. This type of privacy limits the extent that the government can influence individuals' decisions regarding their body and family (Solove, Rotenberg et al. 2005).

The legal privacy interest that the Privacy Rule is designed to protect is informational privacy. Alan Westin defined this privacy interest as “the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin 1967).” The original version of the Privacy Rule follows this definition of informational privacy, and quotes Westin (Department_of_Health_and_Human_Services 2000).”

It is important to understand that privacy has a different meaning from confidentiality and security. Privacy relates to the rights of individuals. Confidentiality, on the other hand, refers to types of information that must be used only for authorized purposes by authorized people (Turn and Ware 1976). The duty of confidentiality refers to “an individual's right to keep private, information exchanged in the course of an intimate relationship (Gostin 2008 (unpublished)).” For example, confidentiality prevents doctors from disclosing information shared with them by a patient in the course of a physician-patient relationship. Security can be defined as “the procedural and technical measure required a) to prevent unauthorized access, modification, use, and dissemination of data stored or processed in a computer system, b) to prevent any deliberate denial of service, and c) to protect the system in its entirety from physical harm (Turn and Ware 1976).” In general, security of information relates to the administrative and technological infrastructure that ensures the protection of data and information.

Modern Concept of Informational Privacy

In the 1960's, the use of computers and technology to store personal information increased greatly, and led to a public debate on privacy. The Department of Health, Education and Welfare (HEW) issued a report on government records maintained in computer databases in 1973. In this report, HEW outlined a Code of Fair Information Practices to ensure that entities that collect and use personal data provide adequate privacy protections for that information. The Code also allocated the rights and responsibilities of different entities in the collection and use of personal information. Although these principles had been discussed prior to the release of the HEW report, they had never before been presented in a comprehensive and succinct manner (Turn and Ware 1976).

There are five main principles in the Code of Fair Information Practices outlined in the HEW report. First, the principle of "collection limitation" requires that individuals be given notice that their information is being collected. There cannot be any secret record systems. Second, the principle of "disclosure" guarantees individuals the right to review the data collected about them and be informed about how the data are used. Third, the principle of "secondary usage" gives individuals the ability to prevent information that was obtained for one purpose from being used or made available for another purpose without that individual giving consent. Fourth, the principle of "record correction" provides individuals with the ability to contest the accuracy and completeness of their collected data. Fifth, the principle of "security" requires that entities that collect and use personal data ensure that the information is accurate and secure. Many later formulations of the Code of Fair Information Practices have included an enforcement principle, subjecting individuals to civil suits for any damages that result from a violation of the other five principles (National_Research_Council 2007).

The privacy principles included in the Fair Information Practices have become the basic framework for most modern privacy protections. These principles have been translated into statutes, administrative practices, and technical regulations, including the HIPAA Privacy Rule and the Privacy Act of 1974 (see discussion below) (Starr 1999). In addition, the Fair Information Practices have also influenced privacy laws worldwide. They were included in the privacy guidelines developed by the Organization for Economic Cooperation and Development (OECD), an organization consisting of 24 leading industrial countries, including the United States. The purpose of the OECD guidelines was to harmonize national privacy laws for the transfer of personal information across national borders. Privacy laws in North America, Europe, and East Asia have been shaped by the OECD privacy guidelines (Solove, Rotenberg et al. 2005).

Importance of Privacy in Research

The success of any health research project depends on community trust and cooperation with the researchers involved. It is often necessary for individuals to share sensitive and potentially embarrassing information with researchers in order for research studies to be conducted. In addition, medical research is more accurate when researchers have access to increased amounts of information. Research participants are more willing to share personal information and more likely to truthfully answer research questions, when they believe that their privacy is protected (Hodge, Gostin et al. 1999).

There are many different types of sensitive information in an individual's medical record that may be important for conducting health research. For example, research often involves looking at an individual's behavioral patterns. This can include private information regarding the individual's sexuality, or smoking, alcohol and drug use habits. Many research projects study an individual's genetic profile to gain insight into that individual's predispositions and diseases. Also, it may be necessary to collect information on an individual's social, race or economic status to conduct studies on poverty, nutrition and social relationships (Gostin 2008 (unpublished)).

Although the success of many research projects depends on the disclosure of sensitive information, the inadvertent or unwanted disclosure of this type of information can produce a variety of different harms to the individual. The disclosure of sensitive personal information may cause intrinsic harm (Saver 2006). This type of harm results merely from the fact that private information is known to others. There is the danger of economic harm to the individual if private health information is disclosed. The individual could lose his or her job, health insurance or housing if the wrong type of information becomes known publicly. Additionally, the disclosure of sensitive information can result in social or psychological harm to the individual. For example, the disclosure that an individual is infected with HIV or another type of sexually transmitted disease can result in social isolation, loss of self-esteem, or other psychologically harmful results (Gostin 2008 (unpublished)).

Because individuals potentially face a variety of harms if they disclose personal health information for research purposes, any legal framework regulating research must also balance personal privacy against the good to society that results from the research study. The justification for protecting individual privacy is based on respect for the individual. In contrast, the justification for collecting personally identifiable health information is for the benefit of society at large. These two competing interests must both be recognized, and a balance must be reached that allows an appropriate level of risk to the individual to be weighed against the common good produced by medical research (Gostin, Lazzarini et al. 1996).

Public Concern with Loss of Privacy

Public opinion polls show that medical privacy is a major concern for many Americans. A Gallup Poll conducted in 2000 found that 78% of respondents believe it is very important that their medical records be kept confidential (Gallup_Organization 2000). In the Forrester Research survey of consumer attitudes toward health privacy conducted in 1999, 3 out of 4 people reported that they have significant concerns about the privacy and confidentiality of their medical records (Forrester_Research 2005).

A similar study conducted by Forrester Research in 2005, suggests that the passage of the Privacy Rule did not alleviate public concern with health privacy. In the 2005 survey, 2 out of 3 people (67%) were concerned about the privacy of their personal health information. 1 out of 8 respondents admitted to engaging in behaviors intended to protect their privacy, even at the expense of risking dangerous health effects. These behaviors included lying to their doctors about symptoms or behaviors, refusing to provide information or providing inaccurate information, paying out of pocket for care that is covered by insurance, and avoiding care altogether. In addition, the survey

showed that many consumers are unfamiliar with the HIPAA privacy protections. Only 59% of respondents recalled receiving a privacy notice, and only 27% believed that they had more rights than they had before receiving the notice (Forrester_Research 2005). If these surveys are correct, researchers have a major hurdle to overcome in gaining potential research subjects trust and consent to participate in research studies.

However, public opinion polls conducted by Harris Interactive show very different results. These polls suggest that the Privacy Rule is having a positive effect on public confidence that personal health information will be kept confidential. Prior to the creation of the Privacy Rule, a 1993 survey by Harris Interactive showed that 27% of Americans believed that their personal medical information had been released improperly in the past three years. In contrast, a 2005 survey showed that only 14% of Americans believe that this has happened to them. Over two-thirds (67%) of respondents reported having received a HIPAA privacy notice. Of these people, 23% stated that the privacy notice increased their confidence that their medical information is being handled properly a “great deal,” and 44% said that it increased their confidence “somewhat” (Harris_Interactive 2005).

A more recent public opinion poll conducted by Harris Interactive provides further evidence that the Privacy Rule is improving the public’s confidence that their health records will be kept confidential. In a March 26, 2007 poll, 70% of respondents indicated that they are generally satisfied with how their personal health information is handled with regards to privacy protections and security. Close to 60% of the respondents reported that they believe the existing federal and state health privacy protection laws provide a reasonable level of privacy protection for their health information. Also, 63% of the respondents agreed that they would consent to having their medical records used for research, as long as there were guarantees that no personally identifiable information would be released (Harris_Interactive 2007).

Individuals’ attitudes towards the use of their medical records in research are likely influenced by the individuals’ state of health. A 2003 study, surveyed patients with preexisting medical conditions’ attitudes toward the use of their medical records in research, and compared those results to polls from the general population. The survey found that 31% of patients with preexisting medical conditions stated that medical researchers should have access to their medical records without their permission, if it would help advance medical knowledge. In contrast, only 18% of the general population agreed that researchers should have access to their medical records without their permission. These results suggest that individuals with serious health problems, are particularly likely to express broad support for medical research and place less value on the protection of privacy (Kass, Natowicz et al. 2003).

A recent study conducted on veterans suggests that the biggest predictor of whether patients are willing to share their medical records with researchers is the patient’s trust that their information will be kept private and confidential. In this study, the patients with the most trust that the Veterans Affairs system would keep their medical records private were more likely to recommend a less-stringent process for obtaining informed consent. The veterans also recommended methods to give research participants more control over how their medical records are used in research. These recommendations included requiring that participants are fully informed about how their medical records are being used in research, providing assurances that the research being

conducted will benefit fellow veterans, updating research participants about findings and on-going research, and setting-out clear and consistent consequences for anyone who violates a patient's privacy (Damschroder, Pritts et al. 2007).

Legal Protections of Health Informational Privacy

The medical community has recognized the importance of protecting privacy in maintaining public trust in doctors and researchers, and the laws regulating medicine are reflective of a desire to increase this public trust. Since the time of Hippocrates, physicians have pledged to keep information about their patients private and confidential (Feld and Feld 2005). The Hippocratic Oath states "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself..." This pledge to privacy has been included in the code of ethics of almost all health care professionals in the United States. For example, the first Code of Ethics of the American Medical Association in 1847 included the concept of confidentiality (Office_of_Technology_Assessment 1993).

Similarly, all 50 states have recognized a right to privacy in their tort laws, either as a statutory right or as a common law right. Tort actions can be maintained under a number of different legal theories, including invasion of privacy, implied breach of contract, and breach of a fiduciary relationship. However, the success rate for plaintiffs in this type of tort action has been very low. As a result, at least twelve states have created a tort for breach of confidentiality in the patient-physician relationship, which allows a patient to bring an action for unauthorized disclosure of health information (Pritts 2002). California and Tennessee have the most privacy protections, and recognize the right to privacy as a matter of state constitutional law (Department_of_Health_and_Human_Services 2000).

In the United States, the Constitution does not provide for a "general constitutional right to privacy."² However, the Supreme Court has recognized various privacy interests that the constitution protects. In Whalen v. Roe, the Supreme Court held that the Constitution protects two different dimensions of privacy: 1) "an individual's interest in independence in making certain kinds of important decisions" (decisional privacy), and 2) "an individual's interest in avoiding the disclosure of personal matters" (informational privacy).³ In this case, the plaintiffs challenged a New York statute that created a database of persons who obtained drugs that have both a lawful and unlawful market. The key issue was whether the constitutional right to privacy gives an individual the right to prevent the government from disclosing personal health information. The Court held that the statute in question was constitutional. However, the Court recognized that an individual's interest in preventing the disclosure of personal health information is an aspect of the right to privacy. In this case there was no violation of this right because the state had adequate standards and procedures for protecting individual privacy.

² Katz v. United States, 389 U.S. 347, 350 (1967).

³ 429 U.S. 589, 599-600 (1977).

Subsequent lower court decisions have interpreted Whalen as creating a narrow right to informational privacy.⁴ Lower courts apply a flexible test, balancing the invasion of privacy against the strength of the government interest to determine whether a state statute infringes on the Whalen privacy interest. In the United States v. Westinghouse Electric Corporation, the court enunciated five factors to be considered when applying the balancing test to determine whether a Constitutional violation occurred.⁵ These factors include the following: 1) the type of record and the information the database contains, 2) the potential for harm in the event of any unauthorized disclosure, 3) the injury from disclosure to the relationship in which the record was generated, 4) the adequacy of safeguards to prevent unauthorized disclosures, and 5) the need for access for a public interest. Many courts have applied this five factor test in subsequent cases.⁶

Both state privacy torts and the Constitutional protection of privacy are incomplete. When the Privacy Rule was created, it was intended to increase privacy protections, and provided the first systematic, national protection for health information privacy. HHS recognized this important goal by stating: “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 Privacy Rule also addressed the lack of uniformity among states in their treatment of confidential health information. (Department_of_Health_and_Human_Services 2002).

Procedural History of HIPAA

Pre-HIPAA Federal Responses Aimed at Protecting Medical Privacy

Prior to the passage of HIPAA, there were a number of other federal responses aimed at protecting medical privacy. In 1965, the House of Representatives created a Special Subcommittee on the Invasion of Privacy to examine privacy issues in the nation. Also during this year, there was a proposal to establish a National Data Center within the federal government. The National Data Center would act as a data repository for all personal information collected by federal agencies for statistical purposes. However,

⁴ See, e.g. Barry v. City of New York, 712 F.2d1554, 1559 (2nd Cir. 1983); Walls v. City of Petersburg, 895 F.2d. 188. 192 (4th Cir. 1990); Plante v. Gonzalez, 575 F.2d. 1119, 1132, 1134 (5th Cir. 1978); Kimberlin v. United States Dep’t of Justice, 788 F.2d. 434 (7th Cir. 1986); In re Crawford, 194 F.3d. 954, 959 (9th Cir. 1999). But see J.P. v. DeSanti, 653 F.2d. 1080, 1090 (6th Cir. 1981); Bloch v. Ribar, 156 F.3d. 673, 684 (6th Cir. 1998); American Federation of Government Employees, AFL-CIO v. Department of Housing & Urban Development, 118 F.3d 786 (D.C. Cir. 1997).

⁵ 638 F.2d 570 (1980).

⁶ See, e.g. Doe v. Southeastern PA Trans. Auth., 72 F.3d 1133 (3rd Cir. 1995); Doe v. Barrington, 729 F. Supp. 376 (NJ 1990); Patients of Doctor Barbara Solomon v. Board of Physician Quality Assurance, 85 F. Supp. 2d 545 (MD 1999); and AA v. New Jersey, 176 F. Supp. 2d 274 (3rd Cir. 2001). Other courts that have recognized constitutionally protected privacy rights in connection with medical records include: Herring v. Keenan, 218 F.3d 1171 (10th Cir. 2000); F.E.R. v. Valdez, 58 F.3d 1530 (10th Cir. 1995); Lankford v. City of Hobart, 27 F.3d 477 (10th Cir. 1994); A.L.A. v. W. Valley City, 26 F.3d 989 (10th Cir. 1994).

Congress rejected this proposal, and it was eventually abandoned. Congress, the media and the public were very concerned about the privacy threats that this type of data collection would create (Turn and Ware 1976).

As discussed above in the section on privacy, the Code of Fair Information Practices presented in the 1973 HEW Report was a major development in the concept of privacy as a legal interest. These principles created a framework for the protection of informational privacy that many future legal privacy-protection systems incorporated. The Privacy Act of 1974 included all five elements of the Code of Fair Information Practices in its privacy protections, and is considered by many to be the most significant privacy law in the United States.

The purpose of the Privacy Act of 1974 was to limit federal agencies' collection and use of personal health information. The five elements of the Code of Fair Information Practices can be seen in the following requirements of the Act: 1) agencies must publish an annual notice of their record-keeping systems,⁷ 2) agencies must notify citizens and lawful permanent residents about the existence of any records of personal information that the agency is maintaining, if that information is requested,⁸ 3) agencies must grant citizens and lawful permanent residents the right to access their records, and make any corrections or amendments they think are necessary,⁹ 4) agencies must obtain prior approval from citizens and lawful permanent residents for any "non-routine" uses or dissemination of their information,¹⁰ and 5) agencies must specify the purpose for which they are collecting personal information, and face civil and criminal penalties for any misuses of information.¹¹

One possible weakness in the Privacy Act of 1974's protection of privacy is that it permits federal agencies to disclose personal information for "routine purposes." This means that an agency can use personal data for any purpose compatible with the purposes for which the data were collected.¹² A second weakness of the Privacy Act's protection is that it applies only to federal agencies, but does not protect the privacy of information collected by businesses, private sector organizations, or state and local agencies (Solove, Rotenberg et al. 2005). However, the Act did establish the Privacy Protection Study Commission to study the record-keeping systems of these non-covered entities in order to recommend whether the Privacy Act should be extended to cover their record keeping systems (National_Research_Council 2007).

In the years following the Privacy Act of 1974, there have been a number of other federal statutes that were intended to protect some aspect of personal privacy within the federal government. Many of these incorporated at least some of the elements of the Fair Information Practices. For example, the Veterans Omnibus Health Care Act of 1976 protects the privacy of medical records relating to the treatment of drug abuse, alcohol abuse, and infection with HIV or sickle cell anemia within the Department of Veterans Affairs. Similarly, the Social Security Act, Section 1106, prohibits the unauthorized disclosure of individually identifiable records held by HHS, Social Security, and their

⁷ 5 U.S.C. § 552a(e)(4).

⁸ 5 U.S.C. § 552a(e)(3).

⁹ 5 U.S.C. § 552a(d).

¹⁰ 5 U.S.C. § 552a(b)(3).

¹¹ 5 U.S.C. § 552a(g)(1) and 5 U.S.C. § 552a(g)(3).

¹² 5 U.S.C. § 552a(b)(3)

contractors. For a complete list of federal privacy statutes see “Table of Federal Privacy Statutes” in Appendix A.

In 1991, HHS convened the leaders of the health care industry to discuss how administrative costs in health care could be reduced. This advisory group organized into the Workgroup for Electronic Data Interchange (WEDI). WEDI concluded that the best way to reduce administrative health care costs was to use an electronic data interchange (EDI) (Hawaii_Medical_Service_Association 2000).

In 1992, WEDI published a report outlining the steps necessary to make the use of EDI routine for the health care industry by 1996. WEDI reconvened in 1993 to resolve the remaining implementation problems for the use of EDI. After conducting a number of studies and hearings, WEDI recommended that federal legislation be passed to ensure a nationwide standard for the use of EDI. WEDI’s suggestions included creating federal privacy protections for individually identifiable health information (Workgroup_for_Electronic_Data_Interchange 1993). When HIPAA was signed into law on August 21, 1996, many of the WEDI suggestions were included in the act (Hawaii_Medical_Service_Association 2000).

Development of the Privacy Rule Regulations

The terms of HIPAA required the Secretary of HHS to submit detailed recommendations to Congress on ways to protect the privacy of individually identifiable health information by August 1997. These recommendations were intended to include suggestions on ways to protect individuals’ rights concerning their individually identifiable health information, procedures for exercising such rights, and the uses and disclosures of information that should be authorized or required under HIPAA.¹³ If Congress did not enact privacy legislation within 3 years of the passage of HIPAA, HIPAA required the Secretary of HHS to issue privacy regulations for the protection of individually identifiable health information within 42 months of HIPAA’s enactment.¹⁴

In response to this mandate, HHS submitted recommendations for protecting the privacy of individually identifiable health information to Congress in September 1997. In these recommendations, Secretary Shalala advocated for the passage of federal privacy legislation, rather than relying on HHS to pass a set of privacy regulations. Shalala’s report stated “This report recommends that Congress enact national standards that provide fundamental privacy rights for patients and define responsibilities for those who service them” (Shalala 1997).

Congress was unable to finalize privacy legislation on the time-schedule mandated in HIPAA. Several health privacy bills were introduced during the 1999 Congressional session, including a bill introduced by Senators Bennett and Leahy, a bill introduced by Representative McDermott, and a bill introduced by Representative Condit. However, none of these bills was passed. In June 1999, the Senate Committee on Health, Education, Labor and Pensions indefinitely delayed an attempt to mark-up a health privacy bill, because lawmakers were unable to agree on whether to give patients the right to sue over privacy breaches to medical records and whether to require preemption of all state health privacy laws. As a result, Congress passed the

¹³ HIPAA section 264 (a)-(b).

¹⁴ HIPAA section 264(c)(1).

responsibility of creating health privacy protections to HHS. HHS, under the Clinton Administration, issued the Privacy Rule to implement the requirements of HIPAA. HHS followed Secretary Shalala's 1997 recommendations to Congress in shaping the regulations (Redhead 2001).

Over the course of developing the current Privacy Rule, HHS went through four iterations of the rule. First, HHS issued a proposed version of the Privacy Rule for public comment on November 3, 1999. This version of the rule collected over 50,000 comments (Stevens 2000).

Based on the comments from the proposed version of the Privacy Rule, HHS issued the second version of the rule, entitled *Standards for Privacy of Individually Identifiable Health Information*, on December 2000.¹⁵ Before this rule could take effect, the Secretary of HHS was flooded with unsolicited public comments and criticism regarding the rule. Healthcare insurers and providers were concerned that the rule would make it difficult for the health care industry to operate efficiently. They were particularly concerned about the requirement that they get consent prior to making any routine disclosure of individually identifiable health information. The comments received also suggested that the original rule would prevent pharmacists from filling prescriptions and searching for potential drug interactions before patients arrived at pharmacies, interfere with providing emergency medicine in situations where it would be impossible to obtain patient consent before treatment, and delay the scheduling and preparation of hospital procedures until the doctor could obtain patient consent (Department_of_Health_and_Human_Services 2002).

In March 2002, HHS published a proposed modification to the rule. HHS, under the Bush Administration, had made significant changes to the regulations. This reopened the rulemaking process, and created a new period for submitting public comments. This version of the Privacy Rule collected over 24,000 comments (Department_of_Health_and_Human_Services 2002)

Incorporating the suggestions collected through the second notice of proposed rulemaking period, HHS issued the final version of the Privacy Rule in August 14, 2002.¹⁶ This is the current, effective, and codified version of the Privacy Rule (45 CFR pts. 160 and 164.) Most health care providers and health plans were required to be in compliance with this version of the Privacy Rule by April 14, 2003. Small health plans were given until April 14, 2004 to be in compliance. The rule tries to balance the need for protecting individually identifiable health information against the important uses for the information in health care and research.

Background: HIPAA and Research

Congress recognized the important role that health records play in conducting health research, and wanted to ensure that the passage of the Privacy Rule would not impede researchers' continued access to such data. This is reflected in two House Reports on HIPAA with identical language, stating: "The conferees recognize that certain uses of individually identifiable information are appropriate, and do not compromise the privacy of an individual. Examples of such use of information include... the transfer of

¹⁵ 65 Fed. Reg. 82,462 (2000).

¹⁶ 67 Fed. Reg. 53,181 (2002).

information from a health plan to an organization for the sole purpose of conducting health care-related research. As health plans and providers continue to focus on outcomes research and innovation, it is important that the exchange and aggregated use of health care data be allowed.¹⁷”

Although Congress was interested in limiting the detrimental effects that the Privacy Rule would have on research, researchers did not play a large role in shaping the final version of the Privacy Rule published by HHS. Most of the comments that HHS received from the research community during the notice of proposed rulemaking period were focused on urging HHS not to include research within the Privacy Rule regulations at all. Very few comments suggested alternatives to the regulatory scheme proposed by HHS, or gave HHS constructive comments on how to incorporate the research provisions into the rule. For an overview of the comments HHS received prior to publishing the final Privacy Rule in 2002, see the “Appendix B: Table of Public Comments.”

One possible explanation for the lack of constructive public comments submitted by the research community to HHS is that the Privacy Rule regulates “covered entities,” not researchers. HIPAA defines covered entities as including health care providers, health plans and health care clearinghouses that electronically transmit any health information in connection with transactions for which HHS has adopted standards.¹⁸ Health plans are individual or group plans that provide or pay the cost of medical care. Examples of private health plans include health insurers or managed care organizations. Public health plans include Medicaid, Medicare, or Veterans Affairs. Health care clearinghouses generally refer to billing services, and health care providers include doctors and health care professionals who provide treatment.

Although researchers do not generally meet any of the definitions of a covered entity, there are several situations where researchers are considered covered entities under HIPAA. First, if researchers provide medical care as part of their research study, they are considered covered entities and are subject to the Privacy Rule. This normally applies to researchers conducting clinical trials. Second, if a researcher works at a covered entity, such as a hospital or health plan, that researcher is considered a covered entity under the Privacy Rule (Department_of_Health_and_Human_Services 2004).

Generally, researchers cannot be held liable for any breaches or violations to the Privacy Rule that they commit. Rather, the covered entity that released the data to the researcher is liable for the researcher’s breach. There are two exceptions to this rule. First, a researcher is liable for his/her own breach under the Privacy Rule, if they fall into one of the situations described above that classifies the researcher as a covered entity. Second, patients can hold researchers accountable for unauthorized disclosures of health information under various state tort theories (see discussion above in section on the Legal Protections of Health Informational Privacy) (Department_of_Health_and_Human_Services 2000).

Even in situations where researchers cannot be held liable for their own privacy breaches under the Privacy Rule, the Privacy Rule is likely to have a significant effect on researchers’ ability to access personal medical records. Since covered entities are liable

¹⁷ H.rpt. 104-496, pt.1 on H.R. 3101, “Health Coverage Availability and Affordability Act of 1996,” March 25 1996. H.rpt. 104-736 conference report on H.R. 3101, “Health Insurance Portability and Accountability Act of 1996”, July 31, 1996.

¹⁸ 45 C.F.R. § 160.103.

for the mistakes and illegal uses of individually identifiable health information made by researchers, covered entities are less likely to release data to researchers. Some covered entities may decide not to disclose data to any researcher, rather than risk the legal repercussions. Also, the Privacy Rule establishes a number of procedural steps and rules that researchers must follow when trying to receive data from a covered entity. Researchers must become familiar with the Privacy Rule in order to effectively get their research projects approved by covered entities and obtain access to their data.

In creating the current research provisions of the Privacy Rule, HHS considered several other options to the system finally adopted. HHS's jurisdiction under HIPAA, gave HHS the choice of not providing any protections for individuals whose information is used in research. However, HHS rejected this option because it would not provide any privacy protections to such individuals. HHS also considered requiring researchers to obtain individual authorization in all situations where a covered entity might want to disclose individually identifiable health information for research. This option would make research projects almost impossible to carry out. Instead, HHS created the current system which balances individual privacy against researchers' need for data.

Current System: HIPAA and Research

In the final version of the Privacy Rule research is defined as “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.¹⁹” The following sections provide a detailed overview of the different provisions regulating research under the Privacy Rule.

Type of Information Protected

During the rulemaking process, HHS decided that only protecting electronic information would provide inadequate protection to patient privacy, and that it would be difficult to distinguish between information held in electronic form versus non-electronic form. As a result, the Privacy Rule protects a subset of individually identifiable health information, known as protected health information (PHI). PHI refers to all individually identifiable health information maintained by a covered entity²⁰. To be a covered entity, the individual or organization must transmit some type of claims information electronically. Once the health care entity conducts a single electronic transaction, all health information that the health care entity controls is protected by the Privacy Rule, regardless of whether the information is in electronic form. The information is protected if it is a paper record, electronic record, or communication. The Privacy Rule does not protect individually identifiable health information that is held or maintained by an organization other than a covered entity or its business associates (Department_of_Health_and_Human_Services).

Research Uses and Disclosures with Individual Authorization

¹⁹ 45 C.F.R. § 164.510.

²⁰ 45 C.F.R. § 160.103.

Individual authorization is a legal document in which an individual grants a covered entity permission to use or disclose his or her PHI for a specific research purpose. Once a covered entity has a signed authorization form from an individual, the covered entity is permitted to grant researchers access to that individual's PHI for the specified research project.²¹ The authorization must be "specific and meaningful."²² This means that the authorization must give a description of the information to be used in the research project, and the name of the person or class of persons authorized to make the use or disclosure. The individuals granting authorization should be given a clear explanation of all of the allowable uses and disclosure of PHI that they are authorizing, and what their rights are under HIPAA

Each authorization that an individual grants can pertain only to a specific research study. The Privacy Rule does not permit an individual to grant authorization to nonspecific research or to future, unspecified projects. The creation and maintenance of a research repository or database is considered a specific research activity under the Privacy Rule. However, every time the covered entity or researcher uses the information stored in the repository or database for a different specific research study, a new legal permission must be obtained for that specified research.

Authorization under the Privacy Rule differs from informed consent. Authorization states how, why and to whom the PHI will be used and/or disclosed for research, and seeks permission for that use or disclosure. In contrast, informed consent describes the research and seeks permission to involve the subject; it also provides research subjects with a description of how the confidentiality of the research records will be protected. Although they are different types of documents, authorization forms and informed consent forms can be combined into one document for research projects (Department_of_Health_and_Human_Services).

Research Uses and Disclosures without Authorization

a) Documented IRB or Privacy Board Approval of such Use or Disclosure

The Privacy Rule permits a covered entity to use and disclose PHI for research purposes without getting authorization in a limited number of situations. One such situation occurs when a researcher gets an institutional review board (IRB) or privacy board to review his or her project, and provide documentation that the research project poses little risk to the participants' privacy. The IRB or Privacy Board will then grant a "waiver" of authorization to the researcher for that particular research protocol.²³

IRBs and privacy boards have different scopes of review. The Common Rule created IRBs to review research projects involving human subjects for risk of harm to the subjects, and to ensure that proper informed consent is obtained for all research study participants (for a complete discussion of the Common Rule see section on the Relationship between HIPAA and Other Laws.) The Privacy Rule added to IRBs' jurisdiction, and gave them the additional responsibility of granting waivers of authorization. In contrast, privacy boards did not exist under the Common Rule. Privacy

²¹ 45 C.F.R. § 164.508.

²² 45 C.F.R. § 164.508(c)(1)(i).

²³ 45 C.F.R. § 164.512(i)(1)(i).

boards were created by the Privacy Rule, and only have authority to review applications for waivers of authorization.

The Privacy Rule sets out a clear standard that IRBs and privacy boards must apply in deciding whether to grant a waiver of authorization for a particular research study:

- § The use or disclosure of PHI must involve no more than a minimal risk to the privacy of the individual.
- § The research could not practicably be conducted without the waiver of authorization.
- § The privacy risks are reasonable in relation to the anticipated benefits, if any, to the individual and the importance of the research.
- § A plan exists to destroy the identifiers, unless there is a health or research justification for retaining them.
- § There are written assurances that the data will not be reused or disclosed to others, except for research oversight or additional research that would also qualify for a waiver.²⁴

An IRB or a Privacy Board may waive the authorization requirement in whole, or in part. A complete waiver of authorization means that no authorization is required for the covered entity to use and disclose PHI. A partial waiver means that the IRB or Privacy Board determined that a covered entity does not need authorization for all of the uses and disclosure of the PHI proposed in the research project. For example, an IRB or privacy board often grants partial waiver to allow PHI to be disclosed to researchers for subject recruitment purposes. However, if only a partial waiver of authorization is granted, the researchers will need to get authorization to actually conduct the research project.

The Privacy Rule did not change the IRB membership requirements from the Common Rule.²⁵ An IRB must be made up of at least 5 members with varying backgrounds who are sufficiently qualified through the experiences and expertise of its members, and the diversity of the members to analyze the proposed research project. The IRB cannot consist entirely of members from one profession. At least one member must be unaffiliated with the institution disclosing the PHI, and must not be part of the immediate family of someone affiliated with the institution. Members cannot have conflicts of interest with regards to the proposed research project. Also, there must be one member whose primary concerns are scientific, and one member whose primary concerns are nonscientific on each IRB. For the approval of the waiver of authorization to be effective, it must be approved by a majority of the IRB members present at the IRB meeting.

Privacy Boards have similar membership requirements to IRBs, and must be made up of members with varying backgrounds and have appropriate professional competency to review the research protocol. There must be one member who is not affiliated with any entity conducting or sponsoring the research project, and not related to

²⁴ 45 C.F.R. § 164.512(i)(1)(i).

²⁵ 45 C.F.R. § 164.512(i)(1)(i)(A).

any person who is affiliated with any of these entities. Also, all members with conflicts of interest must be removed.²⁶

Research studies that require collecting data from multiple sites, involve the jurisdiction of multiple IRBs or privacy boards. The Privacy Rule does not require a researcher to get a waiver of authorization from the IRB or privacy board of every entity that is contributing PHI. Covered entities are permitted to rely on a waiver of authorization approved by as few as one IRB or privacy board with jurisdiction. However, a covered entity may decide to require approval from its' own IRB or privacy board prior to disclosing PHI to the requesting researcher, regardless of whether another IRB or privacy board already granted a waiver of authorization. The Rule does not address potential disagreements between IRBs or privacy boards. But, HHS "strongly encourages" researchers to notify IRBs and privacy boards of any prior reviews of a research protocol to reduce the chance of IRBs disagreeing.

IRBs and privacy boards are not required to review and approve authorization forms. However, under the Common Rule IRBs are required to review and approve any document that includes the informed consent document for human subjects' research. If the Privacy Rule authorization is combined in the same document as the informed consent document, then IRB approval must be sought for the authorization forms as well as the informed consent forms (Department_of_Health_and_Human_Services).

b) Preparatory to Research

A second situation where a covered entity is permitted to use and disclose PHI without getting authorization is for activities that are preparatory to research.²⁷ A covered entity may permit researchers to look through its medical records in order to develop research designs and protocols, as long as the access is necessary for the research purpose. However, the covered entity may not permit the researcher to remove any PHI from the covered entity (Department_of_Health_and_Human_Services).

According to HHS guidance on the Privacy Rule, a researcher who is an employee or member of the covered entity's workforce is permitted to use the "preparatory to research" provision to legally contact prospective research subjects for recruitment purposes. A covered entity may also contract with a researcher as a business associate to assist in recruiting individuals on behalf of the covered entity. However, a researcher who is not an employee or a business associate of the covered entity must obtain a partial waiver of the authorization in order to recruit. The "preparatory to research" provision does not provide a mechanism for non-covered entity researchers to recruit potential research subjects.

It is important to note that any preparatory to research activities involving human subject research must be reviewed and approved by an IRB according to the Common Rule. Therefore, even though the Privacy Rule does not require IRB review prior to "preparatory to research" activities, any research project involving human subjects will be reviewed by an IRB before "preparatory to research" activities can take place (Department_of_Health_and_Human_Services 2003).

²⁶ 45 C.F.R. § 164.512(i)(1)(i)(B).

²⁷ 45 C.F.R. § 164.512(i)(1)(ii).

c) Research on Protected Health Information of Decedents

The third situation where a covered entity is permitted to disclose PHI without authorization is for research using the PHI of decedents. Covered entities are not required to get authorization from the personal representative or next of kin to conduct research on a decedent's PHI, nor are they required to receive a waiver of authorization.

The rule requires that researchers make several representations, either in writing or orally, to the covered entity prior to the covered entity granting the researcher access to decedent's PHI. These representations include:

- § The use or disclosure being sought is solely for research on the PHI of decedents
- § The PHI is necessary for research
- § At the request of the covered entity, documentation of the death of the individual²⁸

d) Limited Data Sets

Limited data sets present a final method for researchers to gain access to PHI without getting authorization. Limited data sets allow a researcher to access large amounts of personal health information. However, prior to disclosing the PHI to the researcher, the covered entity must remove 16 direct identifiers from the individual's records in order for the information to be considered a limited data set. Information that is not removed from a limited data set may include: city, state, zip code, elements of date, and other numbers, characteristics or codes not listed as direct identifiers in the regulation.

Data use agreements establish the permitted uses and disclosures of the limited data set by the researcher. The agreements specify the recipient of the limited data set. They also require the recipient to agree to a number of conditions, including:

- § Not to use or disclose the limited data set other than as permitted by the agreement or as required by law
- § To use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement
- § To report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware
- § To ensure that any agents to whom the recipient provides the limited data set agree to the same restrictions and conditions as the original recipient
- § Not to identify the information or contact the individuals whose records are included in the data set²⁹

e) Other Disclosures

²⁸ 45 C.F.R. § 164.512(i)(1)(iii).

²⁹ 45 C.F.R. § 164.514(e)(1).

In addition to the uses or disclosures permitted without authorization or waiver of authorization for research, there are also a number of situations unrelated to research in which a covered entity may release PHI without authorization or waiver of authorization. These situations include:

- § Disclosures for treatment, payment, and health care operations³⁰
- § Disclosures to business associates³¹
- § Disclosures for public health purposes as required by state and federal law³²
- § Disclosures to public agencies for health oversight activities, such as audits, inspections, civil, criminal or administrative proceedings, and other activities necessary for the oversight of the health care system³³
- § Disclosures to law enforcement officials³⁴
- § Disclosure for judicial and administrative proceedings, if the request for information is made through a court order³⁵

De-Identified Information

De-identified information provides an additional method for researchers to gain access to personal health information stored by covered entities without getting authorization or waiver of authorization. De-identified information is similar to a limited data set, because it includes data that have had personal identifiers removed. However, all personal identifiers are removed from de-identified information and only some are removed from a limited data set. There are two methods to de-identify personal health information. Under the statistical method, a statistician or person with appropriate training verifies that enough identifiers have been removed that the risk of identification of the individual is very small. Under the safe harbor method data is considered de-identified if the covered entity removes 18 specified personal identifiers from the data.³⁶

De-identified information does not qualify as PHI, and therefore, is not protected under the Privacy Rule. De-identified information can be disclosed to researchers at any time. There is no need for a researcher to get authorization to gain access to de-identified information, and the data do not need to fall into one of the exceptions where authorization is not needed (Department_of_Health_and_Human_Services).

Business Associates in Research

One way that researchers have adapted to the restrictions imposed by the Privacy Rule is through the use of business associate agreements. Under the Privacy Rule, covered entities are permitted to use business associates to assist in many of the covered

³⁰ 45 C.F.R. § 164.506(a).

³¹ 45 C.F.R. § 164.506(e).

³² 45 C.F.R. § 164.510(b).

³³ 45 C.F.R. § 164.510(c).

³⁴ 45 C.F.R. § 164.510(f).

³⁵ 45 C.F.R. § 164.510(d).

³⁶ 45 C.F.R. § 164.514(b).

entity's operations and functions. A covered entity may disclose PHI to a business associate only to help the covered entity carry out its own health care functions, not for the business associate's independent use or purposes. In the research context, a business associate cannot be an independent researcher conducting his or her own research project. But, a business associate can assist a covered entity in conducting the covered entity's research project. Common functions or activities that business associates perform for covered entities in research include recruiting subjects; data analysis, processing or administration; utilization review; quality assurance; and practice management.

The covered entity can only use a business associate if the covered entity obtains assurances in writing that the business associate will: 1) use the information only for the purposes for which it was engaged by the covered entity, 2) safeguard the information from misuses, and 3) help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Business Associate contracts must include:

- § A description of the permitted and required uses of the PHI by the business associate
- § A statement that the business associate will not use or disclose the PHI other than as permitted or required by the contract, or as required by law
- § A statement that the business associate will use appropriate safeguards to prevent a use or disclosure of PHI other than as provided for by the contract³⁷

The strict guidelines regulating the circumstances under which a covered entity is permitted to use a business associate provide a strong protection to prevent disclosure of PHI by business associates. The business associate contract makes very clear the circumstances in which the business associate may use and disclose PHI.

If a covered entity becomes aware of a material breach or violation of the business associate contract, the covered entity must take reasonable steps to cure the breach or end the violation. If this is impossible, the covered entity must terminate the contract. If termination of the contract is impossible, the covered entity must report the problem to the HHS's Office for Civil Rights.

No business associate relationship is formed from the disclosure of PHI to a researcher, if patient authorization is obtained, a waiver of authorization has been issued by an IRB, or a limited data set is used. The researcher is not a business associate of the covered entity because he or she is not conducting a function or operation of the covered entity, or providing one of the services listed in the definition of a business associate in the statute (Office_of_Civil_Rights 2002).

Minimum Necessary

For almost all uses and disclosures of PHI under the Privacy Rule, a covered entity is required to make a reasonable effort to use and disclose only the minimum amount of PHI needed for the intended purpose. Researchers are included in this

³⁷ See definition of "business associate" at 45 C.F.R. § 160.103.

restriction. Therefore, covered entities can only disclose the “minimum” amount of information to a researcher that is necessary for the research project.³⁸

The minimum necessary standard does not apply in the following circumstances :

- § Disclosure by a health care provider for treatment
- § Disclosure by an individual who is the subject of the information, or her or her personal representative
- § A use or disclosure made due to an authorization
- § Disclosures to HHS for complaints, investigations, compliance review or enforcement
- § A use or disclosure required by law
- § A use or disclosure required for compliance with the HIPAA transaction rule or the HIPAA Administrative Simplification Rule³⁹

Accounting for Research Disclosures

One provision of the Privacy Rule that has created an additional administrative burden for covered entities is the accounting for disclosures section. This provision gives individuals the right to receive a list of all disclosure that a covered entity has made of their PHI in the last 6 months, including disclosures made for research purposes.⁴⁰ This means that every time a researcher accesses an individual’s PHI, the covered entity must record this occurrence. Disclosures made with an individual’s authorization, disclosures made prior to the compliance date for the Privacy Rule and disclosures made as part of a limited data set are exempt from this requirement (Department_of_Health_and_Human_Services).

Research Started Before the Compliance Date

The privacy rule “grandfathers” certain permissions that were obtained for research purposes prior to the compliance date. A research project can continue if any of the following was obtained before the compliance date: 1) an authorization from an individual to use or disclose PHI for research, 2) an informed consent from the individual to participate in the research, or 3) a waiver of informed consent by an IRB. This rule applies even if the legal permissions obtained prior to the implementation of the Privacy Rule would not satisfy the requirements of the current rule. However, this exception does not apply if any change is made to the legal permission after the compliance date.⁴¹

Hybrid Entities

The use of hybrid entities in the Privacy Rule has caused confusion to both covered entities and researchers. In most circumstances, an organization or individual that meets the definition of a covered entity will be subject, in its entirety, to the Privacy

³⁸ 45 C.F.R. § 164.502(b).

³⁹ 45 C.F.R. § 164.502(b)(2).

⁴⁰ 45 C.F.R. § 164.528.

⁴¹ 45 C.F.R. § 164.532.

Rule. However, if a covered entity performs health care functions that qualify it as a covered entity, and other functions unrelated to health care, it can become a hybrid entity. To take advantage of this option, an organization must designate in writing its “health care components.”⁴² After making this designation, the Privacy Rule will only apply to the health care components of that organization. All other components of the organization are not bound by the Privacy Rule.

HHS guidance material provides a useful example of when it may be useful for an organization to become a hybrid entity, using a hypothetical university. Most universities are a single legal entity. If a university includes an academic medical center with a hospital, the entire university will be classified as a covered entity since it will meet the definition of a health care provider. However, the university can elect to be a hybrid entity by designating the hospital portion of the university as the health care component. By doing this, only the hospital has to comply with the Privacy Rule. The rest of the university is not bound by the Privacy Rule in any way.

Whether to classify a research laboratory within a hybrid entity as part of the health care component of the entity, or as part of the rest of the organization, depends on the exact nature of the work performed in that research laboratory. Any research project where the researchers are functioning as health care providers and conducting certain standard electronic transactions must be included in the health care component and must comply with the Privacy Rule. Researchers that provide health care, but do not conduct any electronic transactions have the option of being included in the health care component of the hybrid entity, but are not required to be included. If the covered entity does not include this type of research project in the health care component, then these research projects are not within the jurisdiction of the Privacy Rule.

A research project where the researchers do not function as health care providers nor conduct business associate-like functions, cannot be included in a hybrid entity’s health care component. These research projects should not be covered by the Privacy Rule. For example, a research laboratory where the researchers only conduct medical records research, are not performing as a health care provider or as a business associate. Thus, this type of laboratory cannot be included in the health care component of the covered entity (Department_of_Health_and_Human_Services).

Public Health Research

Similar to Congress’s recognition that research produces important societal benefits, Congress also recognized the importance of public health work when drafting the Privacy Rule. The rule reflects the fact that there is a legitimate need for public health authorities and others working to ensure the health and safety of the public to have access to PHI. As a result, the Privacy Rule permits covered entities to disclose PHI without authorization for specified public health purposes. The rule defines public authorities as any “federal, tribal or local agency or person or entity acting under a grant of authority or contract with the agency.”⁴³ Examples of public health authorities given by HHS include, state and local health departments, the Food and Drug Administration, the Centers for Disease Control, and the Occupational Safety and Health Administration.

⁴² 45 C.F.R. § 164.105(a)(2)(iii)(C).

⁴³ 45 C.F.R. § 164.501.

The Privacy Rule lists the types of public health uses and disclosures that are permitted. A covered entity can release PHI to a public health authority, without authorization or waiver of authorization, in the following circumstances:

- § Monitoring health threats and diseases
- § Child abuse or neglect
- § Products regulated by the FDA
- § Persons at risk of contracting or spreading a disease
- § Workplace surveillance⁴⁴

Additionally, the Privacy Rule does not preempt state and local laws relating to public health activities.⁴⁵ State laws may permit the release of PHI for other types of activities than the activities listed above. Disclosures permitted under state public health laws should continue under the Privacy Rule.

It is important to note that the Privacy Rule permits covered entities to disclose data to public health authorities, but does not require them to make these types of disclosures. This is because only states have the authority to require mandatory public health reporting. The federal government does not have this power. However, as a result of the permissive nature of public health reporting under the Privacy Rule, many covered entities resist sharing data with public health authorities. It is likely that covered entities are concerned about the privacy of data uses, the security of public health data systems, and the administrative burdens of accounting for these disclosures (Gostin 2008 (unpublished)).

Penalties for Breaching the Privacy Rule

One of the major obstacles to researchers gaining access to PHI from a covered entity is the covered entity's fear of being penalized under the Privacy Rule for a researcher's misuse of PHI. The Privacy Rule sets out both civil and criminal penalties for covered entities that breach the rule, or release data to researchers who breach the rule.⁴⁶ The civil penalty provision allows a \$100 fine per violation for disclosure made in error, with up to a maximum of a \$25,000 fine per year. The criminal penalties for persons who knowingly obtain or disclose individually identifiable information face fines of up to \$50,000 and imprisonment for up to one year. If the crime is committed under false pretenses, the individual or organization faces fines up to \$100,000 and five years imprisonment. Penalties for the sale or use of PHI for commercial advantage, personal gain or malicious harm are fines up to \$250,000 and 10 years imprisonment.

The Privacy Rule does not provide for a private right of action by patients or research participants.⁴⁷ This means that an individual whose privacy is violated under the

⁴⁴ 45 C.F.R. 164.512(b)(i)-(v).

⁴⁵ 45 C.F.R. 160.203(c).

⁴⁶ See 45 C.F.R. Part 160, subpart C and E.

⁴⁷ See example Doe v. Bd. of Trustees of Univ. of Illinois, 429 F. Supp. 2d 930, 944 (N.D. Ill. 2006); Poli v. Mt. Valley's Health Ctrs., Inc., 2006 U.S. Dist. LEXIS 2559, No. 05-2015, 2006 WL 83378, at 13-14 (E.D. Cal. Jan. 11, 2006); Haranzo v. Dep't of Rehabilitative Servs., 2005 U.S. Dist. LEXIS 27302, No. 7:04-CV-00326, 2005 WL 3019240, at 4 (W.D. Va. November 10, 2005) Dominic J. v. Wyo. Valley West High Sch., 362 F. Supp. 2d 560, 573 (M.D. Pa. 2005); Logan, 357 F. Supp. 2d at 155; Univ. of Colo. Hosp.

rule cannot sue the covered entity or individual who breached his or her privacy. Rather, an individual's only option is to file a claim with HHS's Office for Civil Rights (OCR). OCR is in charge of enforcement, and decides whether and when to pursue penalties against a covered entity (Stevens 2003).

Constitutional Challenges

There have been two constitutional challenges to the Privacy Rule since it was published in March 2002. In South Carolina Medical Association v. Tommy Thompson,⁴⁸ the South Carolina Medical Association sought a declaratory judgment that HIPAA is unconstitutional. Plaintiff claimed that HIPAA violated the non-delegation doctrine by authorizing HHS to create the Privacy Rule in the absence of clear guidance from Congress on how to shape the rule. Plaintiff also asserted that the final Privacy Rule exceeds the scope of authority that was granted to HHS in HIPAA. Finally, the plaintiff claimed that HHS' decision that HIPAA does not preempt more stringent state privacy laws is unconstitutionally vague, in violation of the Due Process Clause of the Fifth Amendment. The Fourth Circuit rejected all of the complaints, and held that the Privacy Rule is constitutional.

The second constitutional challenge to the Privacy Rule was heard in the Third Circuit. In Citizens for Health v. Michael O. Leavitt, Secretary U.S. Department of Health and Human Services, plaintiffs asserted that the Privacy Rule is invalid because it unlawfully authorizes covered entities to use and disclose individually identifiable health information for "routine uses" (including treatment, payment, and health care operations) without patient consent.⁴⁹ They claimed that authorizing these types of disclosures violates constitutionally protected privacy rights. The court granted summary judgment to HHS, stating that the Privacy Rule does not interfere with any right protected under the Bill of Rights. Covered entities do not need to obtain patient permission before disclosing personally identifiable health information for routine health care uses.

Conclusions

The Privacy Rule has changed the way that covered entities use and disclose information. This has had a profound effect on researchers' ability to access data and successfully complete meaningful research projects. The debate concerning the right balance between protecting individuals' privacy and ensuring adequate access to health information for researchers is still ongoing. However, as the rule currently exists, researchers are required to use and disclose health data in accordance with the provisions outlined above.

[PLACE HOLDER: Marc Rotenberg suggests including a section on how HIPAA impacts research practices or how researchers have adjusted research practices to

Auth. v. Denver Publ. Co., 340 F. Supp. 2d 1142 (D. Colo. 2004); O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176, 1179-80 (D. Wyo. 2001).

⁴⁸ 327 F.3d 346 (4th Cir. 2003).

⁴⁹ 428 F.3d 167 (3rd Cir. 2005).

accommodate the HIPAA rule. It's important to draw the connection between the specific provision of the regulation and the activity that was suspended.]

Relationship between HIPAA and Other Laws

Federal Research Statutes

Although the Privacy Rule has had a profound impact on health research, there are several other federal statutes that regulate research and affect the types of research projects that can be carried out in the United States. The federal regulations most relevant to health research are the Common Rule⁵⁰ and the FDA Protection of Human Subjects Regulations.⁵¹

The Common Rule is a set of regulations that was promulgated by the Department of Health, Education and Welfare in 1974 after a number of different biomedical research projects that put human lives at risk were disclosed to the public. Fifteen other federal agencies adopted these regulations in 1991, and they became known as the Common Rule. The regulations are intended to provide protection to human subjects in research, and aim at achieving this goal through two separate approaches. First, the regulations require research institutions that receive federal funding, and federal agencies that conduct research, to establish IRBs to review research proposals for risk of harm to human subjects. Second, the regulations stipulate a number of requirements that must be included in an informed consent form (Government_Accountabilty_Office 1996).

The FDA Protection of Human Subjects Regulations are also aimed at protecting the rights of human subjects in research. These regulations are directed at protecting human subjects enrolled in research involving products that the FDA regulates (i.e. drugs, medical devices, biologicals, foods and cosmetics.) For example, the regulations set out a number of steps researchers must go through before conducting drug research on human subjects. Researchers must submit a brief statement to FDA promising that they will uphold ethical research standards, and identifying the IRB that will review the study prior to its start date. The sponsors of the study are required to submit to FDA the results of any chemical and animal study conducted on the new drug, provide the proposed study procedures for using human subjects, and ensure that the researchers' designated IRB will review the proposed study. FDA will then review this information to ensure that there are no unacceptable risks to the human subjects, that the project is ethically sound, and that the research is likely to achieve the study's objectives. The regulations give FDA the right to request modifications to the proposed study, or the right to reject the proposal as presenting an unacceptable risk to human subjects (Government_Accountabilty_Office 1996).

Additionally, the FDA Protection of Human Subjects Regulations allow FDA to conduct onsite inspections of IRBs to determine whether or not they are adhering to the requirements of the regulation. This portion of the regulation provides FDA with the ability to examine IRB minutes, IRB written operating procedures and other documents that substantiate the IRBs' review of the research project. FDA can also ensure that the IRB reviewing the study meets the membership requirements stipulated in the

⁵⁰ 45 C.F.R. part 46 (A).

⁵¹ 21 C.F.R. Parts 50 and 56.

regulations, and that the consent forms contain all the required elements and are signed by all the subjects (Government_Accountability_Office 1996).

The Common Rule and the FDA Protection of Human Subjects Regulations differ from the Privacy Rule in the type of protection the regulations afford to research participants. Both the Common Rule and the FDA regulations are concerned with the risks to humans associated with participation in a research study. Neither set of regulations provides extensive protection for the privacy of research subjects or the confidentiality of their medical information (Office_for_Civil_Rights 2002). The Common Rule's only reference to confidentiality states that the informed consent document must include "a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained (Deapen 2006)." The FDA regulations are similarly bereft of strong privacy protections. In contrast, the Privacy Rule's main focus is protecting the privacy of the research subjects' health information. This difference could be a result of the changing nature of health research, and the growing dependence on detailed personal data that did not exist 30 years ago when the Common Rule and FDA regulations were created.

The Common Rule and the FDA Protection of Human Subjects Regulations also differ from the Privacy Rule in terms of the scope of their protection. The FDA regulations only apply to human subjects participating in research in which the FDA has jurisdiction. Thus, only research projects involving investigations into products in pursuit of FDA approval are affected by these guidelines. The Common Rule only applies to research involving human subjects that is conducted or supported by HHS or one of the other federal agencies that have adopted this rule. Only a segment of research falls under the jurisdiction of either of these regulations. This differs from the Privacy Rule, where all research, federally funded and privately funded, is bound by the Rule if a covered entity is using or disclosing PHI.

[PLACE HOLDER: Marc Rotenberg suggests exploring the relationship between the Privacy Rule and the Common Rule further "in light of the fact that so much research today is data driven, and involves so much personally identifiable information that might be used for other purposes. Given the recent revelations about security breaches and the escalating problem of identity theft, it seems not at all surprising that the ethical rules in this field would require greater concern for the protection of PHI"]

General Federal Laws

In addition to interacting with the Common Rule and the FDA Protection of Human Subjects Regulations, the Privacy Rule also often interacts with other federal laws. In the Preamble to the Privacy Rule, HHS stated that there should be very few instances where the Privacy Rule conflicts with existing statutes or regulations. Where potential conflicts do exist, HHS stated that an attempt should be made to resolve the conflict so that both laws apply. For example, if a statute or regulation permits the dissemination of PHI, but the Privacy Rule prohibits the use or disclosure of PHI without authorization, the covered entity is able to comply with both sets of laws. The entity could obtain HIPAA authorization prior to disseminating the information as required by the other law (Department_of_Health_and_Human_Services 2000).

The fact that a covered entity is permitted to use or disclose PHI “as required by law” under the Privacy Rule reduces a number of potential conflicts between the Privacy Rule and other federal rules.⁵² HHS provided an example to explain this point. If a previous statute or regulation requires a specific use or disclosure of PHI that the Privacy Rule appears to prohibit, the section of the Privacy Rule which permits uses or disclosures “as required by law” would allow this disclosure to be made. This is an example of a use or disclosure required by law. Also, HHS specifically stated that if a statute or regulation prohibits a use or disclosure of PHI that the Privacy Rule permits, the earlier more specific statute applies (Department_of_Health_and_Human_Services 2000).

As a result of the way the Privacy Rule was written, covered entities are often subject to both the Privacy Rule and other federal statutes and regulations simultaneously. In many situations, researchers must comply with the Privacy Rule, and the Common Rule or the FDA Protection of Human Subjects Regulations. Medicare providers must comply with the requirements of the Privacy Rule and the Privacy Act of 1974. Health care providers in schools, colleges and universities must comply with the Privacy Rule and the Family Educational Rights and Privacy Act. Substance abuse treatment facilities must comply with the Privacy Rule and the Substance Abuse Confidentiality provisions of the Public Health Service Act, Section 543 and its regulations. There are innumerable examples where the Privacy Rule and another federal statute both must be followed (Department_of_Health_and_Human_Services 2000).

State Laws

Similar to the Privacy Rules’ relationship to other federal statutes, the relationship between the Privacy Rule and state privacy laws is also complicated. In general, the Privacy Rule preempts contrary state laws relating to the privacy of health information. This means that if it is impossible for a covered entity to comply with both the Privacy Rule and the state law in question, the Privacy Rule will be applied in the situation and the state law will be considered void.⁵³

There are three exceptions to this general rule. First, any state law that is not contrary to the Privacy Rule is not preempted. If it is possible for a covered entity to comply with both the Privacy Rule and the state law simultaneously, the covered entity must comply with both sets of privacy rules. There is no preemption of the state law.

Second, state laws that are contrary to the Privacy Rule, but provide more protection to the privacy of health information are not preempted by the Privacy Rule. The Privacy Rule sets a national floor for the protection of PHI, not a national ceiling. More stringent means that the state law: 1) prohibits or restricts a use or disclosure in circumstances which would be permitted under HIPAA , 2) permits greater rights of access or amendment for the individual who is the subject of the PHI, 3) provides an individual with a greater amount of information regarding disclosure, rights and remedies, 4) narrows the scope or duration of any legal permission to use PHI, or increases the privacy protections afforded to PHI, 5) provides for the retention or

⁵² 45 C.F.R. § 164.512(a).

⁵³ 45 C.F.R. Part 160, Subpart B.

reporting of more detailed information for longer durations or 6) provides greater privacy protection for the individual with respect to any other matter.

Third, the final exception to the general preemption rule is in the public health arena. State laws that are contrary to the Privacy Rule, but provide for the reporting of disease or injury, child abuse, birth or death, or for conducting public health surveillance, investigation and intervention are not preempted by the Privacy Rule. States are permitted to set their own rules regarding what type of information can be collected by public health agents and how that information is used (Department_of_Health_and_Human_Services).

Applying this preemption rule and determining what privacy laws must be followed in any given state is a very difficult task for covered entities. All states provide some protection for the privacy of health information. However, they differ greatly in what type of protection they provide, and thus, interact differently with the federal Privacy Rule. In order to successfully conduct a preemption analysis, a covered entity must become familiar with both the state laws that are regulating its behavior and the Privacy Rule. Once a covered entity is successful with this task, it still must interpret how the state and federal regulations interact with each other, and correctly determine the situations in which the Privacy Rule preempts state law. Many of the provisions in the Privacy Rule do not have directly corresponding provisions in state laws. This makes comparing the two sets of rules a technical and tedious task. It is likely that one of the main impediments to a covered entity complying with the Privacy Rule is lack of understanding of what the Privacy Rule actually requires in each state (Pritts 2002).

European Law

An October 1998 directive prohibited European Union (EU) countries from permitting the transfer of personal data to another country without ensuring that an “adequate level of protection” exists in that country. In July 2000, the European Commission concluded that the U.S. Safe Harbor Privacy Principles constituted adequate protection.⁵⁴ These principles are similar to the principles embodied in the Privacy Rule, and include: 1) notice, 2) consent, 3) subsequent disclosure, 4) security, 5) data integrity, 6) access, and 7) enforcement. U.S. companies are not required to comply with these principles, so only those organizations wishing to process data on European citizens are concerned with these principles. However, since the principles embodied in the Safe Harbor Privacy Principles are similar to the mandatory Privacy Rule regulations, it is likely that many companies will be in compliance with the relevant principles without exerting much effort (Department_of_Health_and_Human_Services 2000).

Enforcement of the Privacy Rule

The Privacy Rule has not been aggressively enforced by the Office for Civil Rights (OCR). As of today, there have been no civil penalties imposed against any

⁵⁴ Department of Commerce, Safe Harbor Principles, July 21, 2000.

covered entity for breaching the privacy of an individual. Similarly, there have only been two criminal prosecutions under the Privacy Rule (Rahman 2006).⁵⁵

The lack of enforcement of the Privacy Rule does not mean that individuals have not complained of privacy breaches. Between April 2003 and March 31, 2007, 26,408 complaints were received by OCR regarding violations of the Privacy Rule. OCR concluded that further investigation was needed in 6,602 of the complaints. Of these 6,602 complaints, OCR took informal action in 4,447 cases. In the 2,155 other cases, OCR found that there was no violation of the Privacy Rule. In the other 13,875 resolved cases, OCR determined that the complaint did not present an eligible case for enforcement, either because OCR lacked jurisdiction, the complaint was untimely, or the activity did not violate the Rule. Currently, 78% of the complaints have been closed, and 384 cases have been referred to the Department of Justice for a criminal investigation. (Department_of_Health_and_Human_Services 2007).

The majority of complaints that OCR has received deal with health information uses, disclosures and safeguards. OCR has also received a number of complaints about access to information, the minimum necessary standards, and violations of the authorization standards and notice. Most of the complaints have been filed against health care providers, including physician practices, general hospitals, pharmacies, and outpatient clinics. It is unclear how many complaints have been received by OCR that relate to research (National_Committee_on_Vital_and_Health_Statistics 2005).

Since the Privacy Rule has been so lightly enforced, it is not surprising that a large number of providers and payers self-report that they are not in compliance with the rule. A recent survey by Phoenix Health Systems found that 20% of providers and 13% of payers report that they have had insufficient incentives to implement the required privacy practices. In the survey, not a single participating provider was able to show that it had complied with every provision of the Privacy Rule. Payers only reported doing marginally better (Phoenix_Health_Systems 2006).

It is possible that recent developments at HHS indicate that the Privacy Rule will be enforced more aggressively civilly in the future. On March 16, 2006 the final Enforcement Rule for HIPAA became effective.⁵⁶ The Enforcement Rule sets guidelines for imposing civil monetary penalties on entities found guilty of violating the Privacy Rule. It also adopts a comprehensive approach to enforcing all of the HIPAA Administrative Simplification Rules (Security Rule, Electronic Transaction and Code Set Rule, and the Identifier Standards.) However, the Enforcement Rule does not effect the enforcement of criminal sanctions under the Privacy Rule, because this responsibility remains with the Department of Justice (Rahman 2006). A second indicator that enforcement might increase is the fact that on April 16, 2007 the Secretary of HHS delegated to the Director of OCR the authority to issue subpoenas in investigations of alleged violations of the Privacy Rule. This permits the Director of OCR to subpoena witnesses to testify before HHS and to issue subpoenas to produce any evidence that relates to a matter under investigation (Department_of_Health_and_Human_Services 2007).

⁵⁵ See U.S. v. Gibson, 2004 WL 2188280 (W.D. Wash. 2004) and U.S. v. Ramirez, Warrant, Criminal No. M-05-708, McAllen Division.

⁵⁶ 42 U.S.C. § 1320d-5(a).

Although the Privacy Rule may result in a greater number of civil suits in the future, it is unlikely that the criminal enforcement of the Privacy Rule will be increased. The Office of the Legal Counsel at the Department of Justice issued an opinion on June 1, 2005 limiting the applicability of the criminal provisions of the Privacy Rule to encompass only covered entities. This means that physicians can be criminally prosecuted under the Privacy Rule, since they qualify as covered entities. However, most employees of covered entities (such as ward clerks, administrative assistants, etc.) can never be criminally liable for privacy breaches under the Privacy Rule, because they are not covered entities. Similarly, hackers and individuals who are unassociated with covered entities, who breach the privacy provisions of the Privacy Rule, cannot be criminally prosecuted because they are not covered entities (Office_of_Legal_Counsel 2005).

This opinion instituted a change from earlier policy. Prior to the Office of Legal Counsel's opinion, it was believed to be possible for any individual who violated the Privacy Rule to be criminally sanctioned under the regulations. An article written by Robert Gellman suggests an alternative method of criminally prosecuting individuals who do not qualify as covered entities under the Privacy Rule, but who violate some aspect of this regulation. The criminal statute, 18 U.S.C. § 2, provides for a criminal penalty for any person who willfully causes an act, which if performed by another, would be a criminal offense. It is possible that non-covered entities (including ward clerks, administrative assistants, and hackers) could be criminally prosecuted for violations of the Privacy Rule under 18 U.S.C. § 2. However, there have not been any cases making use of this legal strategy yet (Gellman 2006).

Recommendations to HHS to Improve the Privacy Rule

Since the compliance date for the Privacy Rule passed, there have been numerous case studies and smaller surveys reporting that the Privacy Rule has had a negative effect on researcher's ability to access necessary health data. In 2004, a series of articles in the *San Francisco Chronicle* reported that the Privacy Rule was forcing 17 hospitals, including the Medical Center at the University of California San Francisco, to restrict researchers' access to California's Cancer Registry. This registry had been recording the names and address of all California residents diagnosed with cancer in the last 16 years, and was used by researchers all over the country to study cancer (Russell 2004; Russell 2004).

A similar series of articles was published in 2006, reporting that a 25 year study into stroke and heart disease was being ended because of the implementation of the Privacy Rule. Prior to HIPAA, researchers were allowed to examine the medical records of over 40,000 residents of Minnesota to gain data on stroke and heart disease. This study produced over 200 medical research papers. However, data collection is now on hold because of the Privacy Rule, and no additional grant money has been sought for this project (Kaiser 2006; Shaffer 2006).

More quantitative data have been collected in several studies examining pre- and post- HIPAA research recruitment rates. One study showed that participation rates in an outcomes research project decreased from 96.4% pre-HIPAA, to 34.0% post-HIPAA (Armstrong, Kline-Rogers et al. 2005). At the National Cancer Policy Forum (NCPF)

workshop, “Effect of the HPA Privacy Rule on Health Research,” Roberta Ness of the University of Pittsburg reported that recruitment rates for two studies that she is involved with were cut in half after the Privacy Rule was implemented. A study on preeclampsia in pregnant women, recruited 10 women per week from 1998-2002, and only 5 women per week after April 2003. Similar results were seen in an ovarian cancer study she is overseeing (Ness 2005; Institute_of_Medicine 2006).

Many other researchers are reporting that the Privacy Rule is greatly affecting their ability to conduct meaningful studies. A survey of the membership of the North American Association of Central Cancer Registries (NAACCR) found that 19% of its members reported that the Privacy Rule has stopped or prevented a research project from being conducted. 68% reported that the Privacy Rule has delayed a research project or caused it to take longer than it otherwise would have taken, and 36% stated that HIPAA has possibly introduced bias into a research project (Deapen 2006). A similar study presented by Carol Stocks, Agency for Healthcare Research and Quality, at the NCPF workshop also found that the research community is reporting that the Privacy Rule has had a significant effect on research. 90% of respondents in this survey reported that they made changes to how they planned for and conducted research after the Privacy Rule, 87% reported increased time for IRB preparation and participant recruitment, and 45% reported a study had been stopped or altered because of the rule (Walker 2005; Institute_of_Medicine 2006).

The Privacy Rule has also had a reported impact on the institutions which provide many researchers with access to PHI. One study suggested that HIPAA has greatly increased the workload and responsibilities of covered entities’ IRBs (O’Herrin, Fost et al. 2004). In addition, the Privacy Rule has increased the cost of conducting research. At John Hopkins alone, 26,000 employees have been required to take HIPAA compliance training. John Hopkins estimated that it will cost an additional \$2 million annually to comply with HIPAA (Friedman 2006).

Because of the reported problems with the Privacy Rule’s regulation of research, several different organizations have provided HHS with recommendations on ways to improve the rule. The recommendations of the National Committee on Vital and Health Statistics, the Association of American Medical Colleges, and the Secretary’s Advisory Committee on Human Research Protections are discussed below.

The National Committee on Vital and Health Statistics

Congress gave the National Committee on Vital and Health Statistics (NCVHS) the responsibility of advising the Secretary of HHS on the adoption of the Privacy Rule standards, monitoring its implementation, and reporting annually to Congress on the progress made in its adoption (National_Committee_on_Vital_and_Health_Statistics 2005). In accordance with this mandate, NCVHS has held a number of hearings on the Privacy Rule and the problems that the medical community has experienced in implementing the requirements of the rule. One of the topics explored during these hearings was the obstacles associated with conducting research under the Privacy Rule. After each hearing, NCVHS subsequently issued a letter to the Secretary of HHS with a set of recommendations for improving the rule.

The first public hearing held by the NCVHS Subcommittee on Privacy and Confidentiality was held August 21-23, 2001. A number of different speakers presented their concerns regarding the implementation of the December 2000 version of the Privacy Rule. (As mentioned above, the final version of the Privacy Rule was not published until 2002.) One of the issues covered during the hearings was the projected effect the rule would have on health research. Based on the information gathered during the hearing, NCVHS issued a number of recommendations to HHS on the research provisions of the Privacy Rule.

First, NCVHS recommended that HHS provide further interpretations, guidance and technical assistance to help the research community understand the relationship between the Privacy Rule and the Common Rule. Second, some witnesses at the hearing suggested that research should be included as part of the “treatment, payment and health operations” (TPO) exception, and allow covered entities to disclose PHI without authorization for research purposes. NCVHS rejected this suggestion. It recommended keeping research separate from the TPO provision, and continuing to require either authorization or IRB/privacy board waiver of authorization for the use or disclosure of PHI for research purposes. Third, NCVHS recommended that HHS take a careful look at whether the de-identification provisions of the Privacy Rule unduly interfere with research. Depending on the findings of this investigation, HHS should research alternative methods of de-identifying data.

Fourth, NCVHS recommended that HHS should provide guidance or an alternative way for researchers to recruit research subjects under the Privacy Rule. NCVHS found that the proposed mechanism for recruiting was too cumbersome and difficult. Fifth, witnesses at the hearing suggested that covered entities were likely to refuse to share PHI because of the burden of accounting for disclosures. NCVHS stated that it supported an individual’s right to an accounting for disclosures. However, NCVHS suggested that HHS issue guidance to provide covered entities with ways to fulfill this requirement in a convenient and practical manner. Finally, NCVHS recommended that HHS make the research provisions a priority for education and outreach efforts. There was considerable misunderstanding about the Privacy Rule, and what the regulations actually required of researchers at this time (National_Committee_on_Vital_and_Health_Statistics 2001).

On November 19- 20, 2003, the NCVHS Subcommittee on Privacy and Confidentiality held another set of hearings on the Privacy Rule. Witnesses reported less confusion with the Privacy Rule and research at this hearing than at the first hearing. However, NCVHS issued another letter to the Secretary of HHS with recommendations on ways to improve the rule in regards to its regulation of research. One of the main points of this letter was that there is still a great need for HHS to expand its outreach and public education activities concerning the Privacy Rule. NCVHS also made several more detailed recommendations.

First, NCVHS recommended that HHS make further efforts to harmonize the Privacy Rule with the Common Rule. Many research projects fall under the jurisdiction of both rules. However, the two rules differ in key ways which makes it difficult for researchers to know which actions are permitted and which are not. For example, the two rules diverge in their regulation of activities that are preparatory to research. The Privacy Rule permits PHI to be reviewed by researchers for purposes that are preparatory to

research without getting authorization or IRB waiver of authorization. According to guidance issued by HHS interpreting the “preparatory to research” provisions, researchers who are workforce members of a covered entity are permitted to recruit potential research subjects as part of the covered entity’s health care operations. This allows the recruitment of research subjects without getting IRB approval. However, under the Common Rule, researchers must get IRB approval before any recruitment of research subjects takes place (National_Committee_on_Vital_and_Health_Statistics 2004).

Second, NCVHS recommended that HHS should clarify that the Privacy Rule neither requires nor precludes IRB review of stand-alone authorizations for the use or disclosure of PHI in research. The Privacy Rule permits an authorization form to be combined with informed consent documents, but according to guidance issued by HHS, the Privacy Rule does not require IRB review of authorizations, even when they are combined with informed consent documents. However, IRBs are required to review informed consent documents under the Common Rule. NCVHS recommended that HHS clarify that there is nothing in the Privacy Rule that prevents IRBs from reviewing authorization forms when considering the adequacy of privacy and confidentiality of subjects under the Common Rule (National_Committee_on_Vital_and_Health_Statistics 2004).

Third, HHS needs to harmonize the Privacy Rule’s regulation of future research with the Common Rule’s regulation in this area. Under the Common Rule, research subjects may provide informed consent for future unspecified research, but the Privacy Rule prohibits this. The only way to conduct future research without getting authorization under the Privacy Rule is to get an IRB waiver of authorization. This additional step complicates the process. Fourth, NCVHS stated that the Privacy Rule’s regulation of genetics research needs to be clarified by HHS. Under the Privacy Rule it is unclear whether DNA samples can be considered anonymous, since analyzing the samples could reveal unique DNA identifiers of the individual. Finally, NCVHS suggested that HHS provide guidance on the applicability of the Privacy Rule to indirect participants (individuals who are not research subjects, but whose PHI may be disclosed by research subjects), and on multi-institutional studies (National_Committee_on_Vital_and_Health_Statistics 2004).

In 2006, NCVHS issued another letter to the Secretary of HHS recommending that the agency consider extending the Privacy Rule to include other forms of health information not managed by covered entities. This would mean that all individually identifiable health information would be protected regardless of the institution that held the information (National_Committee_on_Vital_and_Health_Statistics 2006; National_Committee_on_Vital_and_Health_Statistics 2006).

The Association of American Medical Colleges

The Association of American Medical Colleges (AAMC) has publicly opposed the current research provisions of the Privacy Rule since the final rule was proposed in 2002. During the notice of proposed rulemaking period, it submitted a lengthy and detailed comment urging HHS not to apply the Privacy Rule to research. AAMC has continued to campaign for a change in the rule’s regulation of research since it became

law. AAMC sent a representative to the NCVHS Subcommittee hearing on privacy in November 2003 to present its criticism of the current rule. It also sent a representative on request to the NCPF meeting on the effect of the Privacy Rule on cancer research in February 2006.

In the spring of 2003, AAMC conducted a survey of 331 investigators, IRB personnel, privacy officials, research administrators, deans and others involved in research, to gain knowledge about how the Privacy Rule has influenced the research process. AAMC then created a database of qualitative case reports documenting research projects that were affected, delayed, hindered, benefited, abandoned, or foregone because of the Privacy Rule. The results of the survey showed that many research functions have been affected by the implementation of the Privacy Rule. 74% of those surveyed reported that the Privacy Rule had a negative affect on patient recruitment, 76% on data access, 68% on data acquisition, 51% on data retention, 47% on oral communication, and 34% on written publication of research studies. The Privacy Rule's main effects on research participants that were documented in the database included increased confusions about research studies, diminished access to opportunities to participate in research, and a burdensome informed consent process. The main effects on researchers were difficulty collaborating with other researchers, increased bureaucracy and staffing needs, a negative impact on the quality and cost of research, and confusion over differing interpretations of the Rule's requirements.

Based on the results of the survey, AAMC came up with a number of recommendations for improving the Privacy Rule's regulation of research. First, AAMC recommended changing the accounting for disclosures provision the Privacy Rule. The case reports gathered for AAMC's database indicated that this provision is a tremendous burden to providers and researchers, and has resulted in many covered entities refusing to make PHI available to researcher. AAMC recommended that the accounting for disclosure requirement be eliminated for research, if IRB approval is given. AAMC stated that most accountings for disclosures do not provide any meaningful or relevant information to the individual. A better system would be to investigate any questionable disclosures as they occur, rather than provide an individual with a record of all disclosures.

Second, AAMC stated that the process for obtaining an authorization or waiver of authorization is burdensome and discourages both providers and participants from taking part in research. Plus, this section of the Privacy Rule provides only minimal additional privacy protections beyond the protections given by the Common Rule. AAMC recommended that the requirement for authorizations and waiver of authorizations be eliminated for research purposes. AAMC believes that research disclosures are adequately protected by the Common Rule. HHS should harmonize the Privacy Rule with the Common Rule to reduce confusion, and eliminate the duplicative set of regulations.

Third, AAMC recommended that the de-identification standard in the Privacy Rule be revised. The respondents to AAMC's survey suggested that the de-identification standards remove too much important information, and create data that are useless for many types of health research. Instead, AAMC believes that HHS should simplify the de-identification standard to produce data that can be easily used in biomedical and health sciences research. The current rule is needlessly protecting against the most

extreme cases of misuses of medical information. Instead, it should focus on providing a more basic privacy protection.

Fourth, AAMC recommended that HHS create a new classification system for the types of organizational structures that are permitted under the Privacy Rule (i.e. covered entity, hybrid entity, and affiliated covered entity). The AAMC survey suggested that the Privacy Rule prevents academic medical centers from organizing in a manner which reflects the functional operations of medical schools, affiliated practice plans, and teaching hospitals. AAMC recommended that the covered entity status, hybrid entity status, and affiliated covered entity status be re-defined to reflect the function served by the different parts of the organization, not the organizational form (Ehringhaus 2003).

The AAMC recommendations have not been received very positively because the survey that AAMC used in formulating its recommendations has been criticized. The survey was launched on April 14, 2003, the same day as the compliance date for the Privacy Rule. As a result, the survey did not permit any lapse in time for initial compliance problems to be resolved or for researchers to become familiar with working under the new regulations. Some of the negative impacts of the Privacy Rule reported in the AAMC survey may be due to the fact that there was no opportunity for the transitional problems to be resolved. Also, the study has been criticized for reflecting the viewpoints of a biased group of respondents. Only a select group of individuals was asked to complete the survey and provide AAMC with insight into the Privacy Rule's research provisions, and the response rate was low (Institute_of_Medicine 2006).

The Secretary's Advisory Committee on Human Research Protections

The Secretary's Advisory Committee on Human Research Protections (SACHRP) was charged with advising the Secretary of HHS on human subject research and the protection of human subjects. On March 30, 2004 SACHRP received presentations from a number of different medical experts on the Privacy Rule's impact on human subject research. Based on these presentations, SACHRP submitted recommendations to HHS on September 1, 2004, on areas of the Privacy Rule that need clarification or modification.

First, SACHRP recommended that the use of PHI for research purposes be exempted from the Privacy Rule's accounting for disclosures requirement. As suggested by AAMC, accounting for disclosures is a huge administrative burden. SACHRP stated that the Privacy Rule imposes sufficient privacy protections without applying this portion of the Privacy Rule to research. Researchers must establish a certain standard of privacy protections before an IRB or Privacy Board will grant a waiver of authorization, or before a covered entity will permit a researcher to access PHI preparatory to research. Instead of being required to make accountings for disclosures, covered entities should inform patients in the "Notice of Privacy Practices" that their PHI may be used and disclosed for research purposes without their authorizations, if sufficient privacy safeguards are in place.

Second, SACHRP recommended that HHS reduce the number of data categories that must be eliminated for data to be considered de-identified. In particular, it should be permissible for de-identified data to retain zip codes, geographical subdivisions and treatment dates. This change would more closely align the Privacy Rule with the

Common Rule, and the change would enhance researchers' ability to use de-identified data in conducting important health research.

Third, similar to NCVHS' recommendation, SACHRP recommended that HHS clarify its position on the recruitment of research subjects. As described above, in the section on the current Privacy Rule, both researchers who are employed by the covered entity, and researchers who are independent of the covered entity, are permitted to conduct a review of PHI preparatory to research to identify potential research subjects. However, only researchers employed by the covered entity may contact the potential subjects without IRB approval as part of the covered entity's health care operations. Researchers that are independent of the covered entity are required either to seek authorization through some intermediary to receive a partial waiver of authorization for recruitment purposes, or become business associates of the covered entity to perform this same task.

To address this inconsistency, SACHRP recommended that HHS provide a clear statement that PHI may be used and disclosed by covered entities for research recruitment under the "preparatory to research" provision for all researchers. This would eliminate the distinction between researchers employed by the covered entity, and researchers not employed by the covered entity. It would also eliminate the distinction between activities preparatory to research and recruiting research subjects. There would be little impact on privacy as a result of this change, because IRBs are required to ensure that any recruitment activities are appropriate and ethical under the Common Rule.

Fourth, SACHRP recommended amending several aspects of the Privacy Rule's research authorization requirements. The Common Rule permits an IRB to review and approve consent forms for future research, but the current Privacy Rule does not allow authorization for future uses of PHI. SACHRP recommended revising the Privacy Rule so that when an IRB has considered and approved a consent form for certain future uses under the Common Rule, the Privacy Rule would permit authorization of that future use. Another area needing revision is the Privacy Rules' compound authorization requirements. Under the Privacy Rule, authorization can only be combined with a written permission from the same research study. SACHRP recommended that HHS clarify that the creation of a research database or repository, and the subsequent use or disclosure of the data stored in that database or repository can be authorized in one permission form. Further, SACHRP recommended that HHS revise the categories for which authorization is not required, so that those categories are consistent with the categories of research exempt under the Common Rule.

Fifth, SACHRP recommended that HHS clarify the role of the Privacy Rule in international research. Covered entities differ in their interpretation of how the Privacy Rule applies to foreign nationals. Some covered entities have concluded that the Privacy Rules applies to the use of foreign national's PHI by U.S. covered entities, even if the disclosures are outside the United States. Other covered entities have come to the opposite conclusion, and have interpreted the Privacy Rule as not applying in this situation since foreign laws apply. SACHRP recommended that HHS clearly state that PHI collected from foreign nationals outside the United States is not subject to the Privacy Rule. Alternatively, if HHS determines that the Privacy Rule does apply to foreign nationals, researchers should be able to use a simplified authorization form to ensure that individuals in developing countries can understand the forms.

Finally, SACHRP made recommendations for conducting public health research under the Privacy Rule. Currently, the Privacy Rule permits a covered entity to use and disclose PHI to a public health authority, if the public health authority is “authorized by law” to receive PHI. Many covered entities have been hesitant to disclose information to federal and state agencies that do not technically meet the definition “authorized by law.” SACHRP recommended broadening the definition of public health authority to ensure that all agencies that are responsible for disease prevention, injury or disability clearly qualify as public health authorities under the definition of public health authority (Secretary's_Advisory_Committee_On_Human_Research_Protections 2005; Secretary's_Advisory_Committee_On_Human_Research_Protections 2006).

[PLACE HOLDER: If the committee adopts any of the above suggestions, Marc Rotenberg suggests anticipating likely privacy concerns by explaining how these data, if the Privacy Rules is suspended, will not be used for other purposes, such as insurance or employment determinations, that might negatively impact the data subject.]

Current Debate: Nationwide Health Information Exchange Network

As the procedural history of HIPAA demonstrates, the use of electronic health records has been a topic of political debate for a number of decades. Recently, under President Bush, electronic health records have gained increased attention as a means of addressing rising health care costs, and improving the quality and efficiency of healthcare. Privacy issues are emerging as the primary obstacle to the use of electronic health records, with many privacy and consumer groups pushing for tighter privacy protections than offered under the Privacy Rule. The outcome of the current privacy debate is relevant to health researchers, because the resulting rules will likely have a large effect on researchers’ ability to access data and conduct meaningful health research within an electronic health care system. This section of the paper will set out the current developments in the creation of a nationwide health information network (NHIN) and potential new privacy regulations.

The momentum for the current debate started in 2004 when President Bush issued an executive order calling for the widespread adoption of interoperable electronic health records within 10 years. The executive order designated HHS as the federal agency responsible for overseeing the development of this new system. Bush recognized that privacy issues were likely to become a major point of public contention, and included a directive in the executive order stating that privacy issues must be addressed as HHS implemented the NHIN. Additionally, this order established the position of the National Coordinator of Health Information Technology within HHS. This individual is the government official responsible for overseeing the development and implementation of a NHIN, and reports to the Secretary of HHS regarding any problems (Bush 2004).

To implement the requirements of the executive order, in 2005, HHS awarded several health information technology contracts to different companies to provide policy makers within HHS with information about the privacy and security issues resulting from a NHIN. The contractor responsible for providing potential privacy solutions to a NHIN selected 33 states and Puerto Rico to perform assessments of organizational-level privacy

policies in 2006. The results of these assessments are not yet available (Government_Accountability_Office 2007).

Also in 2006, NCVHS made recommendations to the Secretary of HHS on protecting the privacy of health information within a NHIN. These recommendations were based on 5 hearings held in 2005 by the NCVHS Subcommittee on Privacy and Confidentiality. The recommendations covered a number of different topics, including: 1) the importance of privacy and confidentiality in a NHIN, 2) the role of the individual in making decisions about whether to participate in the NHIN, and their ability to control access to their electronic health records, 3) guiding principles for the controlled disclosures of PHI in a NHIN, 4) regulatory issues, such as jurisdiction, procedures and enforcement, 5) secondary uses of PHI in a NHIN, and 6) establishing and maintaining public trust (National_Committee_on_Vital_and_Health_Statistics 2006).

A second advisory body that provides HHS with advice on creating a NHIN is the American Health Information Community (AHIC). AHIC was formed by the Secretary of HHS in 2005 to help achieve the goal of using electronic health records by 2014. In May 2006, AHIC delivered its first set of recommendations to HHS in a letter sent to Secretary Leavitt. AHIC recommended that by September 30, 2006, HHS should have completed a review of the current laws regulating the release of health information, and determined which require HIPAA guidance, regulation change and/or statute change. AHIC also recommended that a subgroup comprised of privacy, security, clinical and technology experts be created within AHIC to frame the privacy and security issues relevant to the use of NHIN. This subgroup would solicit broad public input and testimony on this issue. In August 2006, the subgroup was created, and it is expected to deliver recommendations to HHS in 2007 (AHIC 2006).

More recently, Senators Daniel Akaka and Edward Kennedy asked the Government Accountability Office (GAO) to study HHS' steps in implementing a NHIN to ensure that privacy protections were included in the strategy. In January 2007, GAO issued its report. The report criticized HHS for failing to define an overall approach for protecting privacy. GAO recommended that HHS create milestones for integrating the outcomes of the ongoing privacy-related initiatives. It also recommended identifying the entity responsible for overseeing the integration of the many privacy initiatives, and ensuring that the privacy principles in HIPAA are fully addressed. The GAO report cites the following items as the key challenges associated with a NHIN: 1) variations in states' privacy laws, 2) ensuring that only the minimum amount of information necessary is disclosed to entities authorized to receive PHI, 3) ensuring individuals have the right to access and amend their PHI, and 4) implementing adequate security measures for protecting PHI. HHS has publicly disagreed with these recommendations, stating that identifying milestones will impede the process of protecting privacy (Government_Accountability_Office 2007).

Based on the results of this GAO report, the Senate Homeland Security and Governmental Affairs Committee's Subcommittee of Oversight of Government Management, the Federal Workforce and DC, held a hearing on the privacy issues involved in creating a NHIN. Mark Rothstein (Director, Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine, and Chair of the Subcommittee on Privacy and Confidentiality in NCVHS) testified at the hearing. He stated that HHS has made little meaningful progress in developing and implementing

measures necessary to protect privacy in a NHIN. The policy developments needed to protect privacy are lagging behind the technical developments used to create a NHIN. Rothstein recommended that Congress condition additional appropriations for a NHIN on HHS demonstrating that it is addressing the existing privacy concerns. Additionally, he suggested that HHS be required to submit a report to Congress identifying the gaps in coverage of the HIPAA Privacy Rule in a NHIN, and ways to address these gaps (Rothstein 2007).

Carol Diamond (Managing Director, Markle Foundation, and Chair, Connecting for Health) also testified at the congressional hearing. She echoed the results of the GAO report and Mark Rothstein's testimony, in expressing concern that HHS is not developing the necessary policies to protect privacy within a NHIN. She believes that the technological design decisions for a NHIN must be made alongside the policy decision to protect privacy. For the past three years, the Markle Foundation and 100 other health stakeholders, through Connecting for Health, have been developing an approach for creating an electronic health system with the necessary privacy protections. Connecting for Health produced a list of attributes that must be present in any successful NHIN. They include: 1) a decentralized architecture, rather than a centralized repository of health information, 2) an index that separates demographic information from clinical information, 3) a flexible platform for innovation, and 4) a list of foundational privacy principles (Diamond 2007).

Consumer groups have also become actively involved in the NHIN debate, and are pushing Congress to include strong privacy principles in any NHIN that is created. 44 different organizations have sent letters to congress expressing concern that current health IT proposals lacks adequate privacy protections (Patient_Privacy_Rights 2007). Patient Privacy Rights (PPR) has been particularly vocal on this issue. In a letter sent to the Secretary of HHS, this group expressed its agreement with the GAO report's conclusion that HHS needs to develop a comprehensive privacy approach. However, PPR wants HHS to develop a new privacy framework from start to finish, rather than rely on the HIPAA Privacy Rule for the protection of medical privacy. PPR stated that the HIPAA Privacy Rule has become a "disclosure rule," not a privacy protection rule (Patient_Privacy_Rights 2007).

Although it is unclear whether privacy protections for a NHIN will be worked into the existing HIPAA Privacy Rule, or be a separate set of privacy principles, it is likely that public demand will ensure that privacy protections are addressed in any NHIN that is created. Public opinion polls reveal that the general population wants strong privacy protections. In a September 2006 poll, 62% of respondents stated that the use of electronic health records will pose new risks to privacy, and only 42% answered that the privacy risks of NHIN outweigh expected benefits (Harris_Interactive 2007). A separate poll found that 80% of Americans say they are very concerned about identify theft or fraud in a NHIN, and 77% are very concerned about the possibility of their information getting into the hands of marketers (Markle_Foundation 2006).

As an NHIN develops it is likely that new rules governing the privacy of medical records will be developed. This healthcare-wide change will have dramatic effects on medical researchers. Researchers will have to work with the new system, and develop research protocols and study designs that abide by any new privacy legislation or changes to the Privacy Rule. As this area of law is developing, researchers and the medical

community should participate in the policy debate to ensure that the resulting privacy rules allow meaningful health research to take place without unnecessary burdens.

References

- AHIC (2006). Letter to Michael Leavitt.
- Armstrong, D., E. Kline-Rogers, et al. (2005). "Potential Impact of the HIPAA Privacy Rule on Data Collection in a Registry of Patients With Acute Coronary Syndrome." *Archives of Internal Medicine* **165**(10): 1125-1129.
- Bush, G. W. (2004). "Executive Order 13335." *69 Fed. Reg.* 24059.
- Centers_for_Medicare_and_Medicaid_Services. (2005). "Overview: Security Standards." Retrieved March 27, 2007, from <http://www.cms.hhs.gov/SecurityStandard/>.
- Chaikind, H., J. Hearne, et al. (2005). The Health Insurance Portability and Accountability Act (HIPAA) of 1996: Overview and Guidance on Frequently Asked Questions. *CRS Report for Congress*.
- Damschroder, L. J., J. L. Pritts, et al. (2007). "Patients, privacy and trust: Patients' willingness to allow researchers to access their medical records." *Social Science & Medicine* **64**(1): 223-235.
- Deapen, D. (2006). "Cancer Surveillance and Information: Balancing Public Health with Privacy and Confidentiality Concerns (United States)." *Cancer Causes and Control* **17**(5): 633-637.
- Deapen, D. (2006). Negative Impact of HIPAA on Population-Based Cancer Registry Research: A Brief Survey, North American Association of Central Cancer Registries.
- Department_of_Health_and_Human_Services. "Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule." Retrieved April 17, 2007, from http://irb.ucsd.edu/NIH_HIPAA_Booklet_4-2003.pdf.
- Department_of_Health_and_Human_Services Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule. D. o. H. a. H. Services, NIH.
- Department_of_Health_and_Human_Services (2000). "Standards for Privacy of Individually Identifiable Health Information; final rule " *65 Fed. Reg.* 82462.
- Department_of_Health_and_Human_Services (2002). "Standards for Privacy of Individually Identifiable Health Information; Final Rule." *67 Fed. Reg.* 53,182: 53,182- 53,273.
- Department_of_Health_and_Human_Services (2003). Institutional Review Boards and the HIPAA Privacy Rule.
- Department_of_Health_and_Human_Services (2004). Clinical Research and the HIPAA Privacy Rule, NIH.
- Department_of_Health_and_Human_Services. (2007). "Compliance and Enforcement: Privacy Rule Enforcement Highlights." Retrieved April 25, 2007.
- Department_of_Health_and_Human_Services (2007). "Office for Civil Rights: Delegations of Authority." *72 Fed. Reg.* 18999.
- Diamond, C. (2007). Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative Markle Foundation.

- Ehringhaus, S. (2003). Testimony on Behalf of the Association of American Medical Colleges Before the National Committee on Vital and Health Statistics Subcommittee on Privacy: 1-11.
- Feld, A. D. and A. D. Feld (2005). "The Health Insurance Portability and Accountability Act (HIPAA): its broad effect on practice." American Journal of Gastroenterology **100**(7): 1440-3.
- Forrester_Research (2005). National Consumer Health Privacy Survey 2005. California_Healthcare_Foundation.
- Friedman, D. S. (2006). "HIPAA and research: how have the first two years gone?" American Journal Of Ophthalmology **141**(3): 543-546.
- Gallup_Organization (2000). Public Attitudes Toward Medical Privacy. Institute_for_Health_Freedom.
- Gellman, R. (2006). "Crimes and Sanctions." Journal of AHIMA.
- Gostin, L. O. (2008 (unpublished)). Surveillance and Public Health Research: Personal Privacy and the "Right to Know". Public Health Law: Power, Duty, Restraint. Berkeley, U.Cal. Press.
- Gostin, L. O., Z. Lazzarini, et al. (1996). "The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy " JAMA **275**: 1921-1927.
- Government_Accountabilty_Office (1996). Scientific Research: Continued Vigilance Critical to Protecting Human Subjects. Report to the Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate: 1-46.
- Government_Accountabilty_Office (2007). Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy.
- Harris_Interactive. (2005). "Health Information Privacy (HIPAA) Notices have Improved Public's Confidence that their Medical Information is being Handled Properly " Retrieved April 3, 2007, from www.harrisinteractive.com/news/printerfriend/index.asp?NewsID=849
- Harris_Interactive. (2007). "The Benefits of Electronic Medical Records Sound Good, but Privacy Could Become a Difficult Issue." Retrieved April 3, 2007, from www.harrisinteractive.com/news/printerfriend/index.asp?NewsID=1174.
- Harris_Interactive. (2007). "Many U.S. Adults are Satisfied with Use of their Personal Health Information " Retrieved May 15, 2007, from http://www.harrisinteractive.com/harris_poll/index.asp?PID=743.
- Hawaii_Medical_Service_Association. (2000). "A History and Overview of HIPAA." Retrieved January 23, 2007, from www.hipaadvisory.com/regs/hipaahistorybyzon.htm.
- Hodge, J. G., Jr., L. O. Gostin, et al. (1999). "Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability." JAMA **282**(15): 1466-1471.
- Institute_of_Medicine (2006). Effect of the HIPAA Privacy Rule on Health Research: Proceedings of a Workshop Presented to the National Cancer Policy Forum. N. A. Press. Washington, DC.
- Kaiser, J. (2006). "Patient privacy. Rule to protect records may doom long-term heart study." Science **311**(5767): 1547-8.

- Kass, N. E., M. R. Natowicz, et al. (2003). "The Use of Medical Records in Research: What do Patients Want?" Journal of Law, Medicine & Ethics **31**.
- Markle_Foundation (2006). Survey Finds Americans want Electronic Personal Health Information to Improve Own Health Care.
- National_Committee_on_Vital_and_Health_Statistics (2001). Letter to Secretary Thompson Reporting on HIPAA.
- National_Committee_on_Vital_and_Health_Statistics (2004). Letter to Secretary Thomson - Recommendation on the effect of the Privacy Rule: 4.
- National_Committee_on_Vital_and_Health_Statistics (2005). Seventh Annual Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA): 18.
- National_Committee_on_Vital_and_Health_Statistics (2006). Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network (NHIN).
- National_Committee_on_Vital_and_Health_Statistics (2006). Personal Health Records and Personal Health Record Systems. Washington, DC.
- National_Research_Council (2007). Engaging Privacy and Information Technology in a Digital Age (Prepublication copy). Washington, DC.
- Ness, R. B. (2005). "A year is a terrible thing to waste: early experience with HIPAA." Annals of Epidemiology **15**(2): 85-86.
- O'Herrin, J. K., N. Fost, et al. (2004). "Health Insurance Portability Accountability Act (HIPAA) Regulations: Effect on Medical Record Research." Annals of Surgery **239**(6): 772-778.
- Office_of_Civil_Rights (2002). OCR Guidance Explaining Significant Aspects of the Privacy Rule
- Office_of_Legal_Counsel (2005). Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6.
- Office_of_Technology_Assessment (1993). Protecting Privacy in Computerized Medical Information. OTA-TCT-576. Washington, DC, U.S. Government Printing Office.
- Patient_Privacy_Rights (2007). Letter to Senators Akaka and Kennedy.
- Patient_Privacy_Rights (2007). Passing HIT Legislation without Privacy Protections is a Prescription for Disaster. Austin, TX.
- Phoenix_Health_Systems. (2006). "US Healthcare Industry HIPAA Compliance Survey Results: Summer 2006." Retrieved April 5, 2007, from www.hipaadvisory.com/action/surveynew/.
- Pritts, J. (2002). Implementation of the Federal Standards for Privacy of Individually Identifiable Health Information Testimony before the National Committee on Vital and Health Statistics, Subcommittee on Privacy and Confidentiality
- Pritts, J. L. (2002). "Altered States: State health Privacy Laws and the Impact of the Federal Health Privacy Rule." Yale Journal of Health Policy, Law & Ethics **2**.
- Rahman, N. (2006). "Medical: Reflections on Privacy: Recent Developments in HIPAA Privacy Rule " I/S: A Journal of Law and Policy for the Information Society **2**.
- Redhead, C. S. (2001). Health Information Standards, Privacy and Security: HIPAA's Administrative Simplification Regulations. CRS Report for Congress.
- Rothstein, M. A. (2007). Capitol Hill Hearing Testimony Congressional Quarterly, Inc. . Washington, DC.

- Russell, S. (2004). Dispute on medical record access settled; Cancer researchers wanted UC data on new cases quicker. San Francisco Chronicle. San Francisco. **Bay Area Section: B1.**
- Russell, S. (2004). Medical privacy law said to be chilling cancer studies; Scientists fight for fast access to patient files. San Francisco Chronicle. San Francisco. **News Section: A4.**
- Saver, R. (2006). "Medical Research and Intangible Harm." University of Cincinnati Law Review **74.**
- Secretary's_Advisory_Committee_On_Human_Research_Protections. (2005). "Summary of SACHRP's Recommendations on the HIPAA Privacy Rule." Retrieved March 10, 2006, from <http://www.hhs.gov/ohrp/sachrp/tableofrecommendations.html>
- Secretary's_Advisory_Committee_On_Human_Research_Protections (2006). Letter to Secretary Thompson
- Shaffer, D. (2006). Privacy Laws Jeopardize Heart Study: Researchers have put a well-known stroke and heart disease study on hold. Star Tribune. Minneapolis.
- Shalala, D. E. (1997). Confidentiality of Individually-Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996.
- Solove, D. J., M. Rotenberg, et al. (2005). Information Privacy Law. New York, Aspen Publishers.
- Starr, P. (1999). "Health and the Right to Privacy." American Journal of Law & Medicine **25.**
- Stevens, G. M. (2000). Summary of the Proposed Rule for the Privacy of Individually Identifiable Health Information. CRS Report for Congress, Congressional Research Service: 1-26.
- Stevens, G. M. (2003). Compliance with the HIPAA Medical Privacy Rule. CRS Report for Congress, Congressional Research Service: 1-6.
- Turn, R. and W. H. Ware (1976). Privacy and Security Issues in Information Systems Santa Monica The Rand Corporation.
- Walker, D. K. (2005). Impact of the HIPAA Privacy Rule on Health Services Research, Abt Associates, Inc.
- Warren, S. and L. Brandeis (1890). "The Right to Privacy " Harvard Law Review **4(193).**
- Westin, A. (1967). Privacy and Freedom. New York, Atheneum.
- Workgroup_for_Electronic_Data_Interchange (1993). Workgroup for Electronic Data Interchange Report.

Appendix A: Table of Federal Privacy Statutes

Statute	Year	Privacy Protection
Freedom of Information Act	1966	Prevents individually identifiable medical information from being included in the release of information from a FOIA request
Fair Credit Reporting Act	1970	Protects the privacy of personal information used in consumer reports created by consumer reporting agencies, such as the Credit Bureau
Privacy Act	1974	Protects the privacy of health, research and other records held by federal agencies
Family Educational Rights and Privacy Act	1974	In most cases, schools must have written permission from a parent or student in order to release any information from a student's education record
Veterans Omnibus Health Care Act	1976	Protects the privacy of medical records relating to the treatment of drug abuse, alcohol abuse, infection with AIDS or sickle cell anemia, in the Department of Veterans Affairs
Right to Financial Privacy Act	1978	Requires government agencies to provide notice and an opportunity to object before a bank or other institution can disclose personal financial information to a government agency
Social Security Act, Section 1106	1986	Prohibits unauthorized disclosure of individually identifiable records held by the Department of Health and Human Services, Social Security and their contractors
Electronic Communications Privacy Act	1986	Establishes privacy protections for electronic communications, and prohibits unlawful access and disclosures of communication contents.
Clinical Laboratory Improvement Amendments	1988	Requires that clinical laboratories protect the confidentiality of test results and reports of patient and clinical study subjects. Medical information may only be disclosed to authorized persons as defined by state or federal law.
Public Health Service Act Health Omnibus Program Extension	1988	Provides for Certificates of Confidentiality that protect personally identifiable research information.
Video Privacy Protection Act	1988	Prevents the disclosure of personally identifiable video rental information, unless

		the consumer consents in writing
Employee Polygraph Protection Act	1988	Prevents employers from using lie detector tests, either for pre-employment screening or during the course of employment
Americans with Disabilities Act	1990	Employers must treat employees' and applicants' medical information and medical conditions confidentially
Drivers Privacy Protection Act	1994	Prohibits state departments of motor vehicles from disclosing personal information about any individual obtained by the department in connection with a motor vehicle record
Balanced Budget Act	1997	Added language to the Social Security Act to require Medicare+Choice organizations to establish safeguards for the privacy of individually identifiable patient information
Identity Theft and Assumption Deterrence Act	1998	Establishes that identity theft is a crime, and that the person whose identity was stolen is a victim. (Prior to this Act, only the credit grantors who suffered monetary losses were considered victims.)
Children's Online Privacy Protection Act	1998	Protects children under 13 when interacting on websites that collect personal information from children
Financial Modernization Bill (Title V of the Gramm-Leach-Bliley Act)	1999	Prohibits financial institutions from disclosing consumers' nonpublic personal information (i.e. any personal information provided by a consumer to a financial institution) to nonaffiliated third parties, without consent
Clinton's Executive Order 13145	2000	Bans the use of genetic information in federal hiring and promotion decisions
Confidential Information Protection and Statistical Efficiency Act	2002	Ensures that information supplied by individuals or organizations to a federal agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes
Medical Prescription Drug, Improvement and Modernization Act	2003	Requires prescription drug plan sponsors to comply with the HIPAA Privacy Rule and the Security Rule requirements
Telephone Consumer Protection Act	2003	Established the National Do-Not-Call Registry, which prevents commercial telemarketers from calling an individual if their number is on the registry
Public Health Service Act Federal	2004	Federally assisted alcohol or substance

Confidentiality Requirements for Substance Abuse Patient Records		abuse programs must keep patient alcohol and drug abuse treatment records confidential, absent patient consent or a court order
------------------------------------------------------------------	--	---------------------------------------------------------------------------------------------------------------------------------

Sources:

GAO Report, *Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy, Appendix V: Descriptions of Federal Laws for Protecting Personal Health Information* (GAO-07-238), January 2007.

Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Federal Register 82462, Dec. 28, 2000.

Appendix B: Table of Public Comments

A. Research Authorizations

<i>Comment</i>	<i>Response</i>	<i>Organization</i>
<p>The requirement of an expiration date or event should be eliminated for all research uses and disclosures of PHI, not just for uses and disclosures for the creation or maintenance of a research database or repository. Researchers are concerned that the Privacy Rule would prohibit uses and disclosures after the termination of the research project (Example – reporting the results of the research to the FDA for an FDA investigational new drug application). Also, researchers cited confusion in creating a clear definition of repositories and databases.</p>	<p>The Final Rule eliminated the requirement for an expiration date for all uses and disclosures of PHI for research purposes, not just for the uses and disclosures for the creation or maintenance of a research database or repository. The Department agreed that the line between research repositories and databases, and research data collection is often unclear. However, in the Final Rule, if the authorization does not contain an expiration date, the authorization must specifically state that there is no expiration date for this authorization. As a result, all authorizations include either an expiration date or event, or a statement that the authorization will have no expiration. Patients continue to control how their PHI is used, since patients can revoke their consent at any time.</p>	<p>Tracy Lugo, MD</p>
<p>Covered entities should be able to use and disclose research data already obtained, even after an individual has withdrawn his or her authorization.</p>	<p>This suggestion was not incorporated into the Final Rule. However, under the reliance exception in the Final Rule, covered entities may continue using and disclosing PHI that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the</p>	<p>Unavailable</p>

	research study. Examples of permitted uses and disclosures after a revocation include submitting a marketing application to the FDA, conducting an investigation into scientific misconduct, or reporting adverse events.	
A single set of authorization requirements should apply to all uses and disclosures, including those for research purposes. And, the Privacy Rule should permit an authorization for use and disclosure of PHI to be combined with any other legal permission related to the research study, including consent to participate in the study.	The Final Rule adopted a single set of authorization requirements for all uses and disclosures, including those for research purposes. The Final Rule also permits an authorization for use and disclosure of PHI to be combined with any other legal permission related to the research study, including consent to participate in the study.	John Orley Good Clinical Practices Officer Pharmacia and Upjohn 7000 Portage Road Kalamazoo, MI 49001
Some researchers supported retaining the December 2000 version of the Privacy Rule, which required that a description of the extent to which PHI will be used or disclosed for treatment, payment or health care operations be included in an authorization to use or disclosure of PHI for a research study that includes treatment of individuals. They argue that in order for an individual to make informed decisions they must know how research information will be used and disclosed.	Creating a distinction between research that includes treatment, and research that does not, is overly subjective and does not provide commensurate gains in privacy protections for individuals. But it may sometimes be advisable for authorization forms to include a statement regarding how PHI obtained for a research study will be used and disclosed for treatment, payment and health care operations, if the information would help the individual in making an informed decision about whether to grant authorization for the research study.	Unknown
Researchers should be allowed to continue to use or disclose PHI after a revocation of the initial	The Final Rule permits the continued use and disclosure of PHI to the extent	Unknown

<p>authorization, but only if an IRB or Privacy Board approved the continuation.</p>	<p>necessary to preserve the integrity of the research study. The additional burden of requiring IRB or Privacy Board approval for the continued use or disclosure of PHI is unnecessary.</p>	
<p>Does the “reliance exception” permit covered entities and researchers to continue analyzing data once an individual has revoked his or her authorization?</p>	<p>Yes. The “reliance exception” does permit covered entities and researchers to continue to analyze data once an individual has revoked his or her authorization, if necessary to protect the integrity of the research project. The Privacy Rule balances patient privacy against other public goods, such as research. The continued uses and disclosures of PHI already obtained and which is necessary to protect the integrity of the research project, would pose minimal privacy risk to individuals, and provide a great benefit to research.</p>	<p>Jeanne Scott Director of Government Relations NDC Health Information Services 1706 Great Falls Rd McLean, VA 22101 -5042</p>
<p>The requirement that an authorization form include a “description of each purpose of the requested use or disclosure” should be interpreted as being sufficiently broad to encompass future unspecified research. This would reduce the burden on covered entities and researchers by permitting covered entities to disclose PHI for re-analysis without having to obtain any additional authorization. The burden to the patients would also be reduced because they would not have to provide additional authorization. In addition, this would more closely</p>	<p>The Final Rule does not broaden the interpretation of this phrase, because of the concern that patients would lack necessary information to make an informed decision. Unlike the Common Rule, the Privacy Rule does not require IRB or Privacy Board review of research uses and disclosures made with individual authorization. Therefore, covered entities would be left to decide whether or not the initial authorization was broad enough to cover subsequent</p>	<p>Unknown</p>

<p>align the Privacy Rule with the Common Rule, which permits broad informed consent or secondary studies if the IRB deems the original informed consent to be adequate.</p>	<p>research analyses, not IRB or Privacy Boards. Also, the Privacy Rule allows re-analysis without patient authorization if the covered entity obtains IRB or Privacy Board waiver of such authorization. As a result, the Final Rule retained the requirement that each purpose of the requested use or disclosure described in the authorization form be research study specific.</p>	
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

B. Approval of a Waiver of Authorization

<i>Comment</i>	<i>Response</i>	<i>Organization</i>
<p>The proposed criteria for waiver of authorization are too subjective. (The proposed criteria are: 1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, 2. The research could not practicably be conducted without waiver or alteration, and 3. The research could not practicably be conducted without access to and use of the PHI.)</p>	<p>The Final Rule adopted the proposed criteria. Although the criteria may initially be difficult for IRBs and Privacy Boards to interpret, the Department issued guidance documents to address this concern. Also, IRBs have successfully implemented the Common Rule, which requires subjective determinations, so IRBs are accustomed to making this type of decision.</p>	<p>R. Philip Eaton Interim Vice President for Health Sciences University of New Mexico Health Sciences Center Health Sciences & Services Building, Suite 302 2500 Marble, NE Albuquerque, NM 87131 -5001</p> <p>Association of American Medical Colleges</p>
<p>The criteria requiring IRB or Privacy Boards to determine that “there is an adequate plan to destroy identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for their retention” should be eliminated. This standard could lead to premature destruction of data, making</p>	<p>The Privacy Rule prevents this problem by permitting the retention of identifiers if there is a health or research justification, or such retention is required by law. IRBs and Privacy Boards should consider the need for investigations into defective data analysis or research misconduct when</p>	<p>Unknown</p>

<p>investigations into defective data analysis or research misconduct impossible.</p>	<p>determining whether the waiver requirements have been met. Destroying identifiers at the earliest opportunity helps protect individual privacy. This Rule puts the burden on researchers to show the need to retain patient identifiers.</p>	
<p>Researchers were concerned that the proposed waiver element that requires IRBs or Privacy Boards to determine whether there are “adequate written assurances that the PHI would not be reused or disclosed to any other person...” would have an adverse affect on retrospective studies involving re-analysis of data.</p>	<p>The Privacy Rule permits the use or disclosure of PHI for retrospective research studies involving re-analysis only if such use or disclosure is made either with patient authorization or waiver of authorization.</p>	<p>Unknown</p>
<p>Recruitment for clinical trials by a covered entity using PHI should be a health care function, not a marketing function. Requiring covered entities to get IRB or Privacy Board waiver of authorization for recruitment purposes is too burdensome for the covered entity, and prevents covered health care providers from communicating with their patients about the availability of clinical trials.</p>	<p>Recruitment is neither a health care function nor a marketing function. The Privacy Rule allows a covered entity to disclose PHI to the individual who is the subject of the information, regardless of the purpose of the disclosure. Therefore, covered health care providers and patients may discuss the option of enrolling in a clinical trial without patient authorization or waiver of authorization. However, a covered entity cannot disclose an individual’s PHI to a third party for the purpose of recruitment into a research study without first getting authorization or waiver of authorization.</p>	<p>Unknown</p>
<p>The Rule should permit a covered entity to get authorization allowing the use and disclosure of PHI for recruitment into a clinical trial</p>	<p>This suggestion was rejected, because such a broad authorization would not provide individuals with</p>	<p>Unknown</p>

<p>without specifying the person to whom the information would be disclosed, or the exact information to be disclosed. The Rule should retain the durational requirement for the authorization, and add a “minimum necessary” requirement.</p>	<p>sufficient information to make a choice about whether to grant the authorization.</p>	
<p>Research that is covered by the Common Rule and/or FDA’s human subject protection regulations should not be within the scope of the Privacy Rule.</p>	<p>The Department rejected this suggestion, stating that the Privacy Rule is necessary to strengthen human subject privacy protections in research. Also, the Privacy Rule creates an equal standard for all research – research governed by the Common Rule and/or FDA’s human subject protections regulations, and research not governed by any existing laws.</p>	<p>Walter Francis, VA</p>
<p>The waiver provision should be eliminated. IRBs and Privacy Boards should not have the right to waive a person’s privacy rights. Rather, individuals should authorize all uses and disclosures of PHI.</p>	<p>No. The Privacy Rule is a balancing act between an individual’s privacy interests and the need for identifiable health information for certain public policy and national priority purposes. The Department believes the Privacy Rule strikes the right balance between these two interests. Research is necessary for continued improvements in health care, and researchers must be permitted to access PHI without individual authorization in some circumstances.</p>	<p>Gautam Nayer, DC Lauren Pankratz, CO Walter Pohl, OK Raymond Taylor, FL Nancy Maison</p>
<p>If the rule permits covered entities to release PHI to FDA regulated entities examining the quality, safety or effectiveness of an FDA regulated product, then this permission should also apply to academic institutes and non-profit</p>	<p>No. The provisions of the rule allowing disclosure to FDA-regulated entities are designed for public health purposes. The Privacy Rule does permit covered entities to disclose PHI to academic</p>	<p>John Houston Director; Data Security Officer; Assistant Counsel UPMC Health System Information</p>

organizations. Otherwise, the Rule establishes a double-standard between FDA regulated entities, and registries created by academic/non-profit sponsored entities.	and non-profit sponsored registries if such disclosures are required by law, made pursuant to an IRB or Privacy Board waiver of authorization, made with the individual’s authorization, or consists only of a limited data set.	Services Division 200 Lothrop St. Pittsburgh, PA 15068 -2582
The definition of “research” should be modified to explicitly permit the building and maintenance of research databases and repositories.	This modification is unnecessary. The Office for Human Research Protections has interpreted the Common Rule definition of “research” to include the development of a repository or database for future research purposes. The Department has interpreted the definition of “research” in the Privacy Rule similarly.	Unknown
The “minimum necessary” requirement for uses and disclosures made pursuant to a waiver of authorization should be eliminated. This would reduce covered entities’ concern that they be held responsible for an IRB or Privacy Board’s inappropriate determination. Thus, covered entities would be more likely to rely on the researcher’s IRB or Privacy Board documentation that patient authorization could be waived. This suggestion would also reduce the likelihood of covered entities requiring duplicative review by the covered entities’ own IRB or Privacy Board.	No. The Final Rule retains the minimum necessary requirement for uses and disclosures made pursuant to a waiver of authorization. Covered entities can already rely on documentation from an external IRB or Privacy Board that the proposed research study meets the requirement for “minimum necessary.” The Department would rather have duplicative review by the covered entities’ own IRB or Privacy Board, than eliminate this requirement and allow unnecessary risk to individual privacy.	M. Elizabeth Ross, M.D., Ph.D. Head, Laboratory of Molecular Neurobiology and Development Center for Clinical and Molecular Neurobiology University of Minnesota Medical School

C. De-Identification of PHI

<i>Comment</i>	<i>Response</i>	<i>Organization</i>
The safe-harbor method for de-identifying PHI is so stringent that	No. The comments received demonstrated that there is	Association of American Medical

<p>it requires the removal of many elements that are essential for data analysis in research.</p>	<p>little consensus as to which data elements are needed for research, and were silent on the feasibility of using the alternative statistical method.</p>	<p>Colleges</p> <p>Jeanne Scott Director of Government Relations NDC Health Information Services</p> <p>Holt Anderson Executive Director NC Healthcare Information & Communications Alliance, Inc</p> <p>Jerry Marquette CEO Coffeyville Regional Medical Center</p> <p>Jac Davies Assistant Secretary, Epidemiology, Health Statistics, and La Washington State Department of Health</p>
<p>Researchers were confused by the relationship between de-identified data, and the provision in the Privacy Rule that permits a covered entity to assign a code or other record identification to an individuals PHI so that it may be re-identified by the covered entity.</p>	<p>The Final Rule was amended so that it explicitly states that re-identification codes are not one of the unique identifying codes that prevent the data from being considered de-identified.</p>	<p>Jo McClain Research Program Manager University of Texas Houston Health Science Center Division of Rheumatology</p>
<p>Can data be linked inside the covered entity and a dummy identifier substituted for the actual identifier when the data is disclosed</p>	<p>Yes. The Privacy Rule does not restrict linkage of PHI inside a covered entity. This dummy identifier is</p>	<p>Mariann Yeager Director, Industry Relations Integrated Visions,</p>

to the external researcher, with control of the dummy identifier remaining with the covered entity?	consistent with the re-identification code allowed under the Rule's safe harbor portion. But note, the dummy identifier cannot be derived from any individually identifiable information (Ex. Social security number, birth date, hospital record number.)	Inc.
Researchers should be able to use a keyed-hashed message authentication code (HMAC) as a re-identification code, even though it is derived from patient information, because it is not intended to re-identify the patient and it is not possible to re-identify the patient from the code. This would be useful in research, because it prevents double counting of cases, and allows the observation of long-term outcomes.	No. HMAC does not meet the requirement for a re-identification code, because it is derived from individually identified information.	Unknown

D. Limited Data Sets

<i>Comment</i>	<i>Response</i>	<i>Organization</i>
Geographical units smaller than a State should be includable in limited data sets (ex. County, city, full zip code, census tract, and neighborhood).	The only geographic subdivision that is considered a direct identifier is a street address. County, city, full zip codes, census tract and neighborhood information can remain in the limited data set.	Unknown
Full birth dates are necessary for longitudinal studies to assure the accuracy of data.	Full birth dates can be included. No dates related to the individual are considered direct identifiers. Researchers can have access to dates of admission and discharge, and the birth and death of the individual. Birth dates are critical for many research projects, including longitudinal research. But	Unknown

	birth date should only be disclosed where it is necessary for the study.	
Data use agreements should include a prohibition on further disclosure of the limited data set, except as required by law or with written consent of the covered entity.	Data use agreements establish the permitted uses and disclosures of limited data sets by the recipient. The agreement must also include assurances that the recipient will use appropriate safeguards to prevent the use or disclosure of the limited data set in ways other than as permitted by the Privacy Rule and the data use agreement, or as required by law. Adding other restrictions, would bring only marginal additional protection while potentially impeding the purposes of the limited data set.	Unknown
Many people questioned the enforceability of data use agreements.	If a recipient breaches a data use agreement, HHS cannot take enforcement action directly against that recipient unless the recipient is also a covered entity. But, if the recipient is a covered entity, it is in noncompliance with the Rule if it violates a data use agreement. The disclosing covered entity is not liable for breaches of the data use agreement by the recipient of the limited data set. But, the covered entity must take reasonable steps to cure a breach or end a violation of a data use agreement if it is aware of the problem. If this is unsuccessful, the covered entity must discontinue disclosure of PHI to the recipient, and report the	Unknown

	problem to the Secretary. The recipient must report to the covered entity any improper uses or disclosures of limited data set information that it knows exists.	
When a covered entity discloses PHI in a limited data set to a researcher who has entered into an appropriate data use agreement, does the covered entity also need to have documentation from an IRB or a Privacy Board that individual authorization has been waived for the purposes of the research?	No. However, the covered entity may not disclose any of the direct identifiers listed in the Rule without either the individual's authorization, or waiver of authorization.	Unknown
Does the minimum necessary requirement of the Rule apply to limited data sets?	Yes. Any use, disclosure, or request for a limited data set must also adhere to the minimum necessary requirement of the Rule.	Unknown
Does the covered entity need to include disclosures of PHI in limited data sets in any accounting of disclosures provided to the individual?	No. All direct identifiers are removed from the limited data set and the recipient of the data agrees not to identify or contact the individual. The burden of accounting for these disclosures in these circumstances is unwarranted.	Unknown
The development of computer-based solutions to support the statistical method of de-identification is advancing rapidly, and is better for research than limited data sets. The authorization of limited data sets will undermine incentives to further develop these computer-based solutions. To prevent this, there should be a sunset clause on the use of limited data sets in order to promote the advancement of computer-based solutions.	The Department is not convinced that current technological advances will meet all the needs of researchers, or are easy enough to use that they can have the broad application needed to support key research. There is no need for a sunset provision. The Office for Civil Rights will periodically assess the need for the limited data set provisions.	Unknown
Since HHS clearly defines direct	Data use agreements are	Unknown

identifiers and facially identifiable information, there is no need for a data use agreement.	necessary to ensure protection of the information once it leaves the control of the covered entity,	
-----------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------	--