The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research

Joy L. Pritts, JD*

"The makers of the Constitution conferred the most comprehensive of rights and the right most valued by all civilized men—the right to be let alone."
—Justice Louis Brandeis (1928)[1]

"You already have zero privacy anyway. Get over it."
—Scott McNealy, Chairman and CEO of Sun Microsystems (1999)[2]

Introduction

The privacy of personal information, and of health information in particular, continues to be a vexing issue in the United States. As more and more health information is computerized, individuals express concern about their privacy and that they are losing control over their personal health information. To help allay public concerns, federal rules governing the use and disclosure of health information were promulgated under the Health Insurance Portability and Accountability Act (known as the HIPAA Privacy Rule). While the HIPAA Privacy Rule does not directly regulate researchers, it does restrict the manner in which health care providers may use and disclose health information for health research.

Health researchers have been critical of the HIPAA Privacy Rule since its inception, concerned that it would interfere with valuable research. Various research organizations and others have requested that the Rule be revised to lessen its effect on research. Most recently, an Institute of Medicine (IOM) committee was formed and charged with reviewing the impact of the Privacy Rule on health research. This paper was commissioned by that committee, the IOM Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule. Because there were a number of other studies presented to the Committee on the impact of research, this paper does not focus on researchers. Rather, it is intended to provide background information on the importance of protecting privacy in general and, more specifically, in the context of research, from the perspective of the individual.

To set the stage, Part I of his paper first gives a very general overview of the various concepts of privacy and its value. Part II focuses specifically on the importance of protecting the privacy of health information. It reviews public attitudes toward the privacy of health information and discusses the value that privacy serves in the health care context. Because the HIPAA Privacy Rule and the "Common Rule," the regulations that directly govern most research, evolved in different contexts and, therefore, take different approaches to protecting privacy, Part III of this paper describes the historical development of the legal protections for health information in the United States. Part IV of the paper examines the interaction of HIPAA and the Common Rule,

[1] *Olmstead v. United States*, 217 U.S. 438, 478 (1928).
[2] John Markoff, "Growing Compatibility Issue: Computers and User Privacy," *New York Times* A-1 (March 2, 1999).

how they differ, and the value that HIPAA adds to the protection of health information in the research context. An overview of the evolving privacy issues presented by developing genetic databases and biobanks is presented in Part V. Finally, Part VI presents some suggested approaches to evaluating the trade offs between protecting privacy and affording researchers access to health information.

I. Concepts and Value of Privacy: In General

Privacy is a deeply felt yet elusive concept.[3] At its core, privacy is experienced on a personal level and often means different things to different people. Most see privacy as allowing us the freedom to be whom and what we are as individuals.[4] Yet, defining privacy has proven difficult, leading one legal scholar to opine, "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[5] In spite, or perhaps because, of its complexity, privacy has been the subject of extensive, and often, heated debate by philosophers, sociologists and legal scholars.

Privacy has deep historical roots. References to a private domain, the private or domestic sphere of family, as distinct from the public sphere, have existed since the days of ancient Greece. [6] Indeed, the English words "private" and "privacy" are derived from the Latin *privatus*, meaning "restricted to the use of a particular person; peculiar to oneself, one who holds no public office."[7] Systematic evaluations of the concept of privacy, however, are often said to have begun with the 1890 Samuel Warren and Louis Brandeis article, "The Right of Privacy," in which the authors examined the law's effectiveness in protecting privacy against the invasiveness of new technology and business practices (photography, other mechanical devices and newspaper enterprises). The authors, perhaps presciently, expressed concern that modern innovations had "invaded the sacred precincts of private and domestic life; and . . . threatened to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[8] They equated the right of privacy with "the right to be let alone" from these outside intrusions.[9]

Since then, the scholarly literature prescribing ideal definitions of privacy has been "extensive and inconclusive."[10] While many different models of privacy have been developed, they generally incorporate concepts of:

- Solitude (being alone)
- Seclusion (having limited contact with others)

---

[3] William Lowrance, *Privacy and Health Research: A Report to the U.S. Secretary of Health and Human Services* (May 1997).
[4] Shari Alpert, "Privacy and the Analysis of Stored Tissues," in National Bioethics Advisory Commission, *Research Involving Human Biological Materials: Ethical Issues and Policy Guidance*, vol. II, Rockville, MD (2000).
[5] Robert Post, "Three Concepts of Privacy," 89 *Georgetown Law Journal* 2087 (2001). *See also* Daniel Solove, "A Taxonomy of Privacy," 154 *University of Pennsylvania Law Review* 477 at 516-518 (January 2006) (noting that privacy is "an umbrella term, referring to a wide and disparate group of related things" the breadth of which is "helpful in some contexts yet quite unhelpful in others").
[6] Alan Westin, *Privacy and Freedom* 7, 22, Atheneum, New York (1967) (hereinafter Westin, *Privacy*).
[7] *Oxford English Dictionary,*(March 2008 revision), *available at*: http://dictionary.oed.com/
[8] Samuel Warren and Louis Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 93 (1890).
[9] *Id.*
[10] Anita Allen, "Genetic Privacy: Emerging Concepts and Values," in *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, Mark Rothstein, ed., 31-59, *Yale University Press*, New Haven (1997).

- Anonymity (being in a group or in public, but not having one's name or identity known to others; not being the subject of others' attention)
- Secrecy or reserve (information being withheld or inaccessible to others)[11]

In essence, privacy has to do with having or being in one's own space.

Some describe privacy as a state or sphere where others do not have access to a person, their information, or their identity.[12] Others focus on the ability of an individual to *control* who may have access to or intrude on that sphere. Alan Westin, for example, considered by some to be the "father" of contemporary privacy thought,[13] defines privacy 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."[14] Privacy can also be seen as encompassing an individual's right to control the *quality* of information they share with others.[15]

In the context of personal information, concepts of privacy are closely intertwined with those of confidentiality and security. *Privacy* addresses "the question of what personal information should be collected or stored at all for a given function."[16] In contrast, *confidentiality* addresses the issue of how personal data that has been collected for one approved purpose may be held and used by the organization that collected it, what other secondary or further uses may be made of it, and when the permission of the individual is required for such uses.[17] Unauthorized or inadvertent disclosures of data are breaches of confidentiality.[18] Informational s*ecurity* is the administrative and technological infrastructure that limits unauthorized access to information.[19] When someone hacks into a computer system, there is a breach of security (and also potentially, a breach of confidentiality). In common parlance, the term privacy is often used to encompass all three of these concepts. This paper will use the generic term privacy rather than repeat the phrase "privacy, confidentiality and security" throughout.

---

[11] *See Id.;* Westin, *Privacy supra* note 6; Charles Fried, "Privacy," 77 *Yale Law Journal* 475-93 (1968); Ruth Gavison, "Privacy and the Limits of the Law," 89 *Yale Law Journal* 421-471 (1980);

[12] *See* Gavison, *supra* note 11; Allen *supra* note 10; Adam Moore, "Intangible Property: Privacy, Power and Information Control," 182-183 in Adam Moore ed., *Information Ethics: Privacy, Property, and Power*, Univ. of Washington Press, Seattle (2005).

[13] Michael Yeo, *Biobank Research: The Conflict Between Privacy and Access Made Explicit*, prepared for the Canadian Biotechnology Advisory Council (Feb. 10, 2004), *available at*: http://cbac-cccb.ic.gc.ca/epic/site/cbac-cccb.nsf/en/ah00514e.html

[14] Westin *Privacy supra* note 6 at 7. *See* also Fried, *supra* note 11 at 482 ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."); and Moore, *supra* note 12 at 186 ("[A]n important part of a right to privacy is the right to control persona information; control in the sense of deciding who has access and to what uses the information can be put.") *See* generally, James Waldo, Herbert Lin and Lynette Millett (eds.) *Engaging Privacy and Information Technology in a Digital* Age, National Academies Press 59-61 (2007) (for a detailed discussion of various concepts of privacy).

[15] Fried *supra* note 11 at 482-83.

[16] Alan Westin, *Computers, Health Records, and Citizen Rights,* 5-6, U.S. Govt. Printing Office, Washington, D.C. (1976) available from http://www.eric.ed.gov/

[17] *Id*. Some see the control of use of data as a component of privacy. *See e.g*., Moore, *supra* note 12 at 186.

[18] *See* National Bioethics Advisory Commission, *Ethical and Policy Issues in Research Involving Human Participants*, 1. U.S. Govt. Printing Office, Rockville, MD (2001) ("NBAC 2001"); Lawrence Gostin and James Hodge, Jr., "Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule, 86 *Minnesota Law Review* 1439 (2002).

[19] Westin, *Computers*, *supra* note 16. *See* also Nicolas Terry and Leslie Francis, "Ensuring the Privacy and Confidentiality of Electronic Health Records," *University of Illinois Law Review* 681, 708 (2007).

Why is privacy important?
Some theorists depict privacy as a basic human good or right that's value is intrinsic.[20] They see privacy as being objectively valuable in itself, as an essential component of human flourishing or well-being.[21]

The more common view is that privacy is valuable because it facilitates or promotes other fundamental values including ideals of personhood such as:

- Personal autonomy (the ability to make personal decisions)
- Individuality
- Respect and
- Dignity and worth as human beings.[22]

Privacy allows us to make our own decisions free from coercion, to totally be oneself and potentially engage in behavior that might deviate from social norms. It allows us the time and space for self-evaluation.[23]

Informational privacy is seen as enhancing individual autonomy by allowing individuals control over who may access different parts of their personal information.[24] It also allows people to maintain their dignity, to keep some aspect of their life or behavior to themselves "simply because it would be embarrassing for other people to know about it."[25] Privacy also allows people to protect their assets[26] or to avoid sharing information with others who would use it against them, such as discrimination by employers, educators, or insurers.[27]

The ability to control one's information has value even in the absence of any shameful or embarrassing or other tangibly harmful circumstances. Privacy is also required for developing interpersonal relationships with others. While some emphasize the need for privacy to establish intimate relationships,[28] others take a broader view of privacy as being necessary to maintain a variety of social relationships.[29] By giving us the ability to control who knows what about us and who has access to us, privacy allows us to alter our behavior with different people so that we may maintain and control our various social relationships.[30] For example, people may share different information with their boss than they would with their doctor, as appropriate with their different relationships.

---

[20] *See e.g.,* Terry and Francis, *supra* note 19. Fried *supra* note 11; Moore *supra* note 12.
[21] Moore, *supra* note12.
[22] *See* Alan Westin, "Science, Privacy and Freedom," 66 *Columbia Law Review* 1003 (1966); Post, *supra* note 4, citing Charles Taylor, *Sources of the Self: The Making of Modern Identity* 15 (1989); Edward Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser," 39 *New York Law Review* 34 (1967); Gavison, *supra* note 11 at 347.
[23] Westin, *supra* note 22.
[24] Gostin and Hodge, "Personal Privacy" *supra* note 18.
[25] James Rachels, "Why Privacy is Important," 4 *Philosophy and Public Affairs* 323-333 (Summer, 1975).
[26] Id.
[27] Lawrence Gostin, "Ethical Principles for the Conduct of Human Subject Research: Population-Based Research and Ethics," 19 *Law, Medicine and Health Care* 191-201 (1991).
[28] *See* Allen, "Genetic Privacy," *supra* note 10 and citations therein.
[29] Rachels, *supra* note 25 at 323.
[30] *Id.*

Most discussions on the value of privacy focus on its importance to the individual. Privacy can be seen, however, as also having value to society as a whole.[31] Privacy furthers the existence of a free society.[32] Large databases, potential national identifiers and wide-scale surveillance, can be seen as threatening not only individual rights or interests but also the nature of our society.[33] For example, preserving privacy from wide-spread surveillance can be seen as protecting not only the individual's private sphere, but also society as a whole: privacy contributes to the maintenance of the type of society in which we want to live.[34] In short, "[S]ociety is better off when privacy exists."[35]

As is clear from the above discussion, privacy is a complex, multifaceted concept which undoubtedly will continue to be the subject of heated discourse. Although there is no clear answer to what is privacy and its value, these general philosophical concepts serve as a useful background for discussing privacy as it applies to health information.

II. Importance and Value of Protecting the Privacy of Health Information

If privacy is essentially having or being in a relatively personal space, it is difficult to think of an area more private than an individual's health or medical information. Medical records can include some of the most intimate details about a person's life. They document a patient's physical and mental health, and can include information on social behaviors, personal relationships and financial status.[36] It is hardly surprising that when surveyed, people consistently report that they are concerned about protecting the privacy and confidentiality of such personal information.

In one recent survey, 67% of respondents said they were concerned about the privacy of their medical records, with ethnic and racial minorities showing the greatest concern.[37] When presented the possibility that there would be a nationwide system of electronic medical records, 70% of respondents were concerned that sensitive personal medical-record information might be leaked because of weak data security, 69% expressed concern that there could be more sharing of medical information without the patient's knowledge and 69% were concerned that strong enough data security will not be installed in the new computer system.[38] People have identified being in control of who could get information about them; being able to share confidential matters with someone they trust; and controlling what information is collected about them as three of the facets of privacy that were most important to them.[39] Half of the respondents in a recent survey believed that "[P]atients have lost all control today over how their medical records

[31] *See* Priscilla Regan, *Legislating Privacy: Technology Social Values, and Public Policy,* University of North Carolina Press, Chapel Hill and London (1995).
[32] Gavison, *supra* note 11 at 423.
[33] Regan, *supra* note 31.
[34] *See* Regan, *supra* note 31 at 219; Gavison *supra* note 11at 455
[35] Regan, *supra* note 31 at 221.
[36] Gostin and Hodge, "Personal Privacy" *supra* note 18.
[37] Forrester Research for the California HealthCare Foundation, National Consumer Health Privacy Survey (CHCF 2005 Survey) 2005.
[38] Harris Interactive for the Program on Information Technology, Health Records and Privacy (2005).
[39] Harris Interactive Survey (2003).

are obtained and used by organizations *outside* the direct patient health care such as life insurers, employers, and government health agencies."[40]

These public opinions about the "privacy" of health information reflect in a very real way the practical importance of privacy to members of the public. They desire control over and security and confidentiality of their health information. They want to know who is using their information and why.

A significant portion of Americans are concerned enough about the privacy of their health information that they take matters into their own hands. In response to a recent California HealthCare Foundation survey, one out of eight respondents reported that they had engaged in a behavior intended to protect his or her privacy, including taking such actions as avoiding their regular doctor, asking their doctor not to record their health information or to "fudge" a diagnosis, paying out of pocket so as not to file an insurance claim and even avoiding care altogether.[41]

In very functional terms, adequately protecting the privacy of health information can help remedy these concerns and, hopefully, reduce this behavior. Ensuring privacy can promote more effective communication between physician and patient, which is essential for quality of care, enhanced autonomy, and preventing economic harm, embarrassment and discrimination.[42]

A number of studies suggest that the relative strength of confidentiality protections can play an important role in people's decisions whether to seek or forgo treatment, particularly with respect to mental health and substance abuse.[43] The willingness of a person to make self-disclosures necessary to such mental health and substance abuse treatment may decrease as the perceived negative consequences of a breach of confidentiality increase.[44] Privacy or confidentiality is particularly important to adolescents who seek health care. When adolescents perceive that

---

[40] Harris Interactive, Online Poll, March 26, 2007, available at http://www.harrisinteractive.com/harris_poll/index.asp?PID=743.

[41] CHCF 2005 Survey *supra* note 37.

[42] Lawrence Gostin, "Health Information: Reconciling Personal Privacy with the Public Good of Human Health," 9 *Health Care Analysis* 321, 324 (2001). *See also* National Bioethics Advisory Commission, *Research Involving Human Biological Materials: Ethical Issues and Policy Guidance, Report and Recommendations* vol. 1 (1999) ("NBAC 1999") ("Concerns about health privacy often are closely related to concerns about dignity given the intimate nature of health information and the fact that it can be considered embarrassing and even shameful."); Joy Pritts, "Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule," 2 *Yale Journal of Health Policy and Ethics* 327- 364 (Spring, 2002) (effective communication between physicians and patients is essential for quality care, citations omitted).

[43] John Petrila, "Medical Records Confidentiality: Issues Affecting the Mental Health and Substance Abuse Systems," 11 Drug Benefit Trends 6-10 (1999) *citing* John McGuire et al., "The Adult Client's Conception of Confidentiality in the Therapeutic Relationship," 16 *Professional Psychology: Research and Practice*, 375-384 (1985); J. Jensen et al., "Parents' and Clinicians' Attitudes Toward the Risks and Benefits of Child Psychotherapy: A Study of Informed-Consent Content," 22 *Professional Psychology: Research and Practice*, 161-170, 199; R. Howland , "The Treatment of Persons with Dual Diagnoses in a Rural Community," 66 *Psychiatric Quarterly* 33-49 (1995); D.A. Sujak et al., "The Effects of Drug-Testing Program Characteristics on Applicants' Attitudes Toward Potential Employment," 129 *Journal of Psychology* 401-416 (1995).

[44] Petrila, *supra* note 43 *citing*: D.O. Taube and A Elwork, "Researching the Effects of Confidentiality law on Patients' Self-disclosures," 21 *Professional Psychology: Research and Practice*, 72-75 (1990); Howard Roback and Mary Shelton, "Effects of Confidentiality Limitations on the Psychotherapeutic Process," 4 Journal *of Psychotherapy Practice and Research,* 185-193 (1995).

health services are not confidential, they report that they are less likely to seek care, particularly for reproductive health matters or substance abuse.[45] These studies show that protecting the privacy of health information is essential to ensuring that individuals will obtain quality care.

Protecting privacy is also seen by some as enhancing data quality for research and quality improvement initiatives. When individuals avoid health care or engage in other privacy protective behaviors, such as withholding information or doctor shopping, inaccurate and incomplete data is entered into the health care system. This data, which is subsequently used for research, public health reporting, and outcomes analysis carries with it the same vulnerabilities. Ensuring individuals that the privacy and confidentiality of health information will be protected should reduce these behaviors and result in more complete and accurate data for these research, public health and quality purposes.[46]

Protecting the confidentiality of health information also protects against the perceived and real potential for economic harm resulting from discrimination in health insurance and employment. Polls consistently show that people are most concerned about insurers and employers accessing their health information without their permission.[47] This concern arises from fears about employer and insurer discrimination. Concerns about employer discrimination based on health information, in particular, increased 16% between 1999 and 2005 with 52% of respondents in the later survey expressing concern that their information might be seen by an employer and used to limit job opportunities.[48] Reports of major employers such as Wal-Mart basing their hiring decisions on the health of applicants appear to justify these concerns. [49]

Studies focusing on genetic information show that individuals go to great lengths to keep their genetic information private and out of the hands of their insurers and employers. Even health care providers are affected by these concerns. In a survey of cancer-genetics specialists, more than half indicated that they would pay out of pocket rather than bill their insurance companies for genetic testing, for fear of genetic discrimination.[50] While surveys do not reveal a significant percentage of individuals who have experienced such discrimination, geneticists have reported that approximately 550 individuals were refused employment, fired or denied life insurance based on their genetic constitution.[51] In addition, studies in the United Kingdom suggested that while insurers in that country do not have a full grasp on the meaning of genetic information and do not assess or act in accord with the actuarial risks presented by the information.[52] There is, therefore, some legitimate basis to individuals' concerns about potential economic harm and the need to protect the privacy of their genetic information.

---

[45] Melissa Weddle and Patricia Kokotailo, "Confidentiality and Consent in Adolescent Substance Abuse: An Update," 7 *Virtual Mentor, Ethics Journal of the AMA*, (March 2005) (citations omitted).
[46] Janlori Goldman, "Protecting Privacy to Improve Health Care," 17 *Health Affairs* 47-60 (1998).
[47] *See* Princeton Research Associates, for California HealthCare Foundation, national poll, 1999; CHCF 2005 Survey, *supra* note 37.
[48] *Id.*
[49] Steven Greenhouse and Michael Barbaro, "Wal-Mart Memo Suggests Ways to Cut Employee Benefit Costs," *New York Times*, C-1 (October 26, 2005).
[50] Kathy L. Hudson, "Prohibiting Genetic Discrimination," 356 *New England Journal of Medicine*, 2021 (May 17, 2007).
[51] NBAC 1999 *supra* note 42.
[52] Lawrence Low, et al., "Genetic Discrimination in Life Insurance: Empirical Evidence From a Cross Sectional Survey of Genetic Support Groups in the United Kingdom," 317 *BMJ* 1632-1635 (Dec. 12, 1998).

In addition to these utilitarian reasons for protecting privacy, some privacy scholars emphasize the value of protecting the privacy of health information in its own right, seeing it as a fundamental human right.[53] They believe that respecting privacy (and autonomy) is a form of recognition of the attributes that give humans their moral uniqueness.[54] Thus, there are a variety of reasons, both concrete and perceived, functional and philosophical, for placing a high value on protecting the privacy, confidentiality and security of health information.

III. Historical Development of Legal Protections of Health Information Privacy

The value of the privacy of health information has been recognized by affording it protection under the law. This section of the paper examines the historical development of these protections both in the clinical care context and in the health research context. The rules for protecting the privacy of health information in these two areas developed along fairly distinct paths until the promulgation of the federal privacy regulations under the Health Insurance Portability and Accountability Act.[55] Prior to HIPAA, health information in the clinical setting was protected primarily under a combination of federal and state constitutional law, as well as state common law and statutory protections. By the late 1970s fair information practices for handling information in the computer-based era began to be incorporated into most state health privacy statutes. These practices were also incorporated in HIPAA, which governs the privacy of health information that is maintained by health care providers. In contrast, research practices have been governed almost exclusively by federal regulations (called the Common Rule) which have historically focused on protecting individuals from physical harm in biomedical trials. The Common Rule, therefore, focuses on procedures for obtaining the individual's informed consent. Although an increasing percentage of health research is now records based, the protection of information has not been addressed in any detail in the Common Rule. The HIPAA Privacy Rule attempted to remedy this gap by imposing requirements on the circumstances under which health care providers may disclose health information to researchers.

This section of the paper traces the development of these legal protections for health information. It first discusses the constitutional and common law protections for health information. It then describes the development of the fair information practices and explores their incorporation into state statutes. The paper then gives an overview of the HIPAA Privacy Rule. Lastly, it describes the evolution of the Common Rule.

---

[53] *See e.g.,* Terry and Francis, *supra* note 19. *See* James Waldo, Herbert Lin and Lynette Millett (eds.) *Engaging Privacy and Information Technology in a Digital* Age, National Academies Press (2007) for a detailed discussion on the intellectual approaches to and conceptual underpinnings of privacy.

[54] J. O'Brien and C. Chantler, "Confidentiality and the Duties of Care," 29 *Journal of Medical Ethics* 36-40 (2003).

[55] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191 (1996) (most relevant sections codified at 42 U.S.C. §§ 1320d -1320d-8).

A. Constitutional Privacy Protections

The United States Constitution does not expressly provide a right to privacy. The courts, however, have determined that various constitutional provisions implicitly create zones of privacy that are protected by the Constitution. The privacy interests recognized include both the individual's interest in making certain kinds of important decisions, and the individual's interest in avoiding disclosure of personal matters. With respect to informational privacy, the courts appear to have afforded limited constitutional protections.[56]

In the seminal case, *Whalen v. Roe*, the Supreme Court was asked to decide whether the constitutional right to privacy protected against the mandatory reporting, maintenance and limited disclosure of sensitive health information in a government computer data base. The Court suggested that the constitutional right to privacy extended to the "individual interest in avoiding disclosure of personal matters" and recognized that "in some circumstances" the duty to avoid unwarranted disclosures of personal matters to the government "arguably has its roots in the Constitution."[57] However, because the state had a legitimate need for the information, and had policies and procedures in place to protect the information from further disclosure, the Court determined that the challenged system did not violate the Constitution. In the subsequent case of *Nixon v. Administrator of General Services*, the Supreme Court more directly determined that individuals have "a legitimate expectation of privacy in . . . personal communications."[58]

The majority of federal circuit courts of appeal have interpreted these cases as affording a constitutionally protected right to informational privacy.[59] Several federal courts have expressly recognized the constitutional right of privacy in connection with medical and prescription records.[60] Although the courts generally recognize a constitutional right to informational privacy, the right is not absolute. In determining whether a state intrusion into personal information is warranted, the courts employ a flexible balancing test, weighing such factors as the type of record and information that it contains, the potential for harm in an unauthorized disclosure and the injury from disclosure to the relationship in which the record was generated against the public interest or need for the disclosure and the adequacy of safeguards to prevent unauthorized access or disclosure.[61]

All states have constitutional provisions similar to those in the U.S. Constitution, which give rise to an implied right of privacy.[62] Unlike the U.S. Constitution, however, constitutions in ten states expressly grant individuals an express right to privacy.[63] Courts have consistently determined

---

[56]Lawrence Gostin, "Health Information Privacy," 80 *Cornell Law Review* 451-528 (1995). Terry and Francis, *supra* note 19.

[57] *Whalen v. Rose* 429 U.S. 589, 599 (1977).

[58] *Nixon v. Administrator of General Services* 433 U.S. 425 (1977).

[59] Gostin "Health Information Privacy," *supra* note 56. Three circuits have rejected attempts to infer a specific right to informational privacy, citing the lack of a clear mandate from the Supreme Court. Jessica A. Bodger, Note, *Taking the Sting Out of Reporting Requirements: Reproductive Health Clinics and the Constitutional Right to Informational Privacy*, 56 Duke L. J. 583-609 (2006).

[60] Terry and Francis, *supra* note 19.

[61] Gostin, "Health Information Privacy," *supra* note 56. Bodger, *supra* note 59.

[62] Pritts, "Altered States" *supra* note 42.

[63] National Conference of State Legislators (NCSL), *Privacy Protections in State Constitutions* (2008) available at http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm.

that health or medical information is an area of privacy that is protected by state constitutions.[64] Whether the right of privacy is express or implied, the vast majority of state constitutions protect only against governmental intrusions.[65] In general, this means that an individual cannot challenge the collection or disclosure of health information by a private party (such as a private hospital or an academic researcher) on constitutional grounds. Since much of the exchange of health information is between private parties, this limits the applicability of constitutional challenges. Individuals may raise constitutional issues when the state allegedly intrudes on their privacy. Challenges to state laws requiring the reporting of health conditions or treatments, for example, have been premised on state and federal constitutional grounds.

To the extent that the challenged access to or disclosure of personal information is a state activity, the constitutionality of the state's intrusion on an individual's right to informational privacy is determined, as under the federal constitution, by applying a flexible balancing test, which weighs the state's interest in accessing the information against the individual's privacy interest.[66] Individuals asserting a constitutional right to privacy are unlikely to prevail unless the state fails to assert any significant interest or need for the information or is particularly lax in the manner in which it handles the information once it has been collected.[67] Thus, individuals generally cannot rely on state constitutions to protect them against the unwarranted use and disclosure of health information either by private parties or by the state.

In sum, both federal and state constitutions generally afford citizens only limited protection for the privacy of their health information. With limited exceptions, individuals are only protected against governmental intrusions into their personal health information and may not raise constitutional challenges to private action. Even when state action is involved, individuals rarely prevail on claims premised on constitutional rights to informational privacy because state interests generally outweigh the individual's privacy interest.

B. Common Law Protections

State common law also affords individuals some degree of protection against the disclosure of their health information. Traditionally, the law's regulation of "privacy" consisted, essentially, of the protection of confidentiality within the doctor-patient relationship.[68] The duty of confidence springs from the ethical principles of respect for persons and non-malfeasance. Some believe that "[f]or its part, the common law has tended to treat confidentiality not as an end in itself, but as an instrumental value that secures public health benefits for society generally."[69]

---

[64] *See e.g., Jeffrey H. v. Imai*, 101 Cal. Rptr. 2d 916, 921 (Cal. Ct. App. 2000) (stating that disclosure of a medical condition concerned 'the core value' protected by California Constitution, article I, section 1, informational privacy); *Painting Indus. of Hawaii Market Recovery Fund v. Alm*, 746 P.2d 79, 82 (Haw. 1987) (holding that the state constitutional right to privacy extends only to highly personal and intimate information such as medical, financial, educational, or employment records).

[65] Gostin, "Health Information Privacy," *supra* note 56; NCSL, *supra* note 63.

[66] *See, e.g*., *Stone v. City of Stow*, 593 N.E.2d 294 (Ohio 1992) (finding that individuals' interests in pharmaceutical records under Ohio and federal constitutions were outweighed by the state's interest in reviewing records). *See generally* Gostin, "Health Information Privacy," *supra* note 56 (discussing difficulties in prevailing on claims based on violation of a constitutional right to privacy).

[67] Gostin & Hodge, *supra* note 18.

[68] Roger Magnussen, "The Changing Legal and Conceptual Shape of Health Care Privacy," 32 *The Journal of Law, Medicine and Ethics,* 681 (Winter 2004).

[69] *Id*., at 682.

Courts have found that actions may be maintained against private parties for unauthorized disclosures of health information under a number of legal theories including invasion of privacy, implied breach of contract, breach of confidentiality and breach of fiduciary relationship. Obtaining a remedy for disclosure of health information under any of these theories, however, is difficult.[70]

A number of states recognize the tort of "invasion of privacy" based on the unreasonable public disclosure of private facts.[71] In order to prevail on such a claim, the individual must prove that there was a public disclosure of a private matter that was not of legitimate concern to the public and that the disclosure would be highly offensive to a reasonable person.[72] In the view of a number of commentators, it is quite difficult for an individual to prove invasion of privacy under these standards.[73] Individuals have generally been able to prove that health information is "a private matter." As one court aptly noted, "[i]f there is any right of privacy at all, it should include the right to obtain medical treatment at home or in a hospital for an individual personal condition (at least if it is not contagious or dangerous to others) without personal publicity.[74] However, establishing that there was a "public disclosure" of information has proven to be more difficult. Some courts have found that the tort requires disclosure to the general public or a wide audience, a standard that may not be met when health information is disclosed to only a few.[75] In addition, the individual may have difficulty showing that the publication of a particular medical condition or treatment is "highly offensive." For example, a television station that filmed a private meeting of couples who had conceived using in vitro fertilization defended itself against an invasion of privacy suit by asserting that a reasonable person would not be embarrassed by the fact that they had undergone such treatment.[76]

Legal commentators have noted that the "invasion of privacy" action is a poor fit for many perceived wrong disclosures of health information. Having struggled in their efforts to devise a civil remedy for wrongful disclosures of health information, courts have increasingly turned towards relying on the tort of breach of confidentiality, which is distinct from the "invasion of privacy" tort.[77] Courts in at least twelve jurisdictions have endorsed the breach of confidence tort.[78] A plaintiff can establish a breach of confidence by proving the existence and breach of a duty of confidentiality.[79] Courts have found a duty of confidentiality by looking to the nature of the relationship between the parties, by reference to the law of fiduciaries or by finding an

---

[70] Gostin, "Health Information Privacy," *supra* note 56, at 508-509; Pritts *supra* note 42, at 330-331; Terry and Francis, *supra* note 19.

[71] Most states follow the "invasion of privacy" taxonomy developed by William Prosser and incorporated in the *Restatement of Torts.* Under this framework the "invasion of privacy" tort encompasses four causes of action including: (1) intrusion upon seclusion, (2) appropriation of likeness, (3) public disclosure of private facts, and (4) false-light publicity. *See* Neil M. Richards & Daniel J. Solove*, "*Privacy's Other Path: Recovering the Law of Confidentiality," 96 *Georgetown Law Journal*, 124 (2007). Causes of action based on the alleged wrongful disclosure of health information are usually brought under the cause of action that addresses the public disclosure of private facts. A few states, such as New York and Nebraska, have affirmatively declined to recognize an invasion of privacy tort based on this "public disclosure." Pritts, *supra,* note 42.

[72] Richards and Solove, *supra* note 71.

[73] *Id*.

[74] *Alberts v. Devine*, 479 N.E.2d 113, 119 (Mass. 1985)

[75] Pritts, *supra* note 42.

[76] *Id.*

[77] *Id*.

[78] *Id*.

[79] Richards and Solove, *supra* note 71.

implied contract of confidentiality.[80]

In the health care context, the promise of confidentiality is intended to encourage patients to fully disclose their most personal information to assist in accurate diagnosis and treatment.[81] Courts have thus found the duty of confidentiality applies to physicians, hospitals, psychiatrists, and social workers.[82] The underlying duty of confidentiality is not absolute, and the courts have indicated that there is no breach of confidentiality when a disclosure is made as required by statute (such as mandatory reporting to state officials of infectious or contagious diseases) or common law (such as a duty to disclose information concerning the safety of third persons).[83]

In sum, state common law generally recognizes that some health care relationships are based on maintaining the confidentiality of information obtained in the course of care and affords a remedy when that confidentiality is breached.[84] The extent to which state common law protects the confidentiality of health information in the evolving health care paradigm, where many people and organizations that receive and maintain health information do not have a direct relationship with the patient is unclear. As one scholar has noted, although a physician's duty of confidentiality is well established, "[I]t is at best uncertain whether [such] a duty extends to …other health care professionals, researchers, or health care institutions, although the risk of harm from disclosure is just as significant."[85]

C. Statutory and Regulatory Protections

Since the 1970s, the trend has been to augment existing constitutional and common law rights with statutory protections specifically designed to protect the privacy and confidentiality of health information. Although the common law continues to be important, the federal and state governments have increasingly focused on promulgating distinct standards for the protection of health information.

The shift to statutory and regulatory protections for health information was largely a response to the changing nature of record-keeping in general, and of the nature of the provision of health care. As noted by the 1977 Privacy Protection Study Commission "The emergence of third-party payment plans; the use of health care information for non-healthcare purposes; the growing involvement of government agencies in virtually all aspects of health care; and the exponential increase in the use of computers and automated information systems for health-care record information have combined to put substantial pressure on traditional confidentiality protections."[86] The existing, common law protections over health information were not well suited to protecting a person's interest in knowing when personal information will be collected and for what purpose(s), nor did they afford a remedy for inadequate controls over storage or security of information.[87]

---

[80] *Id.*
[81] Gostin, *supra* note 56.
[82] Richards and Solove, *supra* note 71.
[83] Pritts, *supra* note 42, at 335-6.
[84] Theoretically, an individual could potentially bring suit against a provider who disclosed information to a researcher under one of these common law theories if they believed the disclosure was improper. However, a brief survey of state common law did not reveal any reported decisions involving such actions.
[85] Gostin, *Health Information Privacy, supra* note 56.
[86] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, 283 (1977) (hereinafter "Privacy Commission Report").
[87] Magnussen, *supra* note 68, at 682.

Principles for Fair Information Practice

The framework in which these concerns were addressed, *i.e*., detailed statutory and regulatory protections, originated with the 1973 report of an advisory committee to the U.S. Department of Health, Education and Welfare (HEW) "designed to call attention to issues of record keeping practice in the computer age that may have profound significance for us all."[88] The principles were intended to "provide a basis for establishing procedures that assure the individual a right to participate in a meaningful way in decisions about what goes into records about him and how that information shall be used."[89] In addition to affording individuals the meaningful right to control the collection, use and disclosure of his information, the fair information practices also impose affirmative responsibilities to safeguard information on those who collect it.

The fundamental principles of fair information practice articulated in the report, have since been amplified and adopted in various forms at the international, federal and state level.[90] The fair information practices endorsed by the Organization for Economic Cooperation and Development (OECD), which have been widely-cited, includes the following principles:[91]

- *Collection Limitation*
  There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- *Data Quality*
  Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.
- *Purpose Specification*
  The purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes, and as are specified on each occasion of change of purpose.
- *Use Limitation*
  Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification] except:
  a) with the consent of the data subject; or
  b) by the authority of law.

---

[88] U.S. Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973) (HEW Report) available at: http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

[89] *Id*.

[90] Robert Gelman, *Fair Information Practices: A Basic History* (2008) available at http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[91] OECD, Guidelines *on the Protection of Privacy and Transborder Flows of Personal Data.* Available at: http://www.oecd.org/document/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

- *Security Safeguards*
  Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- *Openness*
  There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- *Individual Participation*
  An individual should have the right to know whether a data controller has data relating to him, to obtain a copy of the data within a reasonable time in a form that is intelligible to him, to obtain a reason if the request for access is denied, to challenge such a denial; to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- *Accountability*
  A data controller should be accountable for complying with measures, which give effect to the principles stated above.

These principles have been adopted at the federal and state levels to varying degrees. The United States has taken a sector-driven approach toward adopting the principles of fair information practices, with the federal and state governments promulgating statutes and regulations that apply only to specific classes of record keepers or categories of records.[92] [93] [94]

At the federal level, the fair information practices were first incorporated into the Privacy Act of 1974, which governs the collection, use and disclosure of personally identifiable data held by the federal government and certain of its contractors. Hospitals operated by the federal government and health care or research institutions operated under federal contract are subject to the Privacy Act, while other health care entities remained outside its scope.[95] Nevertheless, the Privacy Act afforded perhaps the broadest protection for health information at the federal level until the promulgation of the HIPAA Privacy Rule (discussed in detail in subsection D).

For their part, states have adopted (and continue to adopt) laws that not only mirror the Privacy Act in protecting government-held records, but also that afford broader protections for personally identifiable health information held by private parties. In spite of some concerted efforts,[96] these

---

[92] *Id., at 6.*

[93] The original 1973 HEW Advisory Committee contemplated and rejected the creation of a centralized, federal approach to regulating the use of all automated personal data systems. *See* HEW Report, *supra* note 88 at *"Safeguards for Privacy."*).

[94] Europe, in contrast, has adopted fair information practices in a broad, more uniform fashion by incorporating them into the European Union Directive which protects individuals with regard to the processing of any personal data and on the free movement of such data. The EU Directive applies to personal data of many types, including medical and financial, and widely applies to all who process such data, resulting in protections. *See* Gelman *supra* note 90.

[95] Gostin, "Health Information Privacy," *supra* note 56.

[96] The Uniform Health Care Information Act of 1985, drafted by the National Conference of Commissioners on Uniform State Law, incorporated the fair information principles contained in the Privacy Commission Report. *See*

principles have not been adopted uniformly among states. The net result is a patchwork of state health privacy laws that provide little consistency from entity to entity or from state to state.

Restrictions on Use and Disclosure[97]

Virtually every state has some statute or regulation protecting the privacy and confidentiality of health information. Some states have fairly perfunctory provisions that deem records confidential and provide little additional guidance.[98] However, about one-quarter of the states has enacted legislation that provides broad and fairly comprehensive protection for identifiable health information collected, acquired, used, or disclosed within the state.[99] Many of these statutes have the same overarching framework. They generally provide that an individual's identifiable health information is confidential and that it may not be disclosed without the individual's authorization. The statute may dictate the format and content requirements of the authorization. The statute then specifies a number of purposes for which the provider may disclose health information *without* the individual's authorization. There are often additional conditions that must be met prior to disclosing health information for these permitted purposes. Finally, many states statutorily grant the individual a right of action against a party that violates the state confidentiality restrictions.

As a general rule, most comprehensive state health information confidentiality statutes permit health care practitioners to disclose identifiable health information for research without patient authorization. Although not requiring individual authorization, these statutes may impose other restrictions on the use or disclosure of health information for research.[100] For example, the statutes of a number of states, including Maine, expressly impose restrictions on researchers who receive identifiable health information and prohibit them from identifying any individual patient in any report arising from the research or clinical trial. Some states, such as Maine, also require researchers to return any individually identifiable information to the health care practitioner or facility from which it was obtained or to destroy the information when it is no longer required for the research or clinical trial. [101]

At least one comprehensive state health information confidentiality statute expressly prohibits a provider from releasing identifiable health information to a researcher without the individual's authorization. Minnesota requires a provider to attempt to obtain an authorization from the individual prior to releasing identifiable health information for research. Recognizing that individuals often do not respond at all to requests to provide authorization, the statute provides a type of safe harbor and deems the individual to have provided authorization if certain procedural steps are followed. The state also statutorily requires the provider to make a reasonable effort to determine among other things, that:

- The research requires information in identifiable form;

Prefatory Note to the Uniform Health Care Information Act of 1985 *available at:* , http://www.nccusl.org/nccusl/pubndrafts.asp. The Uniform Act was only adopted by two states, Montana and Washington.

[97] This section of the paper was adopted largely from Pritts, "Altered States," *supra* note 42.

[98] Pritts, *supra* note 42.

[99] Pritts, *supra* note 42; Joy Pritts, et. al. *State of Health Privacy*, 2nd ed. (2002) (state summaries) available at: http://hpi.georgetown.edu.

[100] *See generally*, Pritts, *State of Health Privacy*, *supra* note 99.

[101] *See* Me. Rev. Stat. Ann. tit. 22, 1711-C.

- The recipient has established and maintains adequate safeguards to protect the records from unauthorized disclosure, including a procedure for removal or destruction of information that identifies the patient; and
- Further use or release of the records in individually identifiable form to a person other than the patient without the patient's consent is prohibited. [102]

Minnesota's state restrictions on the disclosure of health information for research are considered to be some of the most stringent in the country.

States with less comprehensive frameworks often have statutes or regulations that specifically protect the confidentiality of health information related to specific health conditions or treatments such as mental health, HIV/AIDS, sexually transmitted disease, alcohol and substance abuse, and genetic status due to their association with potential stigma and discrimination.[103] These laws often require the individual's written consent or authorization to disclose such health information, even for treatment or health care operations purposes.[104] They often also require the individual's authorization to release health information for research. For example, the Illinois Mental Health and Developmental Disabilities Confidentiality Act requires the individual's written consent to disclose records related to the provision of mental health services to a researcher.[105]

Thus, the states have enacted the fair information practice restriction on use and disclosure of information in varying ways. Some allow the disclosure of health information for research without the individual's permission and others require such permission. Yet others only require such permission to release only certain types of information for research.

Notice requirements

Under the principles of fair information practices, patients should be given notice, in plain language, of the information practices of those who generate and maintain their health information.[106] The notice should inform patients how information will be used and to whom it will be disclosed. Notices can also serve to bolster trust between health care providers and patients to the extent they remove the element of surprise about the use and disclosure of health information.[107] Although there seems to be little dispute that the principle of providing a notice of information practice is a sound one,[108] only a few states require health care providers to

---

[102] *See* Minn. Stat. § 144.295.

[103] *Id.*

[104] *See e.g.,* D.C. Code §§ 7-1201.02 and 7-1203.01 (permitting disclosures of mental health information for treatment without patient authorization only to providers employed at the same mental health facility and then only to the extent necessary to facilitate the delivery of mental health services and supports to the client); La. Rev. Stat. § 40:1299.6 (making genetic test results confidential unless express written consent to their release is granted by the person tested, and making an exception only for mandatory reporting requirements) (2007); Mass. Gen. Laws ch.111 §70F (prohibiting providers from disclosing the results of an HIV test without the express written consent of the patient).

[105] Richard H. Sanders and Kathryn L. Stevens, "The More Things Change, the More They Stay the Same: An Analysis of the Impact of the HIPAA Privacy Rule on Illinois Mental Health Providers Fall," 4 *DePaul Journal of Health Care Law* 43 (2003).

[106] National Conference of Commissioners on Uniform State Law, Comment on §5-101 of the Uniform Health Care Act, *supra* note 96. *See also* Privacy Commission Report, *supra* note 101 at 313.

[107] *Id.*

[108] Although the eight comprehensive health privacy bills introduced at the federal level in the 106th Congress varied in many aspects, they uniformly included a requirement that covered health care providers and health plans furnish a notice of information practices to patients. *See* Health Information Act, H.R. 1941, 106th Cong. § 204

furnish such notices to their patients.[109]

Security Safeguards

Under accepted principles of fair information practices, those who maintain identifiable health information should have in place appropriate safeguards to protect unauthorized use or disclosure of the information.[110] These safeguards identify the means by which a provider protects the confidentiality of health information. A few states such as California, Florida and Washington have statutorily required providers to undertake security measures to ensure that health information is used and disclosed properly. Florida, for example, requires those who maintain medical records to develop and implement policies, standards, and procedures to protect the confidentiality and security of the medical record, and to train their employees in these policies, standards, and procedures.[111]

Accountability

Fair information principles provide that data holders be held accountable if they fail to adequately protect the confidentiality or security of information under their supervision. State statutes vary widely in both providing remedies for breaches in confidentiality and security, and with respect to the standard imposed for initiating a suit.[112]

Some state health information confidentiality statutes do not explicitly provide remedies for violations of the standards set by the statute.[113] Many state statutes, however, do provide remedies for breaches either by including civil penalties or by expressly creating a private right of action.[114] The standards for imposing civil penalties or prevailing on a private right of action vary widely. In some states, a remedy is only available when the provider has willfully or intentionally released information in violation of the statutory restrictions. In Hawaii, for example, a person can be fined for willfully violating the state's statutory protection of the confidentiality of HIV/AIDS information.[115] In a similar vein, some states, such as Arizona, expressly provide a "good faith" exception to their specified remedies. Under these state statutes, a health care provider that acts in good faith is not liable for damages in any civil action for the disclosure of medical records or information. In Arizona, the presumption is that the provider has acted in good faith unless the individual can establish otherwise. Yet other states provide remedies for negligent disclosures. These statutes often provide for higher penalties if the violation is knowing or intentional. Some states allow individuals to bring lawsuits. Rhode Island, for example, statutorily provides that a person who violates its Confidentiality of Health

---

(1999); Personal Medical Information Protection Act of 1999, H.R. 2404, 106th Cong. § 103(1999); Consumer Health and Research Technology Protection Act, H.R. 2455, 106th Cong. § 203 (1999); Medical Information Protection and Research Enhancement Act of 1999, H.R. 2470, 106th Cong. § 103 (1999); Medical Information Privacy and Security Act, H.R. 1057, 106th Cong. § 103 (1999); Medical Information Privacy and Security Act, S. 573, 106th Cong. § 103 (1999); Health Care Personal Information Nondisclosure Act of 1999, S. 578, 106th Cong. § 103 (1999); Medical Information Protection Act of 1999, S. 881 106th Cong. § 103 (1999).

[109] *See*, e.g., Me. Rev. Stat. Ann., tit. 22, §§ 1711-C; N.J. Stat. 26:2H-12.9 (requiring the Bill of Rights for Hospital Patients to be posted); Wash. Rev. Code § 70.02.120.

[110] Privacy Commission Report, *supra* note 101 at 304-05.

[111] Fla. Stat. Ann. §§ 456.057(9).

[112] Ariz. Rev. Statutes § 12-2296.

[113] *See* S.C. Code Ann. §§ 44-115-10 to 44-15-150.

[114] *See generally* Pritts, *State of Health Privacy*, *supra* note 99.

[115] Haw. Rev. Stat. § 325-102.

Care Communications and Information Act may be liable for actual and punitive damages.[116] If the violation is knowing or intentional, the person may be subject to criminal penalties including fine and imprisonment.[117]

Although a number of states enacted these protections of health information based on fair information practices, most did not do so in a comprehensive fashion. The result was a patchwork of state laws that afforded disparate protection of the privacy of health information both within a state and among the states. As the nation continued its slow process toward the adoption of electronic maintenance and transmission of health information concerns increased that these protections were inadequate.

D. The HIPAA Privacy Rule: An Overview

In 1996 Congress enacted HIPAA and included provisions intended to encourage the use of electronic technology in the health care industry as a means of improving efficiency and reducing costs.[118] Recognizing public concerns arising from an electronic health information system, Congress included in HIPAA requirements for the development of standards to protect the security and privacy of individually identifiable health information. Intending to enact comprehensive privacy legislation, Congress did not include detailed privacy requirements in HIPAA, but rather directed the Secretary of Health and Human Services (HHS) to promulgate privacy regulations if Congress failed to act by August 1999.[119]

Numerous bills which would have addressed health information privacy in a fairly comprehensive fashion were introduced in Congress. In 1999 alone, eight such bills were introduced. Because Congress missed the deadline for enacting legislation, the task of developing privacy standards fell to the Secretary of HHS. As a result, the vast bulk of the standards governing the privacy of identifiable health information are contained in the federal privacy regulations (the Privacy Rule), rather than in the Act.

The Privacy Rule, which establishes minimum standards for protecting the privacy of individually identifiable health information, constitutes the first broad-ranging federal health privacy law. Incorporating many of the basic fair information practices,[120] the Rule generally restricts the use or disclosure of protected health information, except as permitted by the individual or as authorized or required by the Rule. It also imposes on those covered by its provisions affirmative requirements to safeguard the information in their possession. The Rule confers upon individuals certain rights with respect to their health information. Key aspects of the Privacy Rule are summarized below.

---

[116] R.I. Gen. Laws § 5-37.3-4.

[117] *Id*.

[118] *See* Standards for Privacy of Individually Identifiable Health Information: Final Rule (Preamble) 65 Fed. Reg. 82469 (Dec. 28, 2000) (hereinafter, Final Rule Preamble) (summarizing Congressional objectives).

[119] Public L. No. 104-191 § 264.

[120] *See* U.S. Secretary of Health and Human Services, *Recommendations on the Confidentiality of Individually-Identifiable Health Information to the Committees on Labor and Human Resources* (Sept. 11, 1997) (hereinafter "Secretary Recommendations") (stating that recommendations to Congress were based on fair information practices in a health care setting); Standards for Privacy of Individually Identifiable Health Information: Proposed Rule, Preamble, 64 Fed Reg. 59923 (1999) (stating that recommendations served "as a template" for the Privacy Rule) ("Proposed Rule Preamble").

Entities Subject to the Privacy Rule
The Rule applies directly only to a core group of entities (called "covered entities") that use and share information in the health care system including:

- most health care providers,
- health plans, and
- health care clearinghouses.[121]

HHS recognized that covered entities comprise only a limited subset of those who need access to health information to conduct the core functions of health care. The Privacy Rule, therefore, allows covered entities to disclose health information without individual authorization to its ***business associates***, persons or entities that perform certain functions or services on their behalf that require the use or disclosure of personal health information, provided there are adequate safeguards for the protected health information.[122] As a general rule, these safeguards take the form of a business associate agreement whereby the business associate agrees not to use or disclose the protected health information that they receive except as permitted by the agreement or by law.[123]

Information Protected
The standards in the Privacy Rule apply to "protected health information." In general, protected health information is "individually identifiable health information" that is held or maintained by a covered entity.

Individually identifiable health information is information, including demographic information, that relates to past present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care for the individual" that either identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[124]

Health Information That Is Not Protected by the Privacy Rule
The Privacy Rule standards do *not* apply to:

- Individually identifiable health information that is maintained by someone *other* than a covered entity.
- Information which has been de-identified in accordance with the Rule.[125]

Restrictions on Use and Disclosure
Covered entities generally may not use or disclose protected health information except as permitted or required by the Rule.[126] In general, a covered entity may disclose protected health information without the individual's permission for treatment, payment and health care operations purposes. For other uses and disclosures, the Rule generally requires the individual's

---

[121] 45 C.F.R. §§ 160.102, 164.104. *See* 42 U.S.C. § 1320d-1 (2001) (establishing scope of applicability of HIPAA administrative simplification standards).
[122] *See* 45 C.F.R. § 164.502(e).
[123] *Id.*
[124] 42 USC § 1320d.
[125] 45 C.F.R. § 164.502(d)
[126] 45 C.F.R. §164.502(a).

written permission, an authorization which must meet specific content requirements.[127] The Rule then establishes a number of exceptions to this general rule, under which the covered entity may use and disclose health information without the individual's authorization but usually subject to specified conditions. For example, the Privacy Rule permits the disclosure of protected health information without the individual's authorization:

- When disclosure is required by another law;
- To a government authority authorized to receive reports of abuse, neglect or domestic violence;
- For public health purposes;
- For judicial and administrative proceedings; and
- For research

Most of these permitted uses and disclosures are subject to detailed conditions. For example, a covered entity may not disclose protected health information in response to a subpoena unless it is accompanied by an order of a court or the covered entity receives assurances that reasonable efforts have been made by the party seeking the information that the person who is the subject of the protected health information has been given adequate written notice of the request, including sufficient information to permit the individual to raise an objection to the production of the information.[128] (Disclosures for research are discussed in detail in section V, subsection D.)

These use and disclosure restrictions apply to protected health information of both living and deceased individuals.[129]

Individual Rights

The Privacy Rule also confers rights on individuals with respect to their protected health information. Under the Rule, individuals have the right to:

- Receive a notice of privacy practices from a health care provider or a health plan that must, among other things, inform patients of the anticipated uses and disclosures of their health information that may be made without the patient's consent or authorization.[130]
- See and obtain a copy of their own health information.[131]
- Request an amendment of information that is incomplete or inaccurate[132]
- Obtain an accounting of certain disclosures that the covered entity made of their protected health information over the prior six years.[133]

Remedies and Penalties

HIPAA does not create a private right of action to remedy violations of the regulations.[134] Rather, the responsibility for enforcing the Privacy Rule lies primarily with HHS.[135] Covered entities that fail to comply with the Privacy Rule may be subject to civil penalties of not more than $100 for each violation of the HIPAA standards, with a maximum penalty of $25,000 per

---

[127] *Id.*
[128] *See* 45 C.F.R 164.512(e).
[129] 45 C.F.R. § 164.502(f).
[130] 45 C.F.R. § 164.520.
[131] 45 C.F.R. § 164.524.
[132] 45 C.F.R. § 164.526
[133] 45 C.F.R. § 164.528.
[134] *Acara v. Banks*, 470 F.3d 569 (5th Cir. 2006).
[135] *See* 42 U.S.C. §§ 1320d-5, 1320d-6 (2001).

person for all violations of an identical requirement.[136] Covered entities that *knowingly* disclose individually identifiable health information in violation of the standards, are subject to significantly higher civil and criminal penalties, including fines and imprisonment.[137] The maximum penalties, a fine of $250,000, imprisonment of up to 10 years, or both, are reserved for those who knowingly disclose identifiable health information in violation of the Rule with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.[138]

Although the statutory penalties may sound stringent, the statute provides that no fines may be imposed if the violation was due to reasonable cause.[139] Similarly, the Compliance and Enforcement regulations stress cooperative compliance over the imposition of penalties. The regulations specifically provide that the Secretary will, to the extent practicable, seek the cooperation of the covered entity in obtaining compliance. [140] If an investigation indicates a failure to comply, the regulations provide that the Secretary will first attempt to resolve the matter by informal means.[141] Such informal resolutions include demonstrating compliance, a completed corrective action plan or a resolution agreement.[142] It is only if a covered entity does not take action to resolve the non-compliance at this point that HHS may contemplate imposing civil monetary penalties on the covered entity. [143]

Contrary to popular misconception, a covered entity that is itself in compliance with the Privacy Rule will not be held liable for the actions of a business associate that breaches the terms of its business associate agreement. A covered entity that knows of a pattern of activity or practice of a business associate that constitutes a material breach of its contract must take reasonable steps to cure the breach or end the violation.[144] If such efforts are unsuccessful, the covered entity must terminate the contract if feasible.[145] If termination is not feasible, the covered entity must report the problem to the Secretary.[146] So long as a covered entity complies with these procedures, they are not liable for the actions of their business associates and will not be assessed civil monetary penalties.[147]

To date, although HHS has received over 33,000 complaints, it has not yet assessed a single dollar in civil monetary penalties.[148] However, there have been three prosecutions under the Privacy Rule of individuals essentially involved in medical identity theft. In spite of this enforcement record, many covered entities remain hesitant to share health information due to concerns about liability.

---

[136] 42 USC § 1320d-5
[137] 42 USC § 1320d-6(a)
[138] 42 USC § 1320d-6(b)
[139] 42 USC § 1320d-5.
[140] 45 C.F.R. § 160.304.
[141] 45 C.F.R. §160.312(a)(1).
[142] *Id. See also* Office for Civil Rights, HHS, *How OCR Enforces the HIPAA Privacy Rule (*April 13, 2007). Available at: http://www.hhs.gov/ocr/privacy/enforcement/hipaarule.html
[143] *Id.*
[144] 45 C.F.R. § 164.504(e)(1)(ii).
[145] *Id.*
[146] *Id.*
[147] *See* 45 C.F.R. § 160.402(b); U.S. Dept. of Health and Human Services, *Frequently Asked Questions: Is a covered entity liable for, or required to monitor, the actions of its business associates?* Available at: http://www.hhs.gov/hipaafaq/providers/business/236.html
[148] Sarah Barr, "HIPAA Enforcement of Privacy Rule Stresses Voluntary Compliance, HHS Official Says,"13 BNA Privacy and Security Law Report (March 28, 2008).

Interaction with other law

As a general rule, the HIPAA Privacy Rule preempts (overrides) provisions of state laws relating to the privacy of health information that are contrary to the federal Rule.[149] A state law is considered to be contrary to the Privacy Rule if it is impossible to comply with both laws or if the state law is an obstacle to the purpose of the Privacy Rule.[150]

There are a number of exceptions to this general rule including the following:

- **Public Health**. The HIPAA Privacy Rule does not override state laws that provide for the reporting of disease or injury, child abuse, birth or death, public health surveillance, or public health investigation or intervention.[151]
- **More Stringent Privacy Laws**. State health privacy laws that are more stringent than the comparable federal provision remain in effect.[152]

State health privacy laws that are *not* contrary to HIPAA are not preempted. If a state health privacy law is merely different than HIPAA it may remain in effect. Thus, the federal privacy regulations establish a "floor" for protecting the privacy of health information, leaving the states free to impose privacy protections on health information that are similar to or more stringent than the federal privacy regulations.

Individuals remain free to bring state tort actions based on breach of confidentiality since there are no comparable provisions in HIPAA and the right to bring such suits furthers protection of confidentiality, one of the intents of the Privacy Rule.[153] In fact, some believe that because the standards set in the HIPAA Privacy set a national "floor" they will be used as the standard of care, the breach of which will constitute a state tort action.

The HIPAA Privacy Rule as a general rule does not replace or overrule health privacy protections afforded by other federal laws and regulations that are not conflicting. The requirements of the Privacy Rule are in addition to those of other regulations protecting human subjects.

With respect to clinical health information, privacy protections for the last 30 years have incorporated concepts of fair information practices, first at the state and then at the federal level. These health privacy laws often include confidentiality provisions that require a health care provider to obtain an individual's authorization to disclose health information for purposes unrelated to treatment. In general, however, they do not impose such a requirement on disclosing health information for research purposes so long as other conditions protecting the health information are met. These rules also impose notice and security requirements on those who maintain health information. The next subsection of this paper addresses the development of the federal protections of health information in the context of research which evolved along a different path.

---

[149] 42 U.S.C § 1320d-7(a); 45 C.F.R. § 160.203.
[150] 45 C.F.R. § 160.202.
[151] 42 U.S.C. § 1320d-7(b)
[152] Public L. No. 104-191, § 264.
[153] Peter A. Winn, *"Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law,"* 33 Rutgers Law J. 617-678 (Spring 2002). *See Doe v. Jo Ellen Smith Medical Foundation*, 913 So.2d 140, 143 (La. Ct. App. 2005) (where court upheld patient's right to bring a post-HIPAA negligence action based on health care facility's leaving patient records in publicly accessible parking lot).

E. Federal Protections of Health Information in Research: Historical Development

Federal regulations governing research were developed primarily to address abuses in biomedical experiments. "Scientific research has produced substantial social benefits. It has also posed some troubling ethical questions."[154] The most troubling of these ethical questions arose from reported abuses of human subjects in biomedical experiments including such incidents as Nazi experiments on concentration camp prisoners during World War II and the Tuskegee syphilis study, in which researchers withheld treatment from affected African American men long after a cure for the disease was found. These reported abuses of human subjects in biomedical experiments were largely responsible for the development of international codes, federal legislation and federal regulation of human subjects research. Most of these principles and standards for conducting human subjects research were developed primarily to protect against the physical and mental harms that can result from these types of biomedical experiments. As such, they focus on the principle of autonomy. Although the standards apply to research that uses identifiable health information, that is not their primary focus.

Nuremberg Code

The Nuremberg Code, created by the international community after the Nazi War Crimes Trials, is generally seen as the first codification of ethical norms governing experimentation on humans. The Code established a set of ethical standards for physical experiments on humans emphasizing the following principles:

- The need to obtain the informed consent of the research subject.
- The duty to avoid all unnecessary physical and mental suffering and injury; and
- The requirement that, any and all risks associated with the research must be outweighed by associated benefits.[155]

Although it did not carry the force of law, the Nuremberg Code was the first international document which advocated voluntary participation and informed consent, which is partially based on autonomy.

Declaration of Helsinki

The World Medical Association confirmed these research principles in 1964 with the adoption of the "Ethical Principles for Medical Research Involving Human Subjects," also known as the "Declaration of Helsinki." The Declaration of Helsinki noted that all "[m]edical research is subject to ethical standards that promote respect for all human beings and protect their health and rights," and sets forth ethical principles to provide guidance to investigators and participants in human subjects research.

The Declaration made expressly clear that ethical standards on medical research encompass the protection of research on identifiable human material or identifiable data. The Declaration

---

[154] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. *Ethical Principles and Guidelines for the Protection of Human Subjects of Research* (1979) (hereinafter The Belmont Report).

[155] *See generally*, Erin D. Williams, *Federal Protection for Human Research Subjects: An Analysis of the Common Rule and Its Interactions with FDA Regulations and the HIPAA Privacy Rule (A CRS Report for Congress) (* June 2005) (hereinafter "CRS Report").

reiterated the principles of informed consent found in the Nuremburg Code and amplified them by, among other things, requiring that all experimental research be reviewed by an independent body. [156]

The principles are based on the general concept that "It is the duty of the physician in medical research to protect the life, health, privacy, and dignity of the human subject." They direct researchers to respect the right of research subjects to safeguard their integrity. The principles also require that "[e]very precaution [is made]… to respect the privacy of the subject, the confidentiality of the patient's information and to minimize the impact of the study on the subject's physical and mental integrity and on the personality of the subject."[157] Thus, the Helsinki Declaration promotes the concepts of respect, autonomy, privacy and confidentiality.

Belmont Report

In the United States, perhaps the most influential inquiry into the protection of human subject in research was the 1979 "Belmont Report" of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, created largely in response to the ethical breaches of the Tuskegee Syphilis Study.[158] Believing that existing ethical codes were often inadequate to cover complex situations, the Commission provided a broader analytical framework intended to guide the resolution of ethical problems arising from research involving human subjects.[159]

The report first distinguished between practice (interventions designed solely to enhance the well being of a patient) and research (activities intended to test a hypothesis and gain generalizable knowledge) and concluded that when elements of research are present in an activity, that activity should undergo review for the protection of human subjects.[160]

The Commission then identified and defined three overarching principles applicable to research involving human subjects; respect for persons, beneficence and justice.[161] Two of these principles, respect and beneficence, are particularly relevant to privacy. The principle of "respect encompasses the requirement to acknowledge autonomy. In application, this means that respect for persons requires that subjects, to the degree that they are capable be given the opportunity to choose what will or will not happen to them."[162] Informed consent is closely tied to the principle of respect, and includes information about potential benefits and risks, comprehension of those risks and voluntariness to participate.

The principle of "beneficence" consists of the obligations to not harm the subject and to maximize possible benefits and minimize possible harms. The requirement that research be justified on the basis of a favorable risk/benefit assessment is closely tied to the principle of beneficence. In conducting such an assessment, the harms to be assessed include not only

---

[156] *See* World Medical Association, Declaration of Helsinki, Ethical Principles for Medical Research Involving Human Subjects, (Declaration of Helsinki) available at http://ohsr.od.nih.gov/guidelines/helsinki.html.
[157] *See* Declaration of Helsinki.
[158] *See* B. Furrow, et al., *Bioethics: Health Care Law and Ethics*, 5th ed. St. Paul, Min.: Thomson/West, 2004.
[159] Belmont Report, *Ethical Principles and Guidelines for Research Involving Human Subjects*.
[160] Belmont Report.
[161] *Id.*
[162] *Id.*

physical and psychological harms but also social and economic harms. These harms are to be weighed against the anticipated benefit to the subject (if any) and the anticipated benefit to society. In assessing risks, the Commission stated, "We [should] be concerned about the loss of the substantial benefits that might be gained from research."

The Belmont principles have been elaborated upon in many settings, and served as the basis for formal regulation of human subjects research in the United States.[163] The Belmont Commission's recommendations were incorporated into HHS's Policy for Protection of Human Subjects Research, Section A of 45 CFR 46 ("Section A") in 1979.[164] These protections were considered a benchmark policy for federal agencies and seventeen other federal agencies had adopted the standards as their own respective regulations. Since then, these common standards for federally funded human subjects research have become known as "the Common Rule." [165]

F. The Common Rule: An Overview

The Common Rule governs most federally funded research conducted on human beings. Its focus is to assure that the rights of human subjects are protected during the course of a research project. The framework for achieving this goal is based on two foundational requirements; the informed consent of the research subject when there is more than minimal risk and the review of proposed research for potential risks by an Institutional Review Board (IRB). This section describes some of the basic parameters of the Common Rule. Particular provisions which interact with the HIPAA Privacy Rule are described in more detail in section V, sub-part D.

Scope of the Common Rule

In general, the Common Rule applies only to research on human subjects that is funded by the federal government.[166] This seemingly simple rule entails three separate requirements.

First, the activity must be "research." Research is defined as "a systematic investigation, *including research development*, testing and evaluation, designed to develop or contribute to generalizable knowledge."[167]

Second, the activity must involve human subjects. Under the Common Rule, "human subject" means "a living individual about whom an investigator . . .conducting research obtains (1) Data through intervention or interaction with the individual, or (2) Identifiable private information." . . .Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects. [168] Two elements of the definition of human subject are particularly notable. First, the Common Rule does not apply to information about deceased individuals. This means that research involving deceased individuals is not subject to the Common Rule. Second, in order for obtaining information to

[163] In general, states do not directly regulate the activity of most researchers. *See* Scott Burris and Lance Gable et al. "The Role of State Law in Protecting Human Subject of Public Health Research and Practice," 31 *Journal of Law, Medicine and Ethics* 654 (2003).
[164] The Department of Health Education and Welfare (now HHS) had previously issued policy and guidance on the protection of human subjects. CRS Report, *supra* note 155 at 14).
[165] CRS Report *supra* note 155 at 6.
[166] 45 C.F.R. § 46.101.
[167] 45 C.F.R. § 46.102(d).
[168] 45 C.F.R. § 46.102(f).

constitute research involving human subjects, the private information must be "individually identifiable," *i.e*., the identity of the subject is or may be readily ascertained by the investigator or associated with the information.[169] Research which has been determined to not to involve human subjects research is not subject to the restrictions of the Common Rule.

Finally, the research must be federally funded. As a result of this limitation, the Common Rule does not apply to research which is privately funded. It is generally believed that a significant amount of human subjects research is conducted outside of federal regulation.[170] For example, it has been reported that industry, rather than the federal government, provides an estimated seventy percent of the funding for clinical drug trials conducted in the United States.[171] Companies and other organizations may voluntarily choose to apply the Common Rule to their research projects, and many do. However, research projects in which compliance is voluntary are not subject to oversight or disciplinary action by the HHS. [172]

Informed Consent[173]

Meaningful informed consent is a cornerstone of human subjects protections. Informed consent is required when risks are more than minimal in order to allow the individual to decide whether the potential harms are relevant and substantial.[174] To provide informed consent, a potential research subject must both understand what participation in a study entails (in other words, be informed), and agree to participate (consent). The Common Rule requires that a researcher obtain informed consent (usually in writing) from a person before they can be admitted to a study.[175]

The Common Rule's informed consent regulations focus primarily on the elements and documentation of informed consent rather than on the process used to obtain it. As to the process, the regulations require that informed consent be sought only under circumstances that provide the prospective subject sufficient opportunity to consider whether or not to participate. With respect to informed consent, the Common Rule generally requires that information be given in language understandable to the subject.[176] The Common Rule also specifies a number of elements that must be provided when informed consent is sought. In general the consent form must include an explanation of the purposes of the research and the expected duration of the subject's participation and explain the risks and benefits of the research. In certain limited circumstances, the Common Rule allows an informed consent to be for unspecified future research. For example, under the Common Rule an informed consent can be used to obtain a

---

[169] *Id.*
[170] Janlori Goldman and Angela Choy, "Privacy and Confidentiality in Health Research," in National Bioethics Advisory Commission *Ethical and Policy Issues in Research Involving Human Participant,* Aug. 2001; CRS Report *supra* note 155 at 18.
[171] CRS report *supra* note 155 at 18.
[172] *See* CRS Report at 18, Goldman at C-5.
[173] This section on informed consent is largely adapted from CRS Report *supra* note 155 at 1-2.
[174] National Bioethics Advisory Commission, *Research Involving Human Biological Materials: Ethical Issues and Policy Guidance, Report and Recommendations* (1999).
[175] CRS Report *supra* note 155 at 1-2.
[176] 45 C.F.R. § 46.116.

person's permission to study individually identifiable information maintained in a repository for future, unspecified research purposes. [177]

For the most part, the required elements of an informed consent address biomedical research (*e.g.*, the consent must include a disclosure of appropriate alternative procedures or courses of treatment, if any that might be advantageous to the subject). One required element of informed consent, however, is particularly relevant to research involving health information. The Common Rule requires an informed consent to include a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained.[178]

Institutional Review Board

Adopting the principles of the Belmont report, the Common Rule requires that protocols for human subjects research be reviewed by an IRB before research may begin.[179] The IRB must meet certain membership requirements. Although the Common Rule does not specify the procedures an IRB must follow in its review of protocols, it does require the IRB to have written procedures for how it will review protocols.

The Common rule requires that an IRB determine the following factors are satisfied in order to approve proposed research:

- Risks to subjects are minimized;
- Risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects, and the importance of the knowledge that may reasonably be expected to result;
- The selection of subjects is equitable;
- Informed consent will be sought in accordance with the rules and will be documented
- When appropriate, that the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects; and
- When appropriate, that there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data[180]

An IRB may waive the requirement to obtain informed consent or approve an alteration of the consent form in certain circumstances where the research involves minimal risk to the subject. [181]

The Common Rule requirements for informed consent do not preempt any applicable state, federal or local laws which require additional information to be disclosed to a subject in order for informed consent to be legally effective.[182]

---

[177] *See* U.S. Dept. of Health and Human Services, NIH Publication No. 03-5428, Institutional Review Boards and the HIPAA Privacy Rule 15 (August 2003) *available at:* http://privacyruleandresearch.nih.gov/pdf/IRB_Factsheet.pdf.
[178] *See* 45 C.F.R. § 46.116(b).
[179] 45 C.F.R. § 46.103.
[180] 45 C.F.R. § 46.111. There are additional factors if the study includes subjects who are likely to be vulnerable to coercion or undue influence.
[181] *See* 45 C.F.R. § 46.111(d); 46.117(c)
[182] 45 C.F.R. § 46.116(e).

Federal funding can be suspended or withdrawn from an institution when it is found to be in material violation of the Common Rule.[183] There is no authority to impose penalties directly on individual researchers for violations. Neither does the Common Rule expressly provide a research subject with a private right of action. It should be noted, however, that recent cases indicate that courts may be willing to hold an institution liable under common law negligence theories where the approved informed consent form is determined to be less than adequate.[184]

While the Common Rule has recently incorporated some concepts of the protection of health information, the Rule continues to be primarily focused on protecting individual research subjects from physical and mental harm. This approach makes utmost sense in the biomedical research context. However, the focus on informed consent and autonomy does not adequately address the privacy issues in research that solely involves the use of health data where the primary risks are from inadequate security or improper disclosure. In this respect, the Common Rule has failed to incorporate many of the practices endorsed in established codes of fair information practice.

V. The HIPAA Privacy Rule and Research

Since the proposal of the Privacy Rule, researchers have expressed concern about the potential impact of the Rule on research. HHS responded to those concerns in both the final Privacy Rule issued in 2000 and the amended Privacy Rule issued in 2002. Some of these difficulties arise from the attempts of the Privacy Rule to incorporate concepts of the Common Rule (such as consent) while indirectly imposing fair information practices on research activities. This section discusses the basis for addressing research in the Privacy Rule, gives an overview of researcher concerns with these provisions, summarizes patient perspectives on researchers access to and use of their health information for research and then discusses some of the major provisions of the Privacy Rule that are implicated in research, the interaction of these provisions with the Common Rule and the value added by the Privacy Rule's approach.

A. Basis for Addressing Research in the Privacy Rule

Research is certainly not *the* focus of the Privacy Rule. However, research was specifically and intentionally addressed in the Privacy Rule to remedy some reported shortcomings of the protection of the privacy and confidentiality of health information in research.[185] Although HHS would have preferred to directly regulate researchers, the agency was restricted by the statutory scope of HIPAA and, therefore, attempted to protect the health information released to researchers through restrictions imposed on covered entities.

A U.S. General Accounting Office (GAO) report prepared in anticipation of federal health privacy legislation reported that confidentiality protections were not seen as being a major thrust of the Common Rule and IRBs tended to give confidentiality less attention than other research risks because they have the flexibility to decide when to it is appropriate to review

---

[183] *See* 45 C.F.R. § 46.123 (2005).

[184] Randi Zlotnick Shaul, et al, "Legal Liability in Research: Early Lessons from North America," *BMC Medical Ethics*, 6 (2005). *See also Grimes v. Kennedy Krieger Institute*, 782 A. 2d 807 (Md. Ct. App. 2001); *Gelsinger v. University of Pennsylvania*, (Philadelphia County Court of Common Pleas filed September 18, 2000), *available at*: http://www.sskrplaw.com/links/healthcare2.html

[185] *See* Secretary Recommendations *supra* note 120; Proposed Rule Preamble, *supra* note 120 at 59968; and Final Rule Preamble, *supra* note 118 at 82691.

confidentiality protection issues. [186] The report noted that although "[t]he actual number of instances in which patient privacy is breached is not fully known. . .in an NIH sponsored study, IRB chairs reported that complaints about the lack of privacy and confidentiality were among the most common complaints made by research subjects."[187] In addition, the compliance staff of the Office for Protection from Research Risks, HHS (OPRR, now Office of Human Research Protections (OHRP) related that they had investigated several allegations involving human subject protection violations resulting from a breach of confidentiality over the past several years and that the complaints related both to research subject to IRB review and to research outside federal protection.[188]

Several examples of breaches of confidentiality by researchers were also documented in the report. In one investigation, a university inadvertently released the names of multiple study participants testing positive for HIV to parties outside the research project, including a local television station. In another case, notes on a patient suffering from extreme depression and suicidal impulses stemming from a history of childhood sexual abuse were distributed during a research presentation at a national meeting. The notes included the patient's identity, medical history, mental status and diagnosis, as well as extensive intimate details about the patient's experience. In yet another case, surgeons who had performed experimental plastic surgery published a journal article including before and after photographs of the patients without their permission. OPRR reported that it was unable to take any action against some of the researchers involved in these breaches because their projects were not subject to the Common Rule. [189]

Every health privacy bill introduced in Congress subsequent to the release of GAO's report contained provisions that would have directly regulated the disclosure of health information to researchers and/or the use and safeguarding of health information by health researchers.[190] Sponsors of some of the bills indicated that "[The] proposed legislation strengthens the privacy provisions in the 'Common Rule,' and extends those protections to all health research.[191]

When Congress failed to enact a comprehensive health information privacy law, the duty of crafting privacy standards fell to the Secretary of HHS. In promulgating the Privacy Rule, HHS, like Congress attempted to address two concerns that were identified in the GAO Report:

- Significant research was conducted outside the standards of the Common Rule and
- The Common Rule lacked detailed requirements addressing the confidentiality and privacy of health information.

---

[186] *See* U.S. General Accounting Office, *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Is Limited* (hereinafter GAO Privacy Report) (February 1999) at 13.
[187] *Id.* at 16.
[188] *Id*.
[189] *Id*. at 16-17.
[190] *See* Health Information Act, H.R. 1941, 106th Cong. §§ 304 and 504 (1999); Personal Medical Information Protection Act of 1999, H.R. 2404, 106th Cong. §§ 111 and 208 (1999*)* Consumer Health and Research Technology Protection Act, H.R. 2455, 106th Cong. §§ 101, 106 (1999); Medical Information Protection and Research Enhancement Act of 1999, H.R. 2470, 106th Cong. § § 111, 208 (1999); Medical Information Privacy and Security Act, H.R. 1057, 106th Cong. § §111, 210 (1999); Medical Information Privacy and Security Act, S. 573, 106th Cong. §§ 111, 210 (1999); Health Care Personal Information Nondisclosure Act of 1999, S. 578, 106th Cong. §§ 111, 208 (1999); Medical Information Protection Act of 1999, S. 881 106th Cong. §§ 111, 208 (1999).
[191] *See* Congressional Record S. 2507 (March 10, 1999); Medical Information Privacy and Security Act H.R. 1057 and S. 573, §§ 111, 210, *supra* note 190.

HHS indicated that, ideally, it would have preferred to address these issues directly by extending the protections of the Common Rule to non-federally funded research and imposing additional criteria for the waiver of authorization in research.[192] However, HHS recognized that it did not have the authority to do so, and therefore, it addressed these issues indirectly (but within the scope of its limited authority), by imposing disclosure restrictions on covered entities.[193]

B. Overview of Researchers' Concerns with the Privacy Rule's Impact on Research

Although the Privacy Rule does not directly apply to IRBs or most researchers, it does restrict the manner in which covered entities may use and disclose protected health information for "research," defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[194] The Privacy Rule does not override the Common Rule or FDA regulations governing human subjects.[195]

The Privacy Rule contains detailed provisions describing numerous ways in which covered entities can use or disclose protected health information for research purposes.[196] Recognizing the public benefits of research, HHS attempted to balance these benefits against privacy risks for those who participate in research.[197] In general, a covered entity may use or disclose personal health information for research if it:

- Discloses a limited data set and enters into a data use agreement with the recipient;
- Obtains the authorization of the individual;
- Obtains documentation that an IRB or privacy board (a type of review board created by the Privacy Rule) has waived the requirement for authorization;
- The review of the data is preparatory to research *or*
- The research is on decedents' information.

Researchers have expressed concern with respect to all of these mechanisms for using and disclosing health information for research. They have questioned the Privacy's Rule's layering of additional protections on top of the Common Rule's requirements. Some have requested that the Privacy Rule be modified to characterize use or disclosure of personal health information for research as an element of treatment, payment, and health care operations. This would permit use or disclosure of protected health information for research without either obtaining the patient's authorization or seeking a waiver of such authorization from an IRB or privacy board. They have also expressed concern about the difficulty of conducting research on health data that have been de-identified according to the Privacy Rule requirements. It has been asserted by some that the standards for de-identification are too restrictive (essentially stripping off all identifiers), such that the data have minimal value for research. Other alternatives, such as hiring a statistician, were perceived as unduly burdensome. They have also raised concerns about the recruiting of research subjects. In addition, several members of the research community expressed concern

---

[192] *See* Secretary Recommendations *supra* note 120 and Proposed Rule Preamble *supra* note 120 at 59968.
[193] *Id*.
[194] 45 C.F.R. § 164.510.
[195] *See* Final Rule Preamble, *supra* note 118 at 82538.
[196] *See generally* 45 C.F.R. § 164.512(i).
[197] Final Rule Preamble, *supra* note 118 at 82691; Standards for Privacy of Individually Identifiable Health Information: Final Rule (hereinafter Modified Rule).67 Fed. Reg. 53182, 53231 (Aug. 14, 2002).

about the provisions requiring an accounting of disclosures of protected health information for research. Specifically, researchers were concerned that covered entities would refuse to share protected health information for research because of the requirement of accounting for all disclosures.[198] In the course of the IOM Committee's work, several studies have been commissioned to document these difficulties. It is unclear whether these difficulties, even as documented, stem from the actual requirements of the Privacy Rule itself or from the interpretations various institutions have given to the Rule.[199]

C. Overview of the Public Perspective on Research and Privacy

Although there are a number of studies that evaluate the impact of Privacy Rule requirements on researchers, there are no truly comparable studies that evaluate the issue from the patient perspective. Few studies address the public perception of the use of health information in research in more than a cursory fashion.[200] Even fewer address public perceptions with respect to the functions of IRBs or review boards, or the intricacies of the protections afforded by the Privacy Rule vis a vis the Common Rule. In fact, it is probably safe to say that the majority of Americans do not even know that their health information can be used without their permission for research and are not in the least familiar with IRBs and the Common Rule.[201] The result is that while there are a number of studies examining the impact of the Privacy Rule on researchers, there is very limited information about the value of the Privacy Rule in protecting privacy in research from the consumer/patient perspective.

From general surveys, we do know that Americans rate health research as a high national priority. [202] We also know that people are concerned about the privacy and confidentiality of their health information.

We can glean additional information from the handful of more detailed studies that examine patient views of the use of their medical information in research through surveys, structured interviews or focus groups. A number of common themes emerge from these studies:

- Patients were generally very supportive of research provided safeguards are established to protect the privacy and security of their medical information.[203]

---

[198] *See* National Committee on Vital and Health Statistics, Letter to Secretary Thompson (Nov. 21, 2001) (detailing researcher concerns expressed in a series of public hearings) (NCVHS letter); U.S. Dept. of Health and Human Services, Secretary's Advisory Committee on Human Research Protections, Letter to Secretary Thompson (Sept. 1, 2004) plus attachments.

[199] NCVHS has noted that testimony it received regarding researchers' concerns contained assertions at variance with the actual requirements of the Privacy Rule. *See* NCVHS Nov. 21, 2001 letter, *supra* note 198 .

[200] Donald Willison, Lisa Schwartz, et al., "Alternatives to Project-specific Consent for Access to Personal Information for Health Research: What Is the Opinion of the Canadian Public?" 14 *Journal of the American Medical Informatics Association* 706-712 (Nov. /Dec. 2007).

[201] *See* Laura Damschroder et al., "Patients, Privacy and Trust: Patients' Willingness To Allow Researchers To Access Their Medical Records." 64 *Social Science & Medicine* 223-235 (2007) (At baseline, 75% of veterans surveyed did not know their medical records could, under certain circumstances, be used without their permission for research, even thought they had received notices of privacy practice notifying them of this potential use and disclosure).

[202] Mary Wooley and Stacie Propst, "Public Attitudes and Perceptions about Health Related Research, *JAMA* 294 (2005) 1380-1384.

[203]Nancy Kass et al., "The Use of Medical Records in Research: What Do Patients Want?" *Journal of Law, Medicine and Ethics*, 31 429-433 (203); Willison *supra* note 200 ; Damschroder, *supra* note 201; Harris Interactive and Alan Westin, *How the Public Views Privacy and Health Research* (national survey commissioned by the IOM)

- Patients were much more comfortable with the use of anonymized data (*e.g.*, where obvious identifiers have been removed) than fully identifiable data for research.[204]
- Patients were less comfortable with sharing information about "sensitive" conditions such as mental health with researchers.[205]
- In studies where patients were able to provide unstructured comments, they expressed concern about the potential that anonymized data would be re-identified. They were also concerned that insurers or employers or others who could potentially discriminate against subjects could potentially access information maintained by researchers.[206] Some were fearful that researchers would sell information to drug companies or other third parties.[207]

Although supportive of research, the majority of patients in these studies did not endorse the disclosure of their medical records for research without any input from patients. Most patients expressed a desire to be consulted before their information was released for research.[208] Even where study participants assumed that researchers would receive no directly identifying information (e.g., name, address and health insurance number), the majority of respondents still wanted to have some input before their medical records were disclosed.[209] In studies where participants were able to elaborate on their thoughts, some voiced the opinion that being asked first was "just a basic right" or was common courtesy.[210]

These studies also indicate that public support for research and willingness to share health information varies with the purpose or type of research being conducted.[211] Generally, there was less support for research that was primarily for a commercial purpose, or that might be used in a manner that would not help patients.[212] Some participants expressed concern that some researchers were motivated by monetary rewards and that decision-makers would act out of self-interest.[213]

In studies conducted in the United State, there are some indications that certain subpopulations may be more willing to have data used for research without consent or choice than the general public. For example, in a Johns Hopkins survey of patients having or at risk for serious medical conditions, 31% of respondents agreed that medical researchers should be able to obtain medical

---

(2007) ("Harris-Westin 2007 Survey"). *See also* Michael Robling et al., "Public Attitudes Towards the Use of Primary Care Patient Record Data in Medical Research Without Consent: A Qualitative Study, 30 *Journal of Medical Ethics* 104-109 (2004) (security as concern but not linked to willingness to share).

[204] Kass, *supra* note 203. Damschroder *supra* note 201; Robling, *supra* note 203; Richard Whiddett et al., "Patients' Attitudes Towards Sharing Their Health Information," 75 *International Journal of Medical Informatics* 530-541 (2006).

[205] Damschroder *supra* note 201; Robling, *supra* note 203.

[206] Kass, *supra* note 203; Damschroder *supra* note 20; Robling *supra* note 203.

[207] Damschroder *supra* note 201.

[208] Kass *supra* note 203; Damschroder *supra* note 201; Willison *supra* note 200; Robling, *supra* note 203; Whiddett, *supra* note 204; Harris-Westin 2007 Survey, *supra* note 203.

[209] Willison *supra* note 200; Damschroder *supra* note 201 . *See also* Robling *supra* note 203 (where no percentages are given but participants expressed preference for consent and voiced concern that the data would not be sufficiently anonymized).

[210] Damschroder *supra* note 201; Robling *supra* note 203.

[211] Willison *supra* note 200; Damschroder *supra* note 201.

[212] *Id*.

[213] Damschroder *supra* note 201.

records without permission.[214] Similarly, 34% of veterans who participated in a focus group study were willing to allow researchers associated with the Veterans Health Administration to use their medical records without any procedures for patient input, subject to IRB approval.[215] In contrast, only 19% of respondents in a survey of the general public were willing to share their medical records for research without consent.[216]

Participants in focus groups expressed a desire to be informed of how their health information was used for research. This desire was tied to a sense of altruism—they wanted to know that their information was useful and that they may have contributed to helping others by allowing their medical records to be used for research.[217]

Very few studies address patients' perceptions on the IRB process. The Westin-Harris 2007 survey inquired into the public's preferred means for allowing researchers access to personal health information. Participants were given a lengthy statement about medical records research that included a description of the IRBs role in determining whether a project would be approved. Only 19% of the respondents in that survey endorsed using patient records without consent but with IRB supervision.[218]

The Damschroder study, which consisted of intensive focus groups utilizing the deliberative democracy model, examined the view of veterans toward the use of their medical records in research in more detail. The majority of participants in this study (75% at baseline) were not even aware that "under some circumstances, [their] medical records could be used in some research studies without [their] permission." (It appears safe to conclude that, at baseline, neither were they aware of the function of IRBs.) This lack of awareness existed in spite of the fact that a notice of privacy practice, which included a statement that such research could occur, had been mailed to all participants less than 12 months prior to the study. [219]

Once informed that their records could be used without explicit permission, but only with IRB approval, a number of participants voiced concern along the lines that "a whole lot of research is done and we don't know it is going on." In fact, participants' desire to discuss their views of the ability to use medical records for research without patient consent overshadowed their willingness to discuss the appropriateness of specific waiver criteria, which had been the original focus of the study.[220]

In the Damschroder study, after the participants had been given detailed information about IRBs, they were asked whether they supported the current procedure of not asking for patient permission to use medical records for research but requiring IRB review. As part of the written question, they were specifically reminded that the review board would "always be responsible for making sure each study has scientific merit and that the privacy of medical records in

---

[214] Kass, *supra* note 203.
[215] Damschroder, *supra* note 201.
[216] Harris-Westin 2007 Survey, *supra* note 203.
[217] Damschroder *supra* note 201; Robling *supra* note 203.
[218] Harris-Westin 2007 Survey, *supra* note 203.
[219] Damschroder *supra* note 201.
[220] Joy Pritts, Michael Neblo et al., "Veterans' Views on Balancing Privacy and Research in Medicine: A Deliberative Democratic Study, 12 *Michigan State University Journal of Medicine and Law* 17-31 (Winter 2008).

research would be protected." However, these assurances were not enough to override the desire of a majority of the participants (66%) to have a procedure in place for patients to have some choice whether their records could be used in research.[221] It is possible that the larger proportion of those supporting the current IRB approach in this study (34% v. 19% Harris-Westin) is attributable to the participants being more informed of the IRB process through the deliberative democracy approach.

Ideally, there would be empirical evidence demonstrating the privacy value of all the specific Privacy Rule provisions that impact researchers. However, no studies have gone into that precise detail. Absent such studies, the results of these more general studies may help inform whether the public values the privacy protections afforded by the Privacy Rule with respect to research.

D. Privacy Rule Provisions on Research: Interaction with the Common Rule and Value Added

As discussed briefly above, there are a number of provisions of the Privacy Rule that impact researchers' ability to obtain health information from a covered entity. This section describes some of the major provisions of the Privacy Rule at issue, analyzes the Privacy Rule's interaction with the Common Rule and addresses, to the extent possible given the scant research, the applicable Privacy Rule provisions' value in protecting the privacy, confidentiality and security of health information.

Individually Identifiable Information

Privacy Rule Provisions

As noted above, the HIPAA Privacy rule applies to protected health information, generally individually identifiable health information held or maintained by health plans, most health care providers, or health care clearinghouses. Not all health information is subject to the Privacy Rule. Information that has been de-identified in accordance with the Privacy Rule is not protected health information and can be used and disclosed freely.

There are two accepted methods of de-identifying information under the Privacy Rule:

- A safe harbor method in which all 18 specified identifiers are removed, which was intended to provide a simple, definitive method for de-identifying health information; and
- A statistical method under which some of the specified identifiers may be retained when a statistician makes and documents that the risk of re-identification is very small.

In order to fulfill the safe harbor requirements for de-identification the following 18 specified data elements that could potentially identify an individual must be removed from the data. In addition the covered entity must have no *actual knowledge* that the remaining information can be used alone or in combination with other information to identify the individual who is a subject of the information.[222]

[221] Damschroder *supra* note 201 .
[222] 45 C.F.R. § 164.514(b)(2).

1. Names.

2. All geographic subdivisions smaller than a state,
including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

4. Telephone numbers.

5. Facsimile numbers.

6. Electronic mail addresses.

7. Social security numbers.

8. Medical record numbers.

9. Health plan beneficiary numbers.

10. Account numbers

11. Certificate/license numbers

12. Vehicle identifiers and serial numbers, including license plate numbers.

13. Device identifiers and serial numbers.

14. Web universal resource locators (URLs)

15. Internet protocol (IP) address numbers.

16. Biometric identifiers, including fingerprints and voiceprints.

17. Full-face photographic images and any comparable images.

18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

With the safe harbor method, the covered entity may assign a code to de-identified information so that it may re-identify it. The code may not be derived from information that is related to the individual (e.g., Social Security number). Furthermore, the covered entity may not disclose the key to the code to anyone else.[223]

As an alternative to the safe harbor method, a covered entity may use a statistical method to establish that information is de-identified. Under this method, a qualified statistician must have determined that there is a "very small" risk that the information in the data could be used by the recipient alone, or in combination with other reasonably available information to re-identify the subject of the information.[224]

Information that has been de-identified by either of these methods is not considered protected health information under the Privacy Rule. Accordingly, a covered entity freely may use and disclose de-identified for research without having to consider the requirements of the Privacy Rule.

Individually Identifiable Information: Common Rule and Privacy Rule Interaction
Although there are a number of similarities between the standards for individually identifiable data under the Common Rule and the Privacy Rule, there are some important distinctions. Both

[223] *Id*.
[224] 45 C.F.R. § 164.514(b)(1).

are designed to protect the anonymity of individuals and to protect against their being identified in data *not* protected by study protocol.[225] Both require a determination that it is not easy to associate the subject/individual with the information.

The primary distinction between the two sets of regulation is in the standard used to determine when information is no longer individually identifiable. The Common Rule does not apply to research if the identity of the subject is [not] or may [not] be readily ascertained by the investigator or associated with the information accessed by the researcher.[226] Otherwise identifiable data may be de-identified for purposes of the Common Rule if it is coded and certain other conditions are met. [227] Information is "coded" if:

- Identifying information (such as name or Social Security number) that would enable the investigator to readily ascertain the identity of the individual to whom the private information or specimens pertain has been replaced with a number, letter, symbol, or combination thereof (the code); and
- A key to decipher the code exists, enabling linkage of the identifying information to the private information or specimen.[228]

Under Guidance issued by OHRP, research involving only coded private information or specimens is not considered to involve human subjects under the Common Rule if the following conditions are met:

- The private information or specimens were not collected specifically for the currently proposed research project through an interaction or intervention with living individuals; and
- The investigator(s) cannot readily ascertain the identify of the individual(s) to whom the coded private information or specimens pertain because, for example:
    - The key to decipher the code is destroyed before the research begins;
    - The investigators and the holder of the key enter into an agreement prohibiting the release of the key to the investigators under any circumstances, until the individuals are deceased ;
    - There are IRB-approved written policies and operating procedures for a repository or data management center that prohibit the release of the key to the investigators under any circumstances, until the individuals are deceased; or
    - There are other legal requirements prohibiting the release of the key to the investigators, until the individuals are deceased.[229]

Under this standard, when a researcher accesses or receives data that has been coded and does not have access to the identifying key, the research is not considered human subjects research

[225] *See* Steven Clause, et al. "Conforming to HIPAA Regulations and Compilation of Research Data," 61 *American Journal of Health System Pharmacy* 1025-1031 (2004).
[226] 45 C.F.R. § 46.102(f).
[227] *Id*.
[228] Office for Human Research Protections, Department of Health and Human Services, *Guidance on Research Involving Coded Private Information or Biological Specimens* (Aug. 10, 2004).
[229] *Id*.

and is not subject to the Common Rule's requirements of informed consent or IRB review and approval of protocol.

In addition, the Common Rule exempts from its requirements research that involves:

> [T]he collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects.[230]

This exemption applies to identifiable information that the researcher *records* in a manner that makes it anonymous.[231]

Prior to the Privacy Rule most records research involving "anonymized date," *i.e*., data where the obvious identifiers of name, address and Social Security number, were not subject to IRB review under these Common Rule provisions.[232] Put another way, information which has had obvious identifiers removed is not considered identifiable information under the Common Rule.

The requirements for de-identification under the Privacy Rule are more stringent than the standards that are applied under the Common Rule.[233] Data which has been anonymized sufficiently for the Common Rule by the removal of name, address and Social Security number, would not be considered to be de-identified under the Privacy Rule. Rather, under the Privacy Rule either all 18 data elements must be removed or a qualified statistician must make the determination that there is only a small risk of re-identification. In practice, this can mean that a covered entity may no longer routinely disclose anonymized data for research.

Individually Identifiable Information: Value of the Privacy Rule

To the extent the Privacy Rule imposes more stringent standards, they are more protective of the anonymity of the individual. They help ensure that data is not released in a manner that can be associated with a particular individual and used against them. The Privacy Rule restrictions also ensure that data is not re-identified using publicly available databases. In contrast, the Common Rule appears to only prohibit a researcher from obtaining a key code. It does not appear to address the ability to re-associate data using publicly available data bases.

Some of the intended recipients of research data may have both the *motive* and *opportunity* for re-identifying the data.[234] Research is not conducted solely by academic research centers. It is also conducted by insurers and others who have the motive to use data to reduce costs. As Wolf et al. explain, "Data are a commodity. . . . Employers and insurance companies can save millions

---

[230] 45 C.F.R. §46.101(b)(4).

[231] *See* OHRP Guidance *supra* note 228.

[232] Rachel Nosowsky and Thomas Giordano, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule: Implications for Clinical Research, 57 *Annual Review of Medicine* 575-590 (2006); Jules Berman, "Confidentiality Issues for Data Miners," 26 *Artificial Intelligence in Medicine* 25-36 (2002); Goldman and Choy *supra* note 170 at C-13.

[233] U.S. Department of Health and Human Services, *Research Repositories, Databases, and the HIPAA Privacy Rule*, NIH Pub. No. 04-5489 (2004).

[234] Virginia de Wolf et al., "Part II: HIPAA and Disclosure Risk Issues," 28 *IRB: Ethics and Human Research* 6-11 (2006).

of dollars by knowing the health or genetic status of prospective employees or insurees. Re-identified data could show HIV+ status, cancer diagnoses, bankruptcy, criminal behavior or mental illness." [235] Employers already routinely search MySpace and Facebook, under somewhat questionable circumstances, to obtain information on prospective employees' lifestyles,[236] while insurers are beginning to explore these online resources as a source of information for denying health benefits.[237]

The opportunity for re-identifying data is also apparent. Record linkage technology has advanced rapidly in the last 10 years. Large public list searches are readily available for integration with "de-identified' data. The re-identification of data can be accomplished quickly and inexpensively.[238] Professor Latanya Sweeney has often shown how easy it is to use publicly available information to identify people. Using the birth date and full postal code, for example, she was able to identify the names and addresses of 97% of the registered voters in Cambridge, Massachusetts.[239] In a less academic setting, New York Times reporters were able to identify "anonymous" AOL clients whose search habits had been posted on the web for research projects by linking their search history to other available data.[240] It is notable that in one of the few studies of data de-identified under the safe harbor provisions of the Privacy Rule, the researchers found that even after they had removed the 18 listed identifiers anticipated recipients or the research database, such as pharmacies, employers and insurers, could re-identify their members in the study data set with a moderately high expectation of accuracy by applying only diagnosis and medication combinations.[241] (The researchers collapsed this data into functional groups to avoid re-identification.) In short, even the Privacy Rule's de-identification standard may not be stringent enough to protect the anonymity of data in today's technological environment.

The studies of public perception of the use and disclosure of health information for research indicate that individuals prefer the use of anonymized data to identifiable data, but are well aware of and concerned about the potential to re-identify such data using modern technology.[242] These studies would seem to indicate that people may prefer the higher standard of de-identification under the HIPAA Privacy Rule.

The high standards of de-identification in the HIPAA Privacy Rule serve a purpose: they help protect patients and study participants from being identified in data not protected by study protocol.[243] This is particularly true with respect to researchers who are *not* subject to the Common Rule. Given the motives and opportunities available, the value of these protections should not be underestimated.

---

[235] *Id.* at 8.
[236] Alan Finder, "For Some, Online Persona Undermines a Resume," *New York Times* 1 (June 11, 2006).
[237] Mary Pat Gallagher, "MySpace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders," New Jersey Law Journal (Feb. 1, 2008).
[238] de Wolf et al. *supra* note 234
[239] *See* Latanya Sweeney, "Weaving Technology and Policy together to Maintain Confidentiality, 25 *Journal of Law, Medicine and Ethics* 98-110 (1997).
[240] Michael Barbarq and Tom Zeller, Jr., "A Face Is Exposed for AOL Searcher No. 4417749," *New York Times* A-1 (Aug. 9, 2006).
[241] Clause *supra* note 225.
[242] Damschroder, *supra* note 201; Robling, *supra* note 203.
[243] Clause, *supra* note 225 at 1029.

Individually Identifiable Information--Limited Data Sets

The Privacy Rule Provisions

Many researchers raised concerns that the data de-identified as required by the HIPAA Privacy Rule was not useful, and that they would be required to use other more burdensome methods of obtaining information for research (such as obtaining the individual's authorization or a waiver of authorization from and IRB described below).[244] They expressed concern that they would be unable to do longitudinal studies.[245]

Some stakeholders urged HHS "to permit covered entities to disclose protected health information for research if the protected information is facially de-identified, that is, stripped of direct identifiers, so long as the research entity provides assurances that it will not use or disclose the information for purposes other than research and will not identify or contact the individuals who are subjects of the information."[246] Others were more specific and requested that the Rule be amended to allow the use of keyed-hash message authentication code (MHAC) asserting that this mechanism would be valuable for researchers because it allows the recipient to link clinical information about the individual from multiple entities over time.[247]

In direct response to these requests, [248] HHS modified the Privacy Rule and created a category of partially de-identified data called the "limited data set," which may be used and disclosed for research (and public health and health care operations) without obtaining individual authorization or IRB approval.[249]

In order to qualify as a limited data set, 16 of the more direct identifiers such as names, addresses, social security numbers, and medical telephone numbers must be removed from the data. However, the following elements may be included in a limited data set:

- City, state, zip code
- Any dates related to the individual (such as date of birth and dates of admission and discharge)
- Other numbers, codes or characteristics (including MHAC)[250]

Essentially, the limited data set provisions permit data to be used and disclosed that is coded in such a manner that the recipient of the data can link one person's data longitudinally over multiple settings.[251]

---

[244] U.S. Department of Health and Human Services, Preamble to Proposed Rule, Standards for Privacy of Individually Identifiable Health Information, Federal Register, 67 (March 27, 2002) 14793-14797 (Proposed Modified Rule Preamble) and Modified Rule, Preamble, *supra* note 197 at 53232-53238. Jennifer Kulynych, and David Korn, "The Effect of the New Federal Medical-Privacy Rule on Research." 346 *New England Journal of Medicine* 201-204 (Jan. 2002).

[245] Subsequent research has indicated that information de-identified using the safe harbor method of removing all of the listed identifiers results in lost chronological spacing of episodes of care. Clause *supra* note 225.

[246] Modified Rule Preamble, *supra* note 197 at 53234.

[247] *Id*. at 53233.

[248] *Id*.

[249] 45 C.F.R. § 164.514(e)(3)(i).

[250] Modified Rule Preamble *supra* note 197 at 53233.

[251] *Id*.

A limited data set may be created by a covered entity. Alternatively, the covered entity can enter into a business associate agreement (a contract) with another party, including the intended recipient, to create the limited data set on its behalf.[252]

Recognizing that the retention of some of the identifiers (particularly geographical and date elements) in a limited data set "measurably increases the risk of identification of the individual through matching of data with other public (or private) data sets" over fully de-identified data,[253] HHS included in the Privacy Rule a requirement that the use or disclosure of a limited data be coupled with a data use agreement. To disclose a limited data set for research without individual authorization, the covered entity must enter into a data use agreement with the recipient. A data use agreement:

- Specifies permitted uses and disclosures of the limited data set, which must be in compliance with the Rule (e.g., may only be for research, public health or health care operations)
- Identifies who is permitted to use or receive the limited data set.
- Requires the recipient:
    - To use or disclose the information only as permitted by the agreement
    - Use appropriate safeguards
    - Not identify the information or contact the individuals.[254]

Because the data in a limited data set may not be used to gain knowledge of an individual,[255] HHS exempted disclosures of limited data sets from the accounting of disclosures requirement.[256]

Limited Data Sets: Common Rule and Privacy Rule Interaction

Limited data sets include additional elements that make data more aligned with "anonymized' data under the Common Rule. Unlike the Common Rule, however, the Privacy Rule requires a covered entity that releases a limited data set to a researcher to obtain a data use agreement in which the researcher promises not to re-identify the data or to contact the subjects of the information.

Although some researchers have indicated that the use of limited data sets may be "enticing,"[257] there do not appear to be any studies about the utilization of limited data sets in the United States.[258] It has been reported, however, that France uses the equivalent of limited data sets from numerous hospitals to conduct epidemiologic research.[259]

---

[252] 45 C.F.R. § 164.514(e)(3)(ii).
[253] Modified Rule Preamble, *supra* note 197 at 53236.
[254] 45 C.F.R. § 164.514(e)(3)(ii).
[255] Modified Rule Preamble *supra* note 197 at 53237.
[256] 45 C.F.R. § 164.528(a)(1)(viii).
[257] Pace, Wilson, et al. "Practice-Based Research Network Studies in the Age of HIPAA," 3 *Annals of Family Medicine* (Supp. 1) S38-45 (2005).
[258] The Clause study, *supra* note 225 examined the loss of data when it was converted from a limited data set into a data set that was fully de-identified by removing all 18 identifiers in accordance with the Privacy Rule's safe harbor method.
[259] Berman, *supra* note 232 at 31.

Limited Data Sets: Value of Privacy Rule

Limited data sets in conjunction with data use agreements promote the use of information that is at least "anonymized" while providing some assurance that the individual will suffer no harm through re-identification of their data. Using anonymized data is one acknowledged technique that protects against the casual identification of individuals by those who use the data.[260] The data use agreement helps ensure an individual's anonymity by specifying that the researcher may not re-identify the information. This requirement of the Privacy Rule is broader than the requirement under the Common Rule, which seem to only require that the code key will not be released to the researcher. The data use agreement also encourages security by requiring the recipient to use appropriate safeguards. Data use agreements essentially establish a basic protocol for protecting the privacy and confidentiality of health information in research that is otherwise not overseen by an IRB. Finally, data use agreements afford a method of redress (e.g., breach of contract) to a covered entity if a recipient improperly re-identifies information in the database.

General Waiver or Alteration of the Authorization Requirement

Waiver Procedure in General

In crafting the Privacy Rule, HHS used a balancing approach in deciding that under certain circumstances, authorizations were not necessary for use and disclosure of protected health information for research. HHS realized that it was not always possible to obtain consent for using or disclosing protected health information for research, particularly in health services research where thousands of records may be involved. It also recognized the potential for selection bias. In light of these factors, HHS concluded that there were circumstances under which it may be appropriate to disclose protected health information for research without authorization. HHS noted, however, "[T]he privilege of using individually identifiable health information for research purposes without individual authorization requires that the information be used and disclosed under strict conditions that safeguard individuals' confidentiality."[261] The Privacy Rule therefore permits a covered entity to disclose protected health information for research where it receives documentation that an independent review board has determined that it is appropriate to waive the requirement for authorization using criteria designed to ensure that health information is adequately protected.

Waiver of Authorization: Common Rule and Privacy Rule Interaction

Both the Common Rule and the Privacy Rule have procedures under which a reviewing body (generally an IRB) can waive the requirement that an individual's authorization (or consent) be obtained prior to using health information for research where there is minimal risk to the individual. (The specific waiver requirements are addressed in the next section).

Value of Waiver of Authorization in Protecting Privacy

The requirement that in most cases the use or disclosure of protected health information for research without authorization would be reviewed by an IRB or a Privacy Board adds a layer of protection for individuals. It ensures that an independent body is determining whether it is appropriate to disclose the identifiable health information at issue. While this was already true to a certain extent in federally-funded research, the Privacy Rule extends this requirement to ensure

[260] O'Brien, *supra* note 54.
[261] Proposed Rule Preamble, *supra* note 120 at 59967.

that non-federally funded research is subject to similar safeguards.[262]

It should be noted, however, that the majority of the public does not support the procedure which allows a review board to waive the requirement that individual authorization be obtained to use or disclose health information for research. Numerous individuals who submitted comments to the proposed Privacy Rule voiced the belief that the waiver procedure abridges the individuals' "autonomy right to decide whether or not to participate in research."[263] Although there has been little research that specifically addresses individuals' attitudes toward IRBs' approving the use and disclosure of identifiable health information for research without the individual's authorization, the few studies that have been done indicate that a significant percentage of individuals are reluctant to allow IRBs to make this decision. Both the Damschroder and the Harris-Westin study indicate that the majority of people do not support the waiver procedure, but would prefer that individuals have some choice in whether their health information can be used and disclosed for research. In the Damschroder study, approximately 65% wanted some manner of choice,[264] while 46% of the respondents wanted some sort of consent process in the Westin-Harris survey (with an additional 13% stating they did not want researchers to use their data under any circumstances). [265] These results indicate that the majority of the public wants some voice in whether their health information is used and disclosed for research purposes.

Waiver or Alteration of Authorization Criteria

Privacy Rule Provisions

Under the Privacy Rule, a covered entity may use or disclose protected health information for research when it receives documentation that an IRB or a privacy board has approved a waiver of the authorization requirement based on specific waiver criteria.[266] The covered entity may also use or disclose such information for research under an altered authorization form, where approved by an IRB or privacy board reviewing the same criteria.[267] Because the Common Rule contains criteria for determining when it is appropriate to waive or alter informed consent for human subjects research, HHS considered excluding from these Privacy Rule provisions research covered by the Common Rule. It rejected this approach however, noting that the Common Rule's waiver criteria were not specifically designed to protect individuals' privacy interests. HHS believed that it was essential to adopt additional waiver criteria to ensure that individuals' privacy rights and welfare are adequately safeguarded when protected health information is used for research without authorization.[268] The result is that while the waiver criteria of the Privacy Rule somewhat mirror those of the Common Rule, they also differ from those established standards.

Under the Privacy Rule, documentation relied upon by a covered entity to use or disclose protected health information under a waiver of authorization or an altered authorization must demonstrate that the IRB or privacy board determined that the waiver satisfies the following criteria:

---

[262] *Id*. at 59969. *See* also 45 C.F.R. § 164.512(i)(1)(i) (specifying the criteria for privacy board membership).
[263] Final Rule Preamble, *supra* note 118 at 82694.
[264] Damschroder, *supra* note 201.
[265] *Id.* Harris-Westin 2007 Survey, *supra* note 203.
[266] *See* 45 C.F.R. § 164.512(i)
[267] *Id*.
[268] *See* Proposed Rule Preamble, *supra* note 120 at 59970-59971.

- The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;
    - An adequate plan to protect the identifiers from improper use and disclosure;
    - An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    - Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.
- The research could not practicably be conducted without the waiver of authorization.
- The research could not practicably be conducted without access to and the use of the protected health information.[269]

Waiver Criteria: Common Rule and Privacy Rule Interaction

A comparison of the waiver criteria of the Privacy Rule and the Common Rule is shown in Attachment 1. The Privacy Rule essentially requires IRBs to consider criteria specifically related to protecting the security and confidentiality of the data both in the near term, during the research, and in the future. It also requires written assurances that the information will not be reused or re-disclosed improperly.

Value of Privacy Rule Waiver Criteria

As part of its balanced decision not to require authorizations for all disclosures of protected health information, HHS imposed additional safeguards to protect the confidentiality and security of the information without the individual's permission.[270] Although the Common Rule contains a general requirement that there be minimal risk to the subject, the Privacy Rule lists certain factors that must be considered in respect to health information in determining whether there is only a minimal risk to the privacy of the individual. The first criterion attempts to ensure that the researcher has thought about how it is going to handle the information. The second criterion appears designed to evaluate whether the research reasonably could be carried out using authorizations. The third criterion appears designed to encourage the use of de-identified information where possible. These criteria are in addition to those of the Common Rule and add detail to its very general requirement.

Security Plan

The requirement that researchers have a security plan is derived from fair information practices. Under these established practices, data holders are required to have reasonable security

[269] 45 C.F.R. § 164.512(i)(2).
[270] Proposed Rule Preamble, *supra* note 120 at 59967.

safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.[271]

The limited research done in this area strongly suggests that patients support the inclusion of an adequate security plan as a criterion for granting a waiver of authorization. In the Damschroder study, participants expressed the belief that having a plan in place would encourage the researcher to take additional precautions with the data.[272]

The need to evaluate the adequacy of researchers' plans to protect data is evidenced by the number of breaches researchers have experienced in recent years, which have exposed millions of personal records. Most recently, a laptop computer containing unencrypted medical information on 2,500 patients enrolled in a National Institutes of Health study was stolen. The data, which included patient names, dates of birth and diagnoses were unencrypted.[273] In 2006, an external hacker breached a server that was being managed by a Georgetown University researcher who was working with the District of Columbia's Office of Aging, compromising the data of 41,000 people.[274] A computer housing research information at the University of Iowa's Department of Psychology and Psychiatry was hacked in 2006.[275] In one of the larger security breaches a University of California research system that housed sensitive personal data on 1.4 million Californians was breached in 2004.[276] These are just some examples of the numerous breaches of security of information maintained by researchers that have been reported in recent years. It is apparent from these reported breaches that the security of information maintained by researchers cannot be assumed.

The extent to which these data breaches have resulted in harm is difficult, if not impossible, to quantify. This type of breach makes people more vulnerable and exposes them to potential future harm, including identity theft. [277] The extent to which breaches by researchers have resulted in actual identity theft is not known. The GAO recently conducted a study of major security breaches involving personal identifying information *exclusive* of those involving medical records. [278] In its study, the GAO concluded that most of the breaches it reviewed had not resulted in detected incidents of identity theft.[279] The GAO repeatedly emphasized however, that "The extent to which data breaches result in identity theft is not well known, in large part because it can be difficult to determine the source of the data used to commit identity theft." The GAO also noted difficulties in quantifying harm resulting from the fact that identity theft victims do not know how their personal information was obtained; that stolen data may be held for

---

[271] *See* OECD, *supra* note 91.
[272] Damschroder, *supra* note 201.
[273] Ellen Nakashima and Rick Weiss, "Patients' Data on Stolen Laptop; Identity Fraud Not Likely, Says NIH," *Washington Post,* A-1 (March 24 2008).
[274] Caryle Murphy, "GU Breach Found Almost 3 Weeks Ago," *Washington Post*, A9 (march 5, 2006).
[275] University of Iowa, Department of Psychology, *Clinical Research Laboratory Security Incident*. Available at: http://www.psychology.uiowa.edu/faq.html.
[276] Andrew Lamar, 'State to Alert 1.4 Million About Possible Hacker Access," *San Jose Mercury News* 3-C (Dec. 4, 2004).
[277] *See* Solove, *supra* note 5 at 516-518.
[278] *See* U.S. Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited* (June 2007).
[279] *Id*. at 24-25.

lengthy periods of time before being used to commit identity theft; and that once stolen data have been sold or posted, the fraudulent use of the data may continue for years.[280]

Moreover, it is inappropriate to think of identity theft as the sole potential harm arising from breaches of security. Studies have indicated that security breach victims are likely to lose trust and confidence in the organization that held their information, even if the victim did not suffer direct, tangible harm such as identity theft.[281] There do not appear to be any studies that directly evaluate the intangible harm caused by security breaches in the research environment. However, it is likely that breaches by researchers would similarly undermine patient trust in their physician and researchers to maintain the confidentiality of their medical information. This potential effect was noted by the director of the NIH institute involved in the recent data breach, who issued a statement, that "when volunteers enroll in a clinical study, they place great trust in the researchers and study staff, expecting them to act both responsibly and ethically. . . .[W]e deeply regret that this incident may cause those who have participated in one of our studies to feel that we have violated that trust."[282] It is likely that the loss of trust is not isolated to those who are direct victims of the security breach. Such breaches may also impact the general public's trust that researchers will protect health information with which they have been entrusted.

Practicability

In practice, stakeholders across the board, from researchers to individual patients, questioned the meaning of the "practicability" standard.[283] There is no guidance as to what factors should be considered in determining whether the criteria are met, leaving a wide amount of discretion to individual IRBs or privacy boards. The Damschroder study indicates that patients believe it may be appropriate to consider the following two factors in determining whether it is practicable to conduct the research without the waiver of authorization:

- Having to contact each patient first would make the study less scientifically accurate;
- Having to contact each patient would make the results less useful in improving medical care (i.e., would produce selection bias).[284]

Further study in this area is warranted.

Authorizations to Use and Disclose Protected Health Information for Research: Future Research

Privacy Rule Provisions

The Privacy Rule gives individuals some degree of control over their personal health information by allowing them to authorize the use and disclosure of their protected health information that would otherwise be prohibited by the Rule. An individual may voluntarily authorize the use and disclosure of their protected health information for essentially any reason, including for research purposes.[285] To be valid under the Privacy Rule, an authorization must be written in plain

[280] *Id*. at 28-29.
[281] Ponemon Institute, National Survey on Data Breach Security Notification (Sept. 26, 2005).
[282] Murphy, *supra* note 274.
[283] *See* Stacey Tovino, "The Use and Disclosure of Protected Health Information for Research Under the HIPAA Privacy Rule: Unrealized Patient Autonomy and Burdensome Government Regulation, 49 *South Dakota Law Review* 447, 464 (2003/2004); Pritts and Neblo *supra* note 220.
[284] Pritts and Neblo, *supra* note 220.
[285] As a general rule, covered entities may not condition the provision of treatment payment or eligibility for benefits on the provision of an authorization (with the exception of research-related treatment). 45 C.F.R. § 164.508(b)(4).

language, and contain core elements (e.g., signature of the individual, description of purpose of requested use or disclosure) and statements addressing the individual's right to revoke authorization, circumstances under which services or payment may be conditioned on signing the authorization.

The Privacy Rule provides that an authorization must, among other things, describe "each purpose of the requested use or disclosure."[286] Under HHS's interpretation of this provision, an authorization must be related to a *specific* research study and *cannot* be used for future unspecified research.[287] HHS rejected the proposal to allow authorizations to encompass future research partially out of concern that individuals would lack the necessary information about future research to make an informed decision. In addition, HHS noted that individual authorization would not be required for future research if, with respect to the re-analysis of existing data, the researcher obtains a waiver of such authorization from the appropriate reviewing body. [288]

Authorizations for Future Research: Common Rule and Privacy Rule Interaction

The Common Rule permits the use of a general consent for future research. In practice, one consent is often all that is required to both create and use data in a research repository or database. The Privacy Rule considers the creation and maintenance of a research repository or database as a research activity separate from the subsequent use or disclosure of data from that repository for a research protocol. This means that an authorization to use or disclose protected health information to create a research database does not encompass permission to the future use or disclosure of that information for a particular research protocol. However, the subsequent use or disclosure by a covered entity from the database for a specific research study will require separate authorization unless permitted under some other provision of the Privacy Rule (*e.g.*, as a limited data set or pursuant to a waiver of authorization).[289]

Future Research: Value of Privacy Rule Approach

The requirement of the Privacy Rule that an authorization be limited to a specific research study can be seen as promoting patient autonomy and considered to be a positive development.[290] Under the principles identified in the Belmont Report, the Privacy Rule's requirement for a research study-specific statement arguably increases the likelihood that a particular individual will be able to make a quality decision regarding the use and disclosure of his personal health information.[291] A more specific statement of purpose will allow individuals with particular feelings regarding particular types of research to select those research activities for which they feel their information might to useful, and to decline to participate for research activities that they believe may not be in their best interests.[292] By identifying the specific research study for which the individual's information will be used or disclosed, the covered entity is giving the

---

[286] 45 C.F.R. § 164.508(c).
[287] Modified Rule Preamble, *supra* note 197 at 53226; U.S. Dept. of Health and Human Services, *Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule* NIH Pub. No. 03-5388 (2003) ("Protecting PHI in Research").
[288] *Id.*
[289] *See* U.S. Department of Health and Human Services, *Research Repositories, Databases, and the HIPAA Privacy Rule, NIH Public.* No. 04-5489 at 6 (2004).
[290] Tovino, *supra* note 283.
[291] *Id.* at 464.
[292] *Id*.

individual the freedom to act on his own best judgment. Another benefit of specific consent is that the practice of giving specific information and asking for specific consent shows respect for the individual subjects. [293]

Withholding information regarding the particular study for which the individual's information will be used or disclosed, when there is no compelling need to do so, could obstruct an informed decision and be seen as demonstrating a lack of respect for the individual. The more general the authorization is, the less informed it becomes. Some believe that that a permission to use health information for research that is unforeseen and for which there is no protocol is uninformed and not meaningful.[294]

Another view, however, is that allowing for broad authorizations for future research is laudable. Acceptance of such broad consent and future consent implies greater concern for autonomy than if such consents are prohibited.[295] Surveys consistently show that individuals want to have some say in whether their medical information is used for research.[296] There is some evidence that asking permission in even a general manner is acceptable to many individuals,[297] who view the process as a sign of respect.[298] A growing number of researchers endorse the concept that asking for blanket consent for the use of health information for research may be significantly more acceptable than never asking for authorization and leaving the matter solely in the hands of an IRB or privacy board.[299] This matter is further discussed in Evolving Issues, below.

Required Elements of Authorization Forms

The Privacy Rule specifies a number of elements that must be included on an authorization. These requirements are directed specifically at the use and disclosure of health information. The Privacy Rule's authorization requirements are listed on Table 1.

[293] *Id;* Mats Hansson et al. "Should Donors Be Allowed To Give Broad Consent To Future Biobank Research?" 7 *Lancet Oncology* 266-269 (2006).
[294] *See* Yeo, *supra* note 13.
[295] Hansson, *supra* note 293.
[296] Kass, *supra* note 203. Robling *supra* note 203; Whiddett *supra* note 204; Damschroder, *supra* note 201; Willison, *supra* note 200; Harris-Westin 2007 Survey, *supra* note 203.
[297] Hansson, *supra* at 293; Kass, *supra* note 203, Damschroder, *supra* note 201; Willison, *supra* note 200.
[298] Willison, *supra* note 200 at 707; Pritts and Neblo, *supra* note 220.
[299] *See* Kass, *supra* note 203. Damschroder, *supra* note 201; Paul Applebaum et al., "Researchers' Access to Patient Records: An Analysis of the Ethical Problems," 32 *Clinical Research* 399-403 (1984); O'Brien and Chantler, *supra* note 54; Robling, *supra* note 203.

TABLE 1 **Comparison of Common Rule Consent and Privacy Rule Authorization Requirements***	
Common Rule Consent	**HIPAA Authorization**
	Must be in "plain language"
Statement that study involves research; Description of research	Description of personal health information (PHI) to be used or disclosed; description of each purpose of the disclosure
Can be for unspecified future research	Must be study-specific; "blanket" authorizations for unspecified future research prohibited; Cannot be for various research projects (i.e., no compound authorizations)
Expected duration of subject's participation; approximate number of subjects involved	Expiration date or event ("at the end of the study" or "none" is acceptable for research projects)
Description of procedures to be followed; identification of any experimental procedures	Identification of persons/groups authorized to disclose PHI; identification of persons/groups (e.g., "researchers") authorized to receive PHI
Description of any foreseeable risks and statement that there may be unforeseeable risks; description of any reasonably expected benefits; disclosure of any appropriate alternatives that might be advantageous to the subject; statement describing extra costs to subject	
Statement describing confidentiality procedures;	Statement that once disclosed to researchers, PHI may no longer be protected by HIPAA (May, where applicable, state that researchers may not disclose info. without IRB approval)
Statement that participation is voluntary and withdrawal is permitted; statement that declining to participate or withdrawing will result in no loss of benefits; statement regarding involuntary removal of subject from study; consequences of early withdrawal and procedures for orderly withdrawal.	Statement that use/disclosure of PHI is voluntary or, if applicable, that participation in study requires use/disclosure of PHI; statement that subject can revoke authorization and description of exceptions (e.g., data retained for regulatory purposes)
Statement that significant new findings will be shared with subject	
Signature of subject or legally authorized representative (with description of person's authority) and date	Signature of subject or personal representative (with description of person's authority) and date

Authorization Required Elements: Common Rule and Privacy Rule Interaction

The Privacy Rule authorization form is distinct from the informed consent to participate in research required under the Common Rule, which focuses on a description of the research study and of its anticipated risks and/or benefits. A comparison of the authorization/consent requirements of the Privacy Rule and Common Rule is presented in Table 1. The two overlap in some respects because the Common Rule does require that an informed consent include a description of how the confidentiality of records will be protected. In response to requests from the research community, the Privacy Rule was modified to allow an authorization to be combined with an informed consent to participate in research,[300] but the combined form must contain all of the required core elements and statements.[301] The Privacy Rule does permit a covered entity to disclose information pursuant to an altered authorization form (which presumably could eliminate any duplicative requirements), provided that the alteration has been approved by an IRB.

Value of Privacy Rule Authorization Elements

HHS required specific elements in authorization forms to "ensure that individuals knowingly and willingly authorize the use or disclosure of [their] protected health information."[302] Researchers report that technically complicated informed consent and authorization forms make patients less willing to participate in research.[303] Some have expressed concern that research subjects are now paying less attention to the consent process because of the length of combined consents.[304]

The Privacy Rule requirements for authorization forms are most protective when information is used or disclosed for research that is not protected under the Common Rule, where there are not duplicative consent/authorization requirements. In those cases, the Privacy Rule authorization requirements may very well be the only mandatory requirements for a permission form that will govern.

Studies indicate that individuals want to be able to choose whether their health information is used and disclosed for research. However, we do not know which elements of authorization forms (or informed consent forms) are important to individuals, and which they may find confusing. To the extent that authorization forms as written confuse patients they are not promoting the individual's knowing and willing choice. Because the Privacy Rule permits disclosure under an altered authorization approved by an IRB, researchers may obtain permission to alter the requirements that they believe are duplicative or confusing.

Researchers have also indicated that the required statement that the Privacy Rule may no longer protect health information once it has been disclosed to the recipient is confusing to patients and deters them from signing the authorization.[305] However, HHS has indicated that, where applicable, it is permissible for authorizations for research to include a statement that researchers

---

[300] Modified Rule Preamble, *supra* note 197 at 53224-53225.
[301] 45 C.F.R. 164.508.
[302] Final Rule Preamble, *supra* note 188 at 82657.
[303] *See* J. Shen, L.F. Samson, et al., et al. "Barriers of HIPAA Regulation to Implementation of Health Services Research." 30 *Journal of Medical Systems* 65-9 (2006).
[304] *See e.g*., Susan Ehringhaus, *Testimony on Behalf of the Association of American Medical Colleges Before the National Committee on Vital and Health Statistics, Subcommittee on Privacy* (Nov. 19, 2003).
[305] 45 C.F.R. § 164.508(c).

may only use or disclose protected health information for purposes approved by the IRB or as required by law.[306]

Using and Disclosing Health Information for Reviews Preparatory to Research

Privacy Rule Provisions

The Privacy Rule permits covered entities to use or disclose protected health information for certain activities involved in preparing for research without the individual's authorization or a waiver of authorization. To do so, the covered entity must obtain from the researcher representations that:

- The use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;
- No protected health information is to be removed from the covered entity by the researcher in the course of the review; and
- The information sought is necessary for the research purpose.[307]

The intent of the provision was to permit covered entities to use and disclose personal health information to assist in the development of a research hypothesis and aid in the recruitment of research participants. [308] Researchers primarily have criticized two areas of impact of the Privacy Rule provisions governing activities preparatory to research: chart reviews and recruitment of research subjects.

Chart Reviews: Common Rule and Privacy Rule Interaction

Chart review is often an exempt activity under the Common Rule. [309] As such chart review does not require the informed consent of the research subject, under the Common Rule.[310] Under the Privacy Rule, covered entities may permit researchers to review medical records (*i.e.*, conduct chart reviews) *without* individual authorization provided they receive from the researcher the above representations.[311] The Privacy Rule does *not* require IRB or privacy board approval of such representations, although that is certainly permitted.[312] Neither does the Privacy Rule require that the researcher reviewing the record be an employee or a business associate.[313] The primary distinction between the regulations is the Privacy Rule's requirement for express assurances that the researcher will only review the information for purposes preparatory to

---

[306] Modified Rule, *supra* note 197 at 53226

[307] 45 C.F.R. § 164.512(ii).

[308] Final Rule Preamble, *supra* note 118 at 82537.

[309] Deidre Wipke-Tevis and Melissa Pickett, "Impact of the Health Insurance Portability and Accountability Act on Participant Recruitment and Retention," 30 *Western Journal of Nursing Research* 39 (2008).

[310] Institute of Medicine of the National Academies of Science, *Effect of the HIPAA Privacy Rule on Health Research: Proceedings of a Workshop Presented to the National Cancer Policy Forum,* Statement of Mark Barnes 79-80 (2006).

[311] U.S. Department of Health and Human Services, Clinical *Research and the HIPAA Privacy Rule*, NIH Pub. No. 04-5495 (2004).

[312] *Compare* 45 C.F.R. § 164.512(1)(i) (requiring documentation of board approval of authorization waivers) with 45 C.F.R. § 164.512(1)(ii) (where no board approval is required for reviews preparatory to research). Note, however, that research institutions must have in place a means for determining which studies qualify as exempt, and this duty is often assigned to the IRB. *See* Mary Lynn and Daniel Nelson, "Common (Mis)Perceptions About IRB Review of Human Subjects Research," 16 *Nursing Science Quarterly* 264-270 (2005).

[313] HHS, *Protecting PHI in Research*, *supra* note 287 at 17.

research, that the information sought is necessary for research and that they will not remove the information from the covered entity.

Chart Review: Value of Privacy Rule Preparatory to Review Provisions

The Privacy Rule's preparatory to research provisions allow researchers to review identifiable health information to assist in the development of research protocol and recruitment so long as they do not remove it from the premises. This provision ensures that protected health information remains relatively confidential within the covered entity. It also adds additional security protection for the personal health information by requiring that the information remain in control of the covered entity. Moreover, the Privacy Rule's requirements seem appropriate in light of some developing trends in research. First, there is a growing reliance on contract research organizations, for-profit intermediary companies that serve as the connection between hospitals and private physicians and researchers. [314] Many of these organizations, which may or may not be governed by the Common Rule, are involved in patient screening and recruitment. Some believe these organizations might encounter considerable conflicts of interests due to their for-profit nature.[315] The Privacy Rule preparatory to research provisions will help ensure that individually identifiable information reviewed for research is not improperly removed from the premises for other purposes. In addition, electronic medical records are becoming more prevalent. The Privacy Rule helps ensure that electronic medical records being reviewed in activities preparatory for research are not downloaded into other, potentially less secure, systems.

Some research indicates that the public is most comfortable with a nurse from the doctor's office or a research assistant from a university abstracting data from a medical record. The respondents were most concerned that the individual conducting the record review have confidentiality training.[316]

Recruitment: Common Rule and Privacy Rule Interaction

A key activity in research is often identifying and contacting prospective research subjects. Under the Common Rule, contacting individuals to determine if they would be interested in participating in a research study constitutes human subjects research. Such activities therefore require either:

- that the subject's informed consent be sought; or
- that the IRB approve an informed consent procedure that does not include or alters some of the requirements of informed consent; or
- that the IRB waive the requirement to obtain informed consent.[317]

Some report that the standard research practice is to require any communication about an available research study to come from the individual's treating physician or his/her staff.[318]

Under the Privacy Rule, a covered entity may allow any researcher who makes the appropriate representations review charts for activities preparatory to research, including for the purpose of

---

[314] Karen Morin, Herbert Rakatansky, et al. "Managing Conflicts of Interest in the Conduct of Clinical Trials," 287 *Journal of American Medical Association* 78-84 (2002).
[315] *Id*.
[316] Willison, *supra* note 200.
[317] *See* HHS *Clinical Research supra* note 311 at 5-7.
[318] Secretary's Advisory Committee on Human Research Protections, *supra* note 198 at App. C.

identifying patients. As interpreted by HHS, a researcher who is a workforce member of a covered entity may then contact potential study participants for the purpose of seeking an authorization to use or disclose protected health information under the Privacy Rule as part of the covered entity's health care operations.[319] The covered entity can also enter into a business associate agreement with a researcher to contact individuals on behalf of the covered entity to obtain their authorization.[320] In addition, because a covered entity is always permitted to disclose protected health information to the individual who is the subject of the information, a covered health care provider may freely discuss with the patient the option of enrolling in a clinical trial. [321]

In contrast, a covered entity may not allow an independent researcher not associated with the covered entity to contact individuals for recruitment absent an authorization or waiver of authorization.[322]

Recruitment: Value of Privacy Rule

The ability of a health care provider to disclose information about the potential for enrolling in a clinical trial under the Privacy Rule's provisions for treatment disclosures conforms to the Belmont report's distinction between the boundaries between practice and research. This provision preserves the intimate relationship between physicians and their patients.

The Privacy Rule's provisions that specifically address activities preparatory to research are not designed to address treatment relationships but are designed to govern the activities of researchers and their potential interaction with the patient. They were intended to avoid the unintended consequence of interfering with the development of research protocol and recruitment of research subjects.[323] As interpreted, the Privacy Rule permits any researcher who is employed by a covered entity as well as researchers who are business associates of the covered entity contact patients for recruitment.

Researchers have expressed concern that under current interpretation of the regulations, researchers who are affiliated with, but not part of the covered entity, for example physicians who have staff privileges, are treated differently from researchers employed by the covered entity. Since both may be equally subject to the covered entity's control through policies and procedures they say the distinction makes little sense. However, expanding the interpretation to allow yet more researchers to directly contact patients with whom they have no relationship would only further erode the protections afforded.

NBAC has noted that, "[T]he mere act of contacting people about participating in a research study may be a violation of their privacy, particularly when the prospective participants are identified as having a stigmatizing condition (e.g., HIV/AIDS, drug addiction)." [324] Research shows that patients prefer to be approached by their clinician or an associated nurse as opposed

---

[319] *Id*. at 4.
[320] *See* HHS *Clinical Research, supra* note 311 at 4.
[321] *Id*. at 9.
[322] *Id*.
[323] Preamble Final Rule, *supra* note 118 at 82701.
[324] NBAC 2001, s*upra* note 18 at 105.

to a stranger.[325] In fact, HHS has reported that most allegations of violations of the Privacy Rule related to research come from patients upset at receiving recruitment calls from unknown researchers.[326] In sum, it may appear that, if anything, the public would view the current interpretation of the Privacy Rule's provisions that govern recruitment as too lax.

Accounting of Disclosures

Privacy Rule Provisions

The Privacy Rule gives individuals the right to an accounting of the disclosures of their protected health information.[327] Under this right, individuals may request that a covered entity provide them with a comprehensive list of disclosures over the six years preceding the request, as well as certain substantive information related to each disclosure, including the date of the disclosure, the identity of the person who received the information, a description of the information disclosed, and a statement of the purpose of the disclosure. The accounting rules do not apply with respect to disclosures made pursuant to the individual's authorization or disclosures of a limited data set pursuant to an executed data use agreement.[328]

Researchers objected to the accounting requirements asserting that the need to account for each disclosure in a large research project would be burdensome and may deter covered entities from participating in research. They suggested that the covered entity be required only to disclose a listing of research projects under which an individual's information may have been released. In response, HHS amended the Privacy Rule to accommodate these suggestions.[329] Currently, when a covered entity has made disclosures of protected health information for research for 50 or more individuals, the covered entity may respond to a request for an accounting with a list of all protocols for which a person's personal health information may have been disclosed, including information about the research protocols, such as the name of the protocol and the purpose of the research.[330]

Accounting of Disclosures: Common Rule and Privacy Rule Interaction

The Common Rule has no similar requirement.

Value of Accounting of Disclosures

Individuals have a right to know who is using their health information and for what purpose.[331] The right to receive an accounting of disclosures is designed to provide individuals with this information when their health information is shared beyond the basic purposes of treatment, payment and health care operations.[332] HHS recognized that while individuals generally understand that their health information will be shared for these core purposes, they may not anticipate other disclosures of their health information, such as disclosures "to a university for

[325] *See* Robling, *supra* note 203.
[326] Christina Heide, *HIPAA Privacy Rule & Research: Update from HHS Office for Civil Rights.* Presented at IOM meeting June 14, 2007.
[327] 45 C.F.R. § 164.528.
[328] 45 C.F.R. § 164.528(a).
[329] Modified Rule Preamble, *supra* note 197at 53244.
[330] 45 C.F.R. § 164.528(b)(4).
[331] Final Rule Preamble, *supra* note 118 at 82740.
[332] Proposed Rule Preamble, *supra* note 120 at 59985.

research."[333] The approach is consistent with well-established privacy principles, with other law and with industry standards.[334]

There is insufficient information to gauge the value of the right to request an accounting of disclosures. First, we do not know why there have been relatively few requests for an accounting. There are a number of potential explanations for the scarcity of such requests. First, it is unclear that individuals even know they have a right to request an accounting.[335] Furthermore, presumably, most people request an accounting when they believe their information has been compromised in some fashion. Hopefully, those instances are few and far between, which may account for the relatively few inquiries. Finally, some have also suggested that there are relatively few requests for an accounting because the accounting does not give people the information that they seek.[336] The accounting does not include "uses" or disclosures for treatment, payment or health care operations. Due to this limitation, an accounting would not provide individuals with some of the information they are likely to want, such as a list of employees who looked at their medical record when they were in the hospital. In short, there is no empirical evidence as to why there are few requests for an accounting of disclosures.

Neither do there appear to be any studies that attempt to identify organizations that have successfully implemented the accounting of disclosures requirement, or the practices that they have put in place.

Research indicates that people want to know who has accessed their information and why.[337] One of the primary reasons individuals prefer that their consent be obtained before their health information is shared with researchers is so that they have some degree of control over their information—that they will know who has access to it. It is not a huge leap to conclude that most people would be extremely disturbed to find out that their health care provider cannot give them a list of the people and organizations with whom they may have shared their identifiable data and why. [338]

One justification for the accounting of disclosures requirement is to aid in identifying the source if a breach occurs. The suggestion has been made that the right to an accounting is not necessary for this purpose and other means of investigation would suffice.[339] However, no substitute method of potentially tracing disclosures to track a breach seems to have been proffered. One federal initiative, however, intends to examine the potential of shifting from accounting of disclosures to audit trails (of uses and disclosures).[340]

In sum, in a number of areas, the HIPAA Privacy Rule does afford privacy protections over those afforded in the Common Rule. Of particular importance, the Privacy Rule pertains to disclosures

---

[333] *Id.*
[334] *Id.*
[335] *See generally* CHCF 2005 Survey, *supra* note 37 and Damschroder, *supra* note 201.
[336] American Health Information Community, Confidentiality, Privacy, and Security Workgroup, Summary of the 14th Web Conference, (October 4, 2007) *available at* http://137.187.25.8/healthit/ahic/materials/summary/cpssum_100407.html
[337] Damschroder, s*upra* note 201.
[338] *Id*. Robling, *supra* note 203.
[339] *See* Ehringhaus Testimony, *supra* note 304.
[340] *Id.*

for research that would not otherwise be subject to the Common Rule. HIPAA's indirect method of protecting health information through imposing restrictions on the health care providers is not ideal. However, removing these protections without promulgating more direct regulations would effectively expose individuals to higher risks that their information may be shared, used and maintained in the research context in less than ideal circumstances.

V. Evolving Issues

Research involving genetic information and human tissue from which genetic information can be derived present perhaps some of the most challenging areas for protecting the privacy of health information. The mapping of the human genome in 2000 has led to high hopes for a better understanding of the role that genetics plays in illness, the ability to predict the likelihood of diseases long before they occur, and the creation of personalized medicine leading to more effective treatment.[341] As it has become clear that most common diseases are not linked to a single gene, research has begun to focus on the association of different genes or genomic regions with increased disease risk. [342] These association studies are expected to require data from a large population, resulting in efforts to create large genomic databanks, linking genetic information with personal information such as age, physical measurements, lifestyle and environmental factors.[343] Advances in genetics along with rapid increases in the speed of computing and transmission of data are also transforming the study of human biological materials. Increasingly, researchers are turning to existing repositories of biological samples and requesting patients to donate bodily tissue for storage and possible use at some future date for some human genetic study. [344] "The rapid pace of change in [genetic databases and] biobanks[345] has produced two powerful, but conflicting, social reactions. On the one hand, there is very strong public support for breakthroughs promising better medical diagnosis and treatments and, on the other, there are anxieties about increased loss of privacy and the potential for genetic discrimination, as well about the capacity to regulate genetic science in the public interest."[346]

The ability to assess the potential harms to individuals who are the subjects of research in these rapidly advancing areas is particularly difficult.[347] Precedent does not appear to provide sufficient guidance in this relatively uncharted territory.[348]

---

[341] Yael Bregman-Eschet, "Genetic Databases and Biobanks: Who Controls Our Genetic Privacy?" 23 Santa *Clara Computer & High Tech. Law Journal* 1 (November 2006); Yanick Farmer & Beatrice Godard, "Public Health Genomics (PHG): From Scientific Considerations to Ethical Integration," 3 *Genomics, Society and Policy* 14-27 (2007).

[342] Henry Greely, "The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks," *8 Annual Review of Genomics and Human Genetics* 343, 346 (2007).

[343] *Id.*

[344] M. Kapp, "Ethical and Legal Issues in Research Involving Human Subjects: Do You Want a Piece of Me?" 59 *Journal of Clinical Pathology* 335-339 (2006).

[345] While there is wide variation in the use of the terms genetic database and biobanks (*See* Anne Cambon-Thomsen et al., "Trends in Ethical and Legal Frameworks for the Use of Human Biobanks,"30 *European Respiratory Journa*l, 373, 375 (2007)), some have distinguished the terms on the basis that biobanks refer to databases in which the actual tissue samples and biological material are stored, not just the genetic information derived therefrom. Bregman-Eschet, *supra* note 341, notes 3-4 (citations omitted).

[346] Cambon-Thomsen, *supra* note 345.

[347] NBAC 1999, *supra* note 42.

[348] William Lowrance and Francis Collins, "Identifiability in Genomic Research," 317 Science 600 (Aug. 3, 2007).

Identifiability, *i.e*., the potential of data to be associated with specific individuals, is a crucial issue with respect to these large databanks.[349] As a practical matter, if information is not identifiable, the subject of the information should have fewer concerns about discrimination, stigmatization over recorded behavior and treatment (e.g., psychiatric treatment, abortion) or the potential repercussions of genetic information on family members since the information cannot be linked to them.[350] As a legal matter, information that is not identifiable is not subject to the requirements of the Common Rule. As discussed above, OHRP has issued guidance that, under certain conditions research involving only coded private information or specimens is not identifiable, and therefore, is not subject to the Common Rule because it is not human subjects research. In general, under this Guidance, if the researcher receives only coded information from either medical records or from a genetic database or biobank he would not need IRB approval for the research (or informed consent under the Common Rule) as long as either he had agreed with the holder of the key that the holder would not release the key to him until the subject is dead or the biobank had an IRB-approved policy prohibiting such release.[351] A researcher could use the information without an IRB approving the protocol and without obtaining the consent of the subjects of the information. In short, there is no role for the IRB or informed consent under this guidance.[352] Some researchers endorse this approach.[353] However, a number of experts have raised concerns about this approach, noting that it "potentially creat[es] an enormous regulatory gap in which, with a minimum of effort, the majority of research involving databanks can be excluded from the Common Rule."[354] Some have been particularly disturbed because the guidance allows information where the donors' identities can be readily ascertained to be treated as if it does not involve human subjects research and as if there were no risks involved.[355]

Yet, de-identification (and the less stringent anonymization) of information is particularly troublesome with respect to detailed databases containing genotypic and phenotypic data. The increase in genomic data coupled with the increase of computerization of other records about individuals, many of which are publicly available, increases the likelihood that data subjects can be re-identified. Single nucleotide polymorphisms (SNPs) contain information that can be used to identify individuals. [356] Even a small number of SNPs can identify an individual almost as precisely as a social security number does. [357] People who have access to individual data can potentially perform matches to public SNP data leading to matching and identification of individuals. Similarly, researchers with access to a large number of SNPs and corresponding phenotype data can potentially re-identify some individuals even if the information had been encrypted.[358] Professor Latanya Sweeney has demonstrated that specific DNA sequences of an individual's genomic data can be inferred from publicly available longitudinal clinical

---

[349] *Id*. Greely, *supra* note 342.
[350] Greely, *supra* note 342 at at 349-350. *See also* Yeo, *supra* note 13.
[351] Greely at 355.
[352] Ellen Clayton, "So What Are We Going To Do About Research Using Clinical Information and Samples?" 26 *IRB* 14-15 (2004).
[353] Lowrance and Collins, *supra* note 348.
[354] Clayton, *supra* note 352; *See* also Greely, *supra* note 342.
[355] Greely, *supra* note 342 at 355.
[356] Zhen Lin et al., "Genomic Research and Human Subject Privacy," 305 *Science* 183-184 (July 9, 2004).
[357] Russ Altman, et al., "Response to Protecting Privacy of Human Subjects" Letter, 307 *Science*, 1200-1201 (Feb. 2005).
[358] *Id*.

information.[359] There is thus a growing recognition that truly anonymizing data is becoming more difficult as a practical matter given the volume of genotypic and phenotypic information available, the speed of computing and transmitting that data, and the ability to link coded or anonymous data with publicly available databases. Thus, it will become more questionable to treat this information as if the use and disclosure of this information poses no risk at all to the individual.

Consent is perhaps an even more controversial issue with respect to genetic databases and biobanks.[360] Some believe that individuals have a fundamental right to decide whether and how their body, body parts and associated data will be used in research.[361] With respect to biobanks, some have suggested that at the time a sample is collected, individuals be offered a line-item consent that allows access to their biospecimens for research on particular diseases.[362] However, some have noted that blanket, future consents are particularly problematic since the decision also affects other family members. In such cases, they suggest that even with the individual's permission to use information in the future, extra steps be taken to ensure confidentiality is maintained, for example, requiring IRB review of future studies to ensure that risk is minimal and the research is in line with the individuals' general permission.[363]

The continued evolution of medical research in the age of genetics and electronic medical records depends on public support and trust. As many experts have pointed out, it is clearly the time for public dialogue on these issues.[364] Better informing patients about the importance of medical research and the need for their health records to be accessed by researchers, as well as ensuring them of the confidentiality of their information could potentially go far toward minimizing the tension between privacy and research.

VI. Suggested Approaches to Protecting Privacy While Promoting Research

The tension between personal privacy and the desire to use information for research is not likely to decrease anytime soon. To the contrary, the interests in protecting privacy and in making data more accessible appear to be coming more polarized. Some believe that society as a whole is moving towards a "rights based" approach to citizenship, which is reflected in the increased desire of individuals for control.[365] Some see this rights-based approach as promoting respect for autonomy, and consequently as a form of recognition of the attributes that give humans their moral uniqueness—of preserving human dignity.[366] The development of electronic health records is seen by some as the opportunity to adopt an approach to patient privacy and

[359] Bradley Malin and Latanya Sweeney, "How (Not) To Protect Genomic Data Privacy in a Distributed Network: Using Trail Re-identification To Evaluate and Design Anonymity Protection Systems," 37 *Journal of Biomedical Informatics*, 179-192 (2004).
[360] Cambon-Thomsen, *supra* note 345.
[361] Cambon-Thomsen, *supra* note 345 at 376; Greely *supra* note 342 at 356.
[362] Jimmie Vaught et al., "Ethical, Legal, and Policy Issues: Dominating the Biospecimen Discussion," 16 *Cancer Epidemiology Biomarkers & Prevention* 2521 (2007); NBAC 1999 *supra* note 42 (recommending that consent forms for human biological materials offer a number of options); Mark Rothstein "The Role of IRBs in Research Involving Commercial Biobanks." 30 *Journal of Law, Medicine & Ethics* 105-108 (2002); Hansson, *supra* note 293.
[363] *See* Hansson, *supra* at 293.
[364] *See* Willison, *supra* note 200; O'Brien and Chantler *supra* note 54; Len Doyal, "Informed Consent in Medical Research: Journals Should Not Publish Research To Which Patients Have Not Given Fully Informed Consent—With Three Exceptions," 314 *BMJ* 1107 (April 12 1997).
[365] Gostin, *Reconciling Personal Privacy supra* note 42; O'Brien and Chantler, *supra* note 54.
[366] O'Brien and Chantler, *supra* note 54 citing Doyal.

confidentiality that recognizes an autonomy-based, default position of full patient control over personal information.[367] The promotion of consumer-driven health care, which encourages patients to take greater control over their health care expenditures, their choice of providers and their treatment,[368] is likely to heighten consumers' expectations about the ability to exert more control over their health information.

From the research side, rapidly advancing fields in human genetics and electronic medical records with their tantalizing potential for major advances can make research activities seem especially important and compelling.[369] Some have suggested that certain types of medical records research should be exempt from *both* the Common Rule and the Privacy Rule restrictions. Many recognize, however, that patient privacy and autonomy are not absolute, and have proposed means of respecting the individual while permitting the use and disclosure of health information for research. As these advances in research become reality, it is important to be able to have a framework in which to assess the value of privacy and research.

One school of thought is that, in this changing environment, it is necessary to balance individual privacy rights with the "public good" of research.[370] Under this framework, obtaining individuals consent or permission to use health information for research is not necessary when their information is used for the common good of research, so long as the government has provided reasonably strong assurances of fair information practices and researchers observe the following standards:

- Identifiable data should be collected only when necessary for research;
- Data should be collected and used strictly for scientific assessment of the health care system and other essential public health purposes;
- Researchers should store data securely and allow only those who need access to use such data;
- Secondary disclosures of personally-identifiable data for non-communal goods (i.e., to employers insurers, commercial marketers) should be prohibited without the individual's informed consent;
- Researchers who violate individual privacy should be severely penalized; and
- Access to personally-identifiable health data without consent should also require impartial, outside scientific and ethical review that weighs:
    - Public benefits of research
    - Measures taken to protect the confidentiality of the data, and
    - Potential harms that could result from disclosure.[371]

This framework is intended to support the collection and use of valuable health data while protecting the individual's privacy.[372] It recognizes that although people do not have an absolute "right to be let alone" with respect to the use of their health information for research neither should they have "zero privacy."

---

[367] Terry and Francis, *supra* note 19 at 700.
[368] *See generally*, Greg Scandlen, "Commentary—How Consumer-Driven Health Care Evolves in a Dynamic Market," 39 *Health Services Research* 1113–1118 (2004).
[369] NBAC 1999, *supra* note 42.
[370] Gostin, *Reconciling Personal Privacy*, *supra* note 42.
[371] *Id*.
[372] *Id.*

Some scholars, however, fear that when patient privacy interests are weighed against other competing interests, "The likely result is that these other interests will prevail, particularly when they have been labeled, rightly or wrongly, public interests."[373] Others note that the costs associated with privacy, confidentiality and security breaches are often intangible and difficult to evaluate.[374] To avoid the potential for a "zero sum" result in balancing privacy and research interests, the following factors should be considered: [375]

- Not all research is in the "public good."
  Research is no longer a purely academic exercise and now is often market-driven, involving the pursuit of economically exploitable intellectual property rights.[376] The mind-set of market-driven research is "in distinct opposition" to research that is truly conducted for the public good. The former embraces competition and the private retention of research data and profits, while the latter is based on communitarian values and public dissemination of research results.[377]
- Privacy is not just an individual right, it is also a common good.[378]
  In balancing privacy and research, privacy should be viewed not just an individual right or interest, but in the broader perspective of its importance to society in general. Society itself is better off when privacy exists because it serves common, public and collective purposes. [379]
- Legal rules are written to protect the public from the consequences of the worst case scenario.
  Undoubtedly most researchers are trustworthy and take efforts to protect health information. However, the rules are written to protect society from the small percentage of those who are careless, or worse, but whose actions have the potential to diminish the reputation of all.
- Some difficulties in implementing laws result not from the requirements of the law itself, but from the manner in which parties interpret the law.
  The HIPAA Privacy Rule in particular is a complex regulation, which has been subject to varying interpretation. Guidance from HHS and education could potentially ameliorate some of the concerns voiced by researchers.

Regardless of how these issues are balanced, any potential revision of the HIPAA Privacy Rule would only begin to touch the myriad issues of protecting the privacy of health information in research. Revising the Privacy Rule will not create a uniform set of regulations. Neither would it answer the pressing challenges posed by genetic databases and biobanks. Ultimately, a more uniform approach is warranted, not only for the ease of researchers, but also to afford uniform protection of the privacy of health information.

---

[373] Beverly Woodward, "Confidentiality, Consent and Autonomy in the Physician-Patient Relationship," 9 *Health Care Analysis* 337-351 (2001).
[374] Terry and Francis, *supra* note19.
[375] Valerie Steeves, *Will Changes in Data Health Privacy Legislation Kill Research As We Know It?"* presented at the 2004 Annual Labelle Lectureship, Centre for Health Economics and Policy Analysis, McMaster University, available at: http://www.idtrail.org/files/Steeves_Health_Privacy_Paper.pdf
[376] *See generally* Justin Bekelman, et al., "Scope and Impact of Financial Conflicts of in Biomedical Research: A Systematic Review," 289 JAMA 454-465 (January 22/29 2003).
[377] *See also* Sheldon Krimsky, *Science in the Public Interest: Has the Lure of Profits Corrupted Biomedical Research*? Rowman & Littlefield, Lanham, MD (2004).
[378] Steeves, *supra* note 375.
[379] Regan *supra* note 31 at 231.

Acknowledgments
The author would like to thank Laura Levit, JD of the National Cancer Policy Forum, Institute of Medicine, and Jennifer Libster, JD and Sarah Plake, JD of Georgetown University's Health Policy Institute for their valuable research assistance.

Attachment 1 Comparison of Criteria for Granting Waivers or Alterations of Authorization/Consent‡

Area of Distinction	HIPAA PRIVACY RULE 45 C.F.R. § 164.512(i)(2)(ii)	"Common Rule" (HHS Protection of Human Subjects Regulations 45 C.F.R. § 46.116(d))	"Common Rule" (HHS Protection of Human Subjects Regulations 45 C.F.R. § 46.117(c))
Standard	Permits disclosure of protected health information for research without authorization where IRB or Privacy Board has granted waiver or alteration of authorization when all of the following criteria are met	IRB may waive some or all of the elements of informed consent or to waive the requirement to obtain informed consent provided IRB finds and documents all of the following:	Permits an IRB to waive the requirement to obtain a signed consent for some or all of the research subjects if it finds either of the following
Risk Criteria	Use or disclosure involves no more than *minimal risk* to the privacy of individuals based on: o An adequate **plan to protect** the identifiers from improper use and disclosure; o An adequate **plan to destroy the identifiers** at the earliest opportunity absent a health or research justification or legal requirement to retain them; *and* o Adequate **written assurances that the protected health information will not be used or disclosed to a third party** except as required by law, for authorized oversight of the research, or for other research uses and disclosures permitted by the Privacy Rule; and	The research involves no more than *minimal risk* to the subjects. The waiver or alteration will not adversely affect the rights and welfare of the subjects;	That the only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality* *O r* That the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.**
Practicability Standard	Research could not practicably be conducted without the wavier or alteration The research could not practicably be conducted without access to and the use of the protected health information	Research could not practicably be conducted without the wavier or alteration	N/A
Provision of Pertinent Information Requirement	N/A	Whenever appropriate, the subjects will be provided with additional pertinent information after participation.	N/A

‡Derived from U.S. Department of Health and Human Services, *Protecting Personal Health Information in Research* chart page 15.

* Must ask subject whether he wants documentation linking him with the research, and comply with subject's wishes

* * May require investigator to provide subjects with a written statement regarding the research when waiver granted