2002

The Nationalization of Health Information Privacy Protections

Lawrence O. Gostin
Georgetown University Law Center, gostin@law.georgetown.edu

James G. Hodge Jr.
Arizona State University

Lauren Marks
USAID

This information or any portion thereof may not be copied or disseminated in any form or by any means or downloaded or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

This paper can be downloaded free of charge from:
https://scholarship.law.georgetown.edu/facpub/93


This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author. Follow this and additional works at: https://scholarship.law.georgetown.edu/facpub

Part of the Health Law and Policy Commons
The Nationalization of Health Information Privacy Protections*


Lawrence O. Gostin
Professor of Law
Georgetown University Law Center
gostin@law.georgetown.edu

James G. Hodge, Jr.
Professor of Health Law and Economics
Sandra Day O’Connor College of Law
Arizona State University
james.hodge.1@asu.edu

Lauren Marks
Health Program Private-Public Partnerships Advisor
USAID
lmarks@usaid.gov

This paper can be downloaded without charge from:
Scholarly Commons: http://scholarship.law.georgetown.edu/facpub/93/

Posted with permission of the author

* This information or any portion thereof may not be copied or disseminated in any form or by any means or downloaded or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
THE NATIONALIZATION OF HEALTH INFORMATION PRIVACY PROTECTIONS

Lawrence O. Gostin, James G. Hodge, Jr., and Lauren Marks

I. INTRODUCTION

On April 14, 2001, President George W. Bush approved the Standards for Privacy of Individually Identifiable Health Information. These regulations, which represent the first systematic national privacy protections of health information, flow from a congressional mandate in the Health Insurance Portability and Accountability Act of 1996. HIPAA requires the implementation of health information privacy protections, either through federal leg-

---

1. Hereinafter health data privacy regulations.

Lawrence O. Gostin is Professor of Law, Georgetown University Law Center; Professor, Johns Hopkins Bloomberg School of Public Health; Director, Center for Law and the Public’s Health at Georgetown and Johns Hopkins Universities; and Visiting Fellow, Centre for Socio-Legal Studies, Oxford University. James G. Hodge, Jr., is Adjunct Professor of Law, Georgetown University Law Center; Scientist, Johns Hopkins Bloomberg School of Public Health; and Project Director, Center for Law and the Public’s Health at Georgetown and Johns Hopkins Universities. Lauren Marks will receive her J.D. in May 2003 from Georgetown University Law Center and is a research assistant at the Center for Law and the Public’s Health at Georgetown and Johns Hopkins Universities.


---
islation or administrative regulation, by the Department of Health and Human Services.\(^4\) These health data privacy regulations protect the privacy of individually identifiable health records in any form (e.g., electronic, paper, oral) by limiting disclosure and use, regulating privacy and security policies, and implementing fair information practices. The provisions apply to "covered entities," including health providers, health insurance plans, and health care clearinghouses, as well as their business associates.

There are two primary justifications for safeguarding health information privacy: (1) the personal nature of health data and (2) the rapid shift from paper to electronic records. Health information used by health providers, insurers, and data processors can include intimate details about the patient's mental and physical health as well as information about the patient's social behaviors, personal relationships, and financial status.\(^5\) Unwarranted disclosures of this information could lead to societal stigmatization and discrimination by employers, insurers, and others, as well as a loss of patient trust in medical providers.\(^6\)

Privacy concerns have been compounded by the proliferation of and access to health records resulting from the shift to electronic medical record keeping within the national health information infrastructure. Health information is increasingly accessed, used, disclosed, and stored in electronic format. This does not necessarily mean that health data are less secure, as electronic systems are in many ways safer than manual systems. Nevertheless, electronic data can be accessed in greater quantities and manipulated in ways that are virtually impossible for manual systems. Thus, while significant benefits may flow from the electronic health information infrastructure, the potential to disclose or reveal sensitive health data has raised individual fears of privacy violations.\(^7\) In one recent survey, more than 80 percent of the public respondents felt that they had "lost all control over their personal information.\(^8\)

The new HIPAA regulations provide the most comprehensive national protection of health information. While most states have privacy safeguards, they are so variable and incoherent that they are widely regarded as inadequate. Congress's grant of authority to HHS to develop privacy

---

4. Hereinafter HHS.
6. See id. at 490–91.
regulations offered the promise of a comprehensive solution to the concerns of consumers and privacy advocates. Through the regulations, HHS attempts to protect individual privacy while recognizing legitimate needs for such data to process health claims and deliver medical care, as well as to provide for communal goods (e.g., public health and health research).

Specifically, the regulations implement fair information practices, which have long been a feature of existing federal laws. Fair information practices allow patients to: (1) inspect and amend their records; (2) be notified of covered entities' privacy practices and potential uses and disclosures of health information; and (3) request confidential communications and an account of actual disclosures. The regulations also endeavor to protect patient privacy by limiting uses and disclosures of individually identifiable medical information or “protected health information.”

Disclosure and use of PHI can only occur with patient consent, subject to several exceptions, including: (1) law enforcement: law enforcement officials may receive information from covered entities without consent pursuant to a court order, subpoena, or other legal order; (2) judicial and administrative proceedings: a covered entity may disclose PHI in a judicial or administrative proceeding without the individual's consent in response to a court order or administrative tribunal or in certain circumstances, in response to a subpoena or discovery request; (3) parents of unemancipated minors: parents are recognized as personal representatives of unemancipated minors; while the current rule restricts parents' access to the child's medical record, the Bush administration is likely to relax those limitations; (4) "significant others," including family members, friends, and caretakers of adults and emancipated minors: covered entities may disclose limited health information of an adult or emancipated minor without consent to a relative, personal friend, or designated person in the case of an emergency or in the course of the significant other's basic care-taking duties; (5) public health: PHI can be disclosed for numerous public health purposes without consent, including: (a) to prevent or control disease, injury, or disability; (b) to report child abuse or neglect; (c) to report relevant information to the Food and Drug Administration; and (d) to report to an employer conducting medical surveillance in the workplace if the employee is notified; (6) health research: a covered entity can use or disclose individually identifiable health information for research without consent if it obtains a waiver from an Institutional Review Board or a privacy board; and (7) commercial marketing: covered entities may use or disclose personal health information for

---

9. See infra Part III.C.
10. Hereinafter PHI.
12. Hereinafter IRB.
face-to-face commercial marketing to individuals or for the marketing of products and services of nominal value.

To be effective, a comprehensive, national health information privacy policy should balance individual interests in protecting the privacy of health data with societal needs to share the data for communal purposes. However, many of these provisions leave significant gaps in privacy protection. HHS admits that the regulation only sets a "floor" of protection that "balance[s] the needs of the individual with the needs of society." At times, the regulation makes inappropriate trade-offs between the public welfare and individual privacy that may either fail: (1) to protect individual privacy or (2) to accomplish significant communal benefits (e.g., public health, health research).

In Part II, this article examines the justifications for implementing comprehensive national health information privacy regulations, including the personal nature of health information and the increasing threats to personal privacy from the shift to an electronic health information infrastructure. In doing so, it looks at historical attempts by federal and state officials to regulate the use and disclosure of personal health information, and concludes that prior standards have been largely inadequate. In Part III, this article explains the new national health information privacy regulations: (1) what do they cover?; (2) to whom do they apply?; (3) how do they safeguard personal privacy through notice and security provisions?; and (4) do they preempt existing legal privacy protections?

Part IV of this article examines two autonomy rules established in the national privacy rule: "informed consent" (for uses or disclosures of identifiable health data for health care-related purposes) and "written authorization" (for uses or disclosures of health data for nonhealth care-related purposes). The article observes that the informed consent rule is neither "informed" nor "consensual." The rule is thus likely to thwart the effective administration of health organizations without benefiting individuals. Requiring written authorization, on the other hand, protects individual privacy to prevent disclosure of information to entities that do not perform health-related functions, such as employers and life insurers. Lastly, this article also examines various contexts in which data can be shared for public purposes under the national privacy rule: to law enforcement officials; for judicial and administrative proceedings; to parents of unemancipated minors; to "significant others"; to public health authorities; for health research; and for commercial marketing.

II. PERSONAL PRIVACY IN THE ELECTRONIC HEALTH INFORMATION INFRASTRUCTURE

A. Electronic Health Data

Protecting the privacy of identifiable health information was one of Congress's key priorities in enacting HIPAA. Congress desired better privacy protections because of its concern over the proliferation of electronic health information. During the mid-1980s, fundamental shifts in the organization, delivery, and financing of health care services led to the development of more sophisticated health information systems. Individual patient medical records are increasingly stored in electronic databases by the government and private medical providers. The goal of HIPAA, as expressed by the Institute of Medicine and others, was that patient medical records should be recorded in every health care setting so they could be accessed widely among health care professionals. These changes are transforming the ways in which health information is acquired, used, disclosed, and stored in the modern health care system.

There are many advantages to the systemic collection and use of electronic health data. More accurate and accessible data allow consumers to make more informed decisions about their individual health care needs, including health plans, providers, diagnoses, products, and treatments. Clinical care is improved through faster and more accurate diagnoses, increased checks on medical procedures, prevention of adverse drug events, and the dissemination of expert medical information in areas traditionally underserved through telemedicine and other techniques. Public health surveillance of injuries and diseases in the population is facilitated. Medical research on the causes of injuries and disease and health services research concerning the quality and cost effectiveness of health care services are improved through increased access to (and more accurate) infor-

16. See Gostin, supra note 5, at 452.
Electronic security tools, including personal access codes, encryption programs, and audit trials, can more efficiently monitor health care fraud and abuse and protect data from unauthorized uses and disclosures.

Along with these benefits, however, come significant costs. The computerization of health data raises significant privacy concerns. Health care data concerning individuals are among the most sensitive types of personal information. These records contain large amounts of personal information that can be used to create a profile of an individual, including:

1. Demographic information, such as age, sex, race, marital status, children, and occupation;
2. Financial information, such as employment status, income, and methods of payment;
3. Medical information about diagnoses, treatments, disabilities, end-of-life decisions, and disease histories of the individual and family members;
4. Genomic information such as diagnostic tests for carrier traits and genetically related diseases;
5. Personal identifiers other than name, including Social Security number, addresses, and phone numbers; and
6. Information about why treatment is sought, such as being the victim of a violent crime, firearm injury, or the at-fault party in an auto accident.

In a society that strongly values individual autonomy and decision making, protecting the privacy of personally identifiable health data is critical. Insufficient protection of health care information can lead to unauthorized disclosures, which in turn may subject individuals to social stigma and discrimination by insurance companies, health care professionals and institutions, and employers. Patients have a reasonable expectation of privacy in their personal affairs provided that the exercise of these interests does not harm others. Respecting personal privacy requires that individuals maintain some degree of control over their personal information. In addition, protecting the privacy of individually identifiable health information is important to achieving benefits for the population, such as public

---

23. See Gostin, supra note 5, at 481.
health surveillance and longitudinal health research. As we (and others) have stated, protecting health information privacy (e.g., by providing individuals some control over their health data without severely restricting warranted uses of the data) directly improves the quality of health care and public health data (e.g., by encouraging individuals to fully utilize health services and cooperate with health agencies).

B. Existing Legal Protections

Safeguarding personal privacy through legal mechanisms allows for the creation of standards that are enforceable through courts and administrative bodies. Legal safeguards may be expressed through federal or state constitutional protections of health information privacy, case law, or legislative and administrative law. Despite the potential of the law to protect privacy, existing safeguards are inadequate, fragmented, and inconsistent. There exist major gaps in legal protection of health privacy as well as significant theoretical problems with the structure of privacy protections.

1. Constitutional Right to Privacy

Apart from the Fourth Amendment, the U.S. Supreme Court has not articulated a clear, strong standard for a constitutional right to informational privacy. Judicial recognition of a constitutional right to informational privacy is particularly important because the government is a primary collector and disseminator of health information. A constitutional right could shield individuals from unauthorized government acquisition or disclosure of personal information.

The U.S. Constitution does not expressly provide a right to informational privacy. The judiciary, however, has recognized a limited right to informational privacy as a liberty interest under the substantive Due Process Clauses of the Fifth and Fourteenth Amendments. In Whalen v. Roe, the U.S. Supreme Court examined whether the constitutional right to privacy encompasses the collection, storage, and dissemination of health information in government data banks (specifically, a New York public health database containing pharmaceutical records). Although the Court acknowledged a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive govern-


31. See Gostin, supra note 5, at 495–98.

ment files," it failed to tailor a constitutional remedy to meet this threat. Justice Stevens, writing for a unanimous Court, simply recognized that "in some circumstances" the duty to avoid unwarranted disclosures "arguably has its roots in the Constitution." Provided that the state had adequate standards and procedures for protecting the privacy of sensitive medical information, the Court found no privacy violation. Whalen has been subsequently interpreted as affording a tightly circumscribed right to informational privacy.

In general, courts have employed a flexible test balancing the government invasion of the individual's privacy against the strength of the government interest. Where the government can articulate a valid societal purpose and employs reasonable security measures, traditional governmental activities of information collection do not infringe an individual's constitutional informational privacy rights. Any right to privacy under the federal or state constitutions is, of course, limited to government action. Thus, collection and use of health data by private or quasi-private health data organizations, health plans, researchers, and insurers are constitutionally unprotected.

2. Common Law Protections

Most states recognize, via common and statutory law, the legal duties of confidentiality of certain health care professionals (e.g., physicians, nurses, lab technicians) not to disclose health information. Yet, these duties are not absolute. Disclosures without individual consent may lawfully be made to: (1) protect third parties from identifiable harm, (2) report information for public health purposes as required by state law, or (3) notify in some cases of medical emergency. Unwarranted disclosures, however, may subject responsible parties to civil liability.

33. Whalen, 429 U.S. at 605.
34. Id.
35. Id.
36. See United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980) (holding that the National Institute of Occupational Safety and Health was entitled to receive the medical records of private employees exposed to toxic substance, subject to their informed consent). The court enunciated five factors to be balanced in determining the scope of the constitutional right to informational privacy: (1) the type of record and the information it contains, (2) the potential for harm in any unauthorized disclosure, (3) the injury from disclosure to the relationship in which the record was generated, (4) the adequacy of safeguards to prevent nonconsensual disclosure, and (5) the degree of need for access, i.e., a recognizable public interest. Id. at 578.
37. See, e.g., Rasmussen v. S. Fla. Blood Serv., Inc., 500 So. 2d 533 (Fla. 1987). "Since the 1970's, more than a dozen states have adopted constitutional amendments designed to protect a variety of privacy interests, including limitations on access to personal information." Gostin, supra note 5, at 498.
Although a traditional construct of privacy protections and a forerunner of modern privacy theory, the duty of confidentiality is antiquated. Confidentiality is predicated on the existence of a physician/patient relationship. Modern data collection is based only in small part on this relationship. Health records contain a substantial amount of information gathered from numerous primary and secondary sources: laboratories, pharmacies, schools, public health officials, researchers, insurers, and other individuals and institutions. Paper or electronic patient health records are kept by government agencies, regional health database organizations, and information brokers. The duty of confidentiality arising at the point of clinical care or research simply does not protect the patient from disclosure by these secondary sources of data.

3. Existing Legislative and Administrative Protections

Federal and state legislatures and executive agencies have enacted and considered a growing number of statutes and regulations to protect privacy. The federal government has previously enacted several statutes and regulations to protect privacy of health information. The Privacy Act of 1974 requires federal agencies to utilize fair information practices regarding the collection, use, or dissemination of systematized records, including health data. The Freedom of Information Act of 1966 exempts personally identifiable health information from public dissemination by the federal government. Other federal regulations protect health information privacy relating to the treatment of persons for drug or alcohol dependency in federally funded facilities, and the administration of human subject research.

Most states have passed privacy statutes that mimic the federal Privacy Act and FOIA, both of which apply to state collections of data. A few states have enacted comprehensive medical information privacy acts. These laws provide broad protections of health information acquired, collected, used, or disclosed within the state. States have also passed disease-specific privacy laws that set forth stringent privacy and security protections for certain types of information, including medical information concerning one's HIV status.
or other communicable diseases, genetic information, information utilized in medical research (such as state cancer registries), or public health information.

Although existing federal and state privacy statutes and regulations are meaningful and serve valuable ends, they share several weaknesses: (1) like constitutional privacy protections, most statutes apply primarily to government collections, uses, or disclosures of health information, and thus often do not confer protections to health information in the private sector; (2) they fail to address the new challenges to individual privacy arising from the automation of medical records; (3) they collectively represent a patchwork effort to address the privacy and security of specific health information; (4) some kinds of data are treated as superconfidential (e.g., HIV/AIDS), while other data are virtually unprotected, leading to inconsistencies and unfairness; (5) they do not effectively balance competing individual interests in privacy with the need to use the data for the common good; and (6) some state laws prohibit disclosures without informed consent, but make so many exceptions as to negate the prohibition.

These weaknesses in existing law suggest the need for a comprehensive approach to privacy protection. The health data privacy regulations provide a national standard to protect health data. However, like existing privacy laws, the regulations may inadequately protect individual privacy and also fail to assure that data are shared where necessary to protect the public's welfare.

III. HEALTH INFORMATION PRIVACY PROTECTIONS UNDER THE NATIONAL REGULATIONS

The creation of national health information privacy regulations might seem uncontroversial in light of existing public apprehensions to disclosure, current gaps in legal protections, and Congress's commitment to better protect such data. However, the health privacy rule was established only after years of struggle and efforts in the legislative and executive branches. Under HIPAA, Congress created a self-imposed deadline of August 21, 1999, to pass health information privacy legislation. As a result of interest group lobbying, a diverse health law and policy agenda, and politics, Cons...
gress failed to pass comprehensive privacy laws by the deadline.\(^{53}\) HIPAA authorized the Secretary of HHS to issue privacy regulations if Congress failed to act.\(^{54}\) The initial publication, HHS's proposed regulations in November 1999,\(^{55}\) garnered over 52,000 public comments.\(^{56}\) The final rule was promulgated in December 2000, at the end of President Clinton's term.\(^{57}\) Reflecting President Bush's promise to reassess regulations enacted late in his predecessor's term,\(^{58}\) the comment period was reopened and HHS received several thousand additional comments.\(^{59}\) Although privacy advocates were concerned that the Bush administration would scale back or eliminate the rules altogether,\(^{60}\) HHS announced on April 12, 2001, that the final regulations as previously constructed would go forward, subject to interpretive guidelines developed by HHS.\(^{61}\) The first of these guidelines was released in July 2001.\(^{62}\) The regulations take effect for most covered entities on April 12, 2003, and one year later for small health plans.

Although their development was convoluted, the health data privacy regulations attempt to establish a national baseline of health information privacy protection,\(^{63}\) although individual privacy is both under- and overprotected.

A. The Scope of the Standard

At least two questions are important in the development of national health information privacy regulation: (1) what information should be protected,
and (2) from whose actions should the information be protected? These questions are partially answered by the limits of HHS’s authority under HIPAA.64

**What Information Is Protected?** The regulations explicitly cover health information65 that is individually identifiable.66 Individually identifiable health information includes any data that contain unique identifiable characteristics, including a name, Social Security or driver’s license number, fingerprint, or genetic link.67 Where health data are truly nonidentifiable (e.g., aggregate statistical data, nonlinked data, or other data stripped of all individual identifiers), privacy interests are minimal. Consequently, the national privacy rules do not restrict access, use, or disclosure of nonidentifiable data.68 HHS permits covered entities to assign codes69 to allow for later re-identification, but requires steps to prevent harmful identifications.70

---

64. For a discussion on the constitutional issues raised by the jurisdictional concerns, see A. Craig Eddy, *A Critical Analysis of Health and Human Services’ Proposed Health Privacy Regulations in Light of The Health Insurance Privacy [sic] and Accountability Act of 1996*, 9 ANNALS HEALTH L. 1, 50–60 (2000).

65. Health information is comprehensively defined as data (1) “created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse,” and (2) “relat[ed] to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.” 45 C.F.R. § 160.103 (defining “health information”).

66. *Id.* § 164.514. HHS defines individually identifiable health information as health information that “identifies an individual . . . or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.” *Id.* § 164.501. The regulatory definition limits the term to only a subset of health information, specifically information created or received by health care providers, health plans, employers, or health care clearinghouses. *Id.*

67. The health data privacy rule outlines two means for determining if health information is not individually identifiable, or “de-identified,” and thus no longer regulated by the rule. First, an expert utilizing accepted analytical techniques can conclude that “the risk is very small that the information could be used, alone or in combination with other reasonably available information” to identify the subject of the information. *Id.* § 164.514(b)(1)(i). A second permitted means of de-identification is that the covered entity can remove a comprehensive set of identifiers of the individual and of relatives, employers, and household members of the individual. These identifiers include: names; geographic subdivisions smaller than a state; dates more specific than years; contact information such as telephone and fax numbers and e-mail addresses; identification numbers such as Social Security numbers, account and medical record numbers, and license place numbers; and full face photographic images. *Id.* § 164.514(b)(2)(i)(C).


69. Information can be ostensibly anonymous, yet linkable to an individual because of codes frequently utilized by health care organizations, researchers, and the government. Concern is raised about deliberate or accidental disclosures of coded information, not literally protected by law, where the code is broken or inadequate. See Gostin, *supra* note 5, at 520.

70. The code must not be derived from or related to information about the individual or able to be translated so that the individual can be identified. 45 C.F.R. § 164.514(c)(1). The covered entity must also not disclose or use the code for other purposes than record identification and cannot disclose the mechanism for re-identification. *Id.* § 164.514(c)(2).
PHI is comprised of all forms of information, including electronic, oral, and paper communications. Realistically, it is impractical to separate protections for paper-based records from electronic or oral-based data. Under HIPAA, Congress may have limited HHS's authority to regulate nonelectronic communication. Although HHS maintains that it has "ample legal authority," provisions concerning nonelectronic communications are severable from electronic communications by court action. Protecting all health information enhances the efficacy of the regulation. Otherwise, a significant amount of nonelectronic health communications would remain unregulated by federal law. Additional complications relate to enforcing a national regulation that applies to only some types of health data depending on how they are communicated or stored.

Who Is Covered? HHS regulates "covered entities," which include all possible groups that it is authorized to reach under HIPAA. These covered entities include health plans, health care clearinghouses, and health care providers. Health plans, which provide or pay for the cost of medical care, are covered whether they are private entities (e.g., health insurer,
managed care organization) or government organizations (e.g., Medicaid, Medicare, the Veterans Administration).\textsuperscript{77} Health care providers (e.g., physicians, hospitals, clinics) are covered if they “transmit any health information in electronic form in connection with a transaction covered by [the regulation].”\textsuperscript{78} Such electronic exchanges can include billing and fund transfers in addition to health information communications.

The regulations also cover business associates of the covered entities. Business associates are lawyers, accountants, billing companies, and other contractors whose positions involve the use or disclosure of individually identifiable health information.\textsuperscript{79} Although HHS lacks the authority to directly regulate business associates, it requires covered entities to obtain satisfactory assurances that their business associates will comply with privacy standards.\textsuperscript{80} Should a covered entity know of a violation and do nothing to address it, the covered entity may be considered to be violating HIPAA's privacy standards.\textsuperscript{81} Through this oversight function, HHS is able to regulate the downstream users and processors of PHI.\textsuperscript{82}

Although the regulations are comprehensive, not all persons or entities that regularly use, disclose, or store identifiable health data are covered. The regulations do not cover groups such as life insurers and worker’s compensation insurers and programs, even though these entities regularly use personal medical information.\textsuperscript{83} Additional protections governing all identifiable health data, regardless of its holder or manner of communication, are needed to complete a national standard of health information privacy.

B. Privacy and Security Policies for Covered Entities

In addition to an individual’s right to control uses and disclosures, the development of privacy and security policies for covered entities is important to prevent privacy breaches and maintain consumers’ trust in the health care system. Without such policies, accidental disclosures from

\textsuperscript{77} Id. § 160.103 (defining “health plan”). Employers utilizing employer-sponsored health plans (governed by ERISA) are not considered covered entities when administering the plan (as “plan sponsors”). However, the standard outlines numerous requirements for employer-sponsored health plans, which are covered entities, to disclose PHI to plan sponsors/employers, including an agreement that the sponsor will not use or disclose the information for employment decisions. Id. § 164.504(f)(1), (2).

\textsuperscript{78} Id. § 160.102(a)(3).

\textsuperscript{79} Id. § 160.103.

\textsuperscript{80} Id. § 164.502(e)(1)(i).

\textsuperscript{81} Id. § 164.502(e)(iii).

\textsuperscript{82} See Lawrence O. Gostin, National Health Information Privacy: Regulations Under the Health Insurance Portability and Accountability Act, 285 JAMA 3015, 3016 (2001).

sloppy record keeping and purposeful disclosures by and to unscrupulous parties may increase.\textsuperscript{84} The health data privacy regulations mandate that covered entities develop privacy and security policies while maintaining the flexibility necessary for the large variety of participants covered.\textsuperscript{85} Covered entities must implement policies that reasonably protect individuals from any "intentional or unintentional use or disclosure in violation of the standards, implementation specifications or other requirements."\textsuperscript{86} Covered entities must not only guard against a deliberate attempt to use protected information, but must also endeavor to prevent accidental uses and disclosures. Procedures must be developed to allow for complaints concerning the policies or the covered entities’ compliance with the policies.\textsuperscript{87} Persons who violate privacy policies could be sanctioned.\textsuperscript{88}

A covered entity may not require an individual to waive these rights in order to receive care, enroll in a health plan, or obtain benefits.\textsuperscript{89} However, covered entities are not mandated to create a formal appeals process or a form of "due process."\textsuperscript{90} When violations occur, the covered entity must mitigate "to the extent practicable" any harmful effect known to result from the infraction.\textsuperscript{91}

\textsuperscript{84} For more on the impact on personal privacy from security policies, see generally Health Privacy Project, supra note 60, at 20–22.

\textsuperscript{85} Specific concerns calling for flexibility include that the nature of the health information held by covered entities may differ, smaller organizations may be burdened greatly by requirements more appropriate for larger firms, and the swift changes in technology may require a fast process to update the privacy and security policies. See Gostin, supra note 5, at 526.

\textsuperscript{86} 45 C.F.R. § 164.530(c)(2). Group health plans that provide benefits only through a health maintenance organization (HMO) or an issuer and that do not create, receive, or maintain PHI are not subject to any of the requirements under this section except documentation of their plan materials. Id. § 164.530(k). The issuers and HMOs must still follow all of the elements of the privacy and security policy mandates. See Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,563–64 (2001).

\textsuperscript{87} 45 C.F.R. § 164.530(d). Covered entities are also forbidden from taking any "intimidating or retaliatory acts" against an individual involved in the privacy policy process, including those filing a complaint. Id. § 164.530(g).

\textsuperscript{88} Id. § 164.530(e)(1).

\textsuperscript{89} Id. § 164.530(h).

\textsuperscript{90} Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,562 (2001).

\textsuperscript{91} 45 C.F.R. § 164.530(f). Balancing the protections for individuals allows flexibility for businesses. Every covered entity is not compelled to develop the same privacy and security policies. Instead, the policies must be "reasonably designed, taking into account the size of and the type of activities that relate to PHI undertaken by the covered entity." Id. § 164.530(i)(1). This generalized description of the requirement allows small businesses to develop plans that reflect the nature and size of their enterprise without burdening them more than necessary. Small businesses may still find some of the requirements overly burdensome. For example, a sole practitioner largely relying on paper medical records might be challenged by the need to prevent accidental disclosure from a misplaced record. As the health data privacy rule mandates that covered entities’ privacy policies "promptly" comply with changes in law, id. § 164.530(j)(3), further difficulties can arise for small businesses with
C. Fair Information Practices

Persons and entities maintaining PHI must adhere to a range of fair information practices that allow individuals to make informed choices about the delivery and financing of their health care. The health data privacy regulations proscribe several fair information practices for health consumers, including the right to: (1) notice; (2) access protected health information; (3) amend protected health information; and (4) request an accounting of disclosures.

Notice. Health care consumers have the right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity. Individuals are also entitled to know their legal rights, as well as the covered entity's privacy and security policies, including fair information practices requirements. The notice must be in plain language. Health plans must provide notice to covered individuals by the regulation's compliance date, while health care providers must provide this notice upon the first service delivery after the compliance date. Additionally, consumer safeguards apply to covered entities that provide notice electronically.

Access to Protected Health Information. The new regulations offer individuals a broad opportunity to access their PHI. Access rights include an on-site inspection of the records and the provision of copies of their records. Covered entities must act within thirty days upon the request for access to health data. If the individual agrees in advance, the covered entity may

limited resources to monitor legal developments and implement swift changes. See Gostin, supra note 82, at 3018.

92. 45 C.F.R. § 164.520(a)(1). For more on the necessity of providing such notice, see generally Gostin, supra note 5, at 522–24; HEALTH PRIVACY PROJECT, supra note 60, at 19–20.

93. 45 C.F.R. § 164.520(a)(1). The notice must include information about how individuals may complain about potential misuses or violations to the covered entity and the Secretary of HHS or about how to contact the covered entity with questions. Id. § 164.520(b)(vi).

94. Id. § 164.520(b)(1).

95. Id. § 164.520(c)(1)(i)(A), (c)(2)(i). New enrollees must get the notice at the time of enrollment. At least once every three years, the health plan must notify enrollees in the plan that the notice is available and the methods by which they can obtain it. Id. § 164.520(c)(1)(i), (c)(2).

96. An individual must agree to obtain the notice via e-mail. A paper copy must be provided if the covered entity knows that the e-mail transmission failed. Id. § 164.520(c)(3)(ii). Health care providers must give electronic notice automatically and simultaneously when their first service delivery is electronic. Id. § 164.520(c)(3)(iii). If a covered entity maintains a website that offers information about its benefits and services, it must also prominently post its notice on the website as well as make it available electronically. Id. § 164.520(c)(3)(i).

97. Id. § 164.524. The covered entity may require that the request be in writing. Id. § 164.524(b)(1). For more on the significance of the individual's ability to access his or her personal medical data, see Gostin, supra note 5, at 524; HEALTH PRIVACY PROJECT, supra note 60, at 18–19.

98. 45 C.F.R. § 164.524(c)(1).

99. Id. § 164.524(b)(2)(i). Sixty days is allowed if the information is held off-site. Id. § 164.524(b)(2)(ii). Delay is also allowed if the covered entity informs the individual in writing
provide a summary of the PHI instead of the actual documents.\textsuperscript{100} The standard does permit narrow, unreviewable reasons for denial regarding requests for psychotherapy notes; information likely to be used in a civil, criminal, or administrative proceeding; and requests by inmates to their correctional facility or health care provider that might threaten the health or safety of the individual or others.\textsuperscript{101} Also, in limited circumstances,\textsuperscript{102} a covered entity may deny access although the individual may request a review of the grounds for denial.\textsuperscript{103} If the covered entity decides to deny access to the individual of any part of the PHI, the health data privacy regulation ensures a fair and informed process.\textsuperscript{104}

\textit{Amend Protected Health Information.} Individuals can amend their PHI if they report inaccuracies or missing information.\textsuperscript{105} The covered entity must act within sixty days on a request to amend.\textsuperscript{106} If the covered entity agrees to the amendment, it must: (1) identify the records that are affected by the amendment; (2) append or provide a link to the amendment;\textsuperscript{107} and (3) inform the individual of the amendment.\textsuperscript{108} Additional covered entities that possess or receive the data must correctly amend their records concerning the relevant individual.\textsuperscript{109} As with access rights, covered entities

\begin{itemize}
\item[] of the reasons why it requires more time and when the request will be granted. \textit{Id.} § 164.524(b)(2)(iii)(A).
\item[] 100. \textit{Id.} § 164.524(c)(2)(ii).
\item[] 101. \textit{Id.} § 164.524(a)(1)(ii), (a)(2)(ii). Information obtained from another based on a promise of confidentiality that would likely reveal the identity of the source may be denied without review. \textit{Id.} § 164.524(a)(2)(v). Health care providers may also temporarily deny access during research based on an individual's care if the individual has consented to both the research and the denial of access during research. \textit{Id.} § 164.524(a)(2)(iii).
\item[] 102. These situations include where a licensed health care professional determines that access will endanger the life or physical safety of the individual or another person. \textit{Id.} § 164.524(a)(3)(ii).
\item[] 103. \textit{Id.} § 164.524(a)(3). This provision specifically covers determinations that references to another person will endanger that other individual, or that, if a personal representative is making the request, substantial harm will come to the individual or another person. \textit{Id.} § 164.524(a)(3)(ii).
\item[] 104. The denial must be in writing and in plain language. It must explain the reasons for the denial, any rights for review over the decision, and methods of complaint to the covered entity. \textit{Id.} § 164.524(d)(2)(j)–(iii). Access should be granted to any information that does not meet the specific grounds for denial. \textit{Id.} § 164.524(d)(1). If a review of the denial is warranted, it is conducted by a licensed health care professional who is designated by the covered entity but is not directly involved in the decision to deny access. \textit{Id.} § 164.524(d)(4).
\item[] 105. \textit{Id.} § 164.526(a)(1). See Gostin, \textit{supra} note 5, at 524, and \textit{Health Privacy Project, supra} note 60, at 19, for more on the significance of this right.
\item[] 106. 45 C.F.R. § 164.526(b)(2)(i). An extension of thirty days is possible if the covered entity explains the reasons for delay and the date on which it will respond to the request in writing to the individual. \textit{Id.} § 164.526(b)(2)(ii).
\item[] 107. \textit{Id.} § 164.526(c)(1).
\item[] 108. \textit{Id.} § 164.526(c)(2), (3)(i). It must also notify persons or entities identified by the individual as needing the amended information, or (2) known by the covered entity to have PHI about the individual and who may rely on the information to the detriment of the individual. \textit{Id.}
\item[] 109. \textit{Id.} § 164.526(e).
\end{itemize}
may deny amendments in certain circumstances, including upon a determination that the record is "accurate and complete." The entity must then give written notice to the individual. Yet, unlike disputes over access denial, there is no final review to clarify which party, the individual or the covered entity, is correct. Should the individual disagree in writing, the covered entity can respond with a written rebuttal, which must be included in future disclosures.

III. Request an Accounting of Disclosures. Patients have a limited right to receive an accounting of disclosures of their PHI (other than for disclosures related to treatment, payment, and health care operations, among other exceptions) over the six-year period prior to the request. The accounting includes the name of the person or entity that received the information (and their address if known), the date of the disclosure, a brief description of the information disclosed, and a brief explanation of the reasons for disclosure if not authorized by the patient.

D. The Effects of Preemption

Under HIPAA, HHS cannot preempt state health information privacy laws that are more protective of patients than the national rule. Some states may offer more protections through, for example, "superconfidentiality" laws for genetic, mental health, or HIV/AIDS information. Thus, because existing federal or state laws that provide more privacy protections remain, HHS's privacy regulations create a federal "floor" of protections.

This multilevel approach allows states to tailor health information pri-
privacy policies to the specific needs of their populations, but there are at least two disadvantages: (1) it allows individuals in some states to benefit from greater privacy protections than in others, and (2) where most electronic health data are exchanged across state boundaries, covered entities (specifically, larger health providers, plans, and clearinghouses) must adhere to national and regional privacy standards. This results in higher costs than would occur if a uniform national standard were in place.

IV. BALANCING INDIVIDUAL AND COMMUNAL INTERESTS IN HEALTH DATA: USES AND DISCLOSURES OF HEALTH INFORMATION

A. Disclosures of Protected Health Information

Under the national privacy regulations, individuals exercise some level of control over the use and disclosure of PHI, which ensures individual privacy protection from unlimited sharing of personal medical data. The principal question, however, is how much control individuals should exercise. Privacy protections that allow consumers to restrict the flow of their data through informed consent or advance authorization requirements may hinder the collection of comprehensive and accurate information that may benefit health consumers. 118

The regulations differentiate among the various purposes for which data may be used and disclosed. Uses and disclosures for health care-related purposes (e.g., provision or payment for health care services) are liberally permitted, albeit with the advance "informed consent" of each patient. Uses and disclosures of PHI for other purposes outside the health care context are limited. Disclosures may only be made pursuant to written authorization by the individual, subject to some exceptions. In either context, a minimum disclosure rule applies: when using or disclosing PHI, the covered entity must make reasonable efforts to limit the information to the minimum necessary to accomplish its purpose. 119 The minimum disclosure rule helps patients maintain privacy by enhancing patient autonomy and promoting their trust in the health care system (e.g., in reimbursement transactions, where only specific health information is needed). 120

119. 45 C.F.R. § 164.502(b)(1).
120. See HHS, Standards, supra note 61. HHS's recent guidance has clarified a significant concern of health care providers over the permitted uses during treatment when consulting with other physicians or medical staff. The standard as written specifies that the minimum disclosure requirement applies for use of PHI during treatment by health care providers, but not disclosures. This has caused confusion about how health care providers can utilize vital health information in the course of treatment as they work with other medical professionals. In the July 2001 guidance, HHS explained that the exemption for disclosures during treatment allows health care providers to share information with other providers.
Rules protecting the privacy of individuals are most important when the benefit to the individual is large, and the burden on the public is small. The following sections clarify that informed consent, which applies for health care-related purposes, provides little benefit to the individual at some cost to society, while written authorization, which applies for non-health care-related purposes, is a somewhat more effective means of protecting individual privacy.

1. Written Consent for Disclosure and Use for Health Care Purposes

The regulations presently require covered health care entities to obtain written consent from individuals before using or disclosing information for treatment, payment, or health care operations. Such consent must: (1) be in plain language;¹²¹ (2) inform the individual that PHI may be used and disclosed to carry out treatment, payment, or health care operations;¹²² (3) indicate that the individual can revoke the consent in writing;¹²³ and (4) include a request that the covered entity restrict how PHI is used or disclosed for health care purposes (although the covered entity is not required to agree).¹²⁴ Certain exceptions for specific disclosures are discussed below.

The written consent requirement for use and disclosure of PHI in health care activities is largely inadequate.¹²⁵ Consent under these circumstances is neither informed nor consensual. A patient may sign a consent form on his or her first visit to a physician that applies to all future disclosures and uses. In such cases, the individual will not be aware of the substance of the data protected, because the individual will typically not know what information is contained in his or her current records or what may be contained in his or her future medical records.¹²⁶ At the time of consent, the patient will also not be aware of the specific uses or disclosures because the form need only say “treatment, payment, or health care operations.” For these reasons, his or her execution of a written authorization prior to treatment is uninformed. Such authorization also lacks effective consent where the rule allows providers to condition enrollment in a plan or medical treatment on whether the individual signs the consent form.¹²⁷ As a result, the patient can be coerced into consenting if he or she wants to obtain treatment or health insurance.¹²⁸

¹²¹. 45 C.F.R. § 164.506(c).
¹²². Id. § 164.506(c)(1). The consent may not be combined in a single document with the notice. Id. § 164.506(b)(3).
¹²³. Id. § 164.506(c)(5).
¹²⁴. Id. § 164.506(c)(4)(i). If the covered entity does agree, the agreement is binding. See id. § 164.522(a)(ii) (restating the standard for an individual’s right to request restrictions of uses and disclosures and documenting the requirements for termination of the restrictions).
¹²⁵. Note that the requirement was not in the proposed rule.
¹²⁶. See Gostin, supra note 82, at 3017.
¹²⁷. 45 C.F.R. § 164.506(b)(1), (2).
¹²⁸. See HEALTH PRIVACY PROJECT, supra note 60, at 16; Pritts, supra note 75.
2. Authorization for Disclosures Not Related to Health Care

A different consent model for disclosures and uses of PHI unrelated to health care (e.g., for employment decisions or evaluation of credit status) is employed in the regulations. Prior to using or disclosing PHI for non-health care purposes, covered entities must obtain a written authorization from the individual. The authorization, unlike the written consent required for health care purposes, contains specific information to help individuals decide whether to permit disclosure or use. Such authorizations must:

(1) identify the information to be used or disclosed in a "specific and meaningful fashion";\(^{129}\) (2) provide the names of the persons or organizations who will make and receive the use or disclosures;\(^{130}\) (3) explain the purpose for each request; (4) notify the individual of his or her right to refuse to sign the authorization without negative consequences to treatment or health plan eligibility (except under specific circumstances);\(^{131}\) (5) be written in plain language;\(^{132}\) (6) include an expiration date;\(^{133}\) and (7) explain that the individual has a right to revoke the authorization\(^ {134}\) at any time in writing except regarding actions taken by the covered entity in reliance of the authorization.\(^ {135}\) Unlike the informed consent requirement for health care-related disclosures, the individual's choice is respected. The exercise of the right of refusal cannot be used to deny the patient treatment or health insurance.\(^ {136}\)

B. Making Exceptions: Balancing Communal Goods and Personal Privacy

The privacy regulations do, however, make several exceptions to the authorization provisions related to the use and disclosure of PHI. These exceptions include disclosures: (1) to law enforcement officials; (2) for judicial and administrative proceedings; (3) to parents of unemancipated minors; (4) to "significant others," such as family members, close friends, or designated persons, of an adult or an emancipated minor; (5) to authorized

\(^{129}\) 45 C.F.R. § 164.508(c)(1)(i).
\(^{130}\) Id. § 164.508(c)(1)(ii), (iii).
\(^{131}\) Id. § 164.508(e)(1)(iii).
\(^{132}\) Id. § 164.508(c)(2).
\(^{133}\) Id. § 164.508(c)(1)(iv).
\(^{134}\) Id. § 164.508(c)(1)(v).
\(^{135}\) Id. § 164.508(b)(5)(i).
\(^{136}\) Id. § 164.508(b)(4). There are some limited exceptions. One is that health care providers may condition provision of research-related treatment on authorization. Another is that if the covered entity is gathering individually identifiable health information solely for the purposes of disclosing it to a third party, such as an employer, the covered entity may condition this care on the authorization to disclose it to the third party. Further protection is offered regarding psychotherapy notes; authorization is always required for use and disclosure of psychotherapy notes except in specified health care operations. Id. § 164.508(b)(5)(i)–(iv).
public health authorities; (6) for health research; and (7) for commercial marketing purposes.

**Law Enforcement.** A covered entity may disclose PHI to a law enforcement official without informed consent pursuant to a court order, subpoena, or administrative request, including a civil investigative demand or an administrative subpoena. Judges are given no criteria from which to make their determination as they balance individual privacy and law enforcement. In addition, a covered entity may disclose limited information without prior judicial approval where: (1) the information relates to a crime victim who is incapacitated and disclosure is necessary and in the best interests of the individual; (2) PHI is evidence of criminal conduct that occurred on the premises of the covered entity; and (3) in the course of an emergency, disclosure is necessary to alert law enforcement officials of the location, commission, and nature of the crime, victims, or perpetrators.

**Judicial and Administrative Proceedings.** PHI may be disclosed at any judicial or administrative proceeding without the person's permission in response to a court order or administrative tribunal. As in the law enforcement context, judges are given no criteria in the regulation to exercise their discretion. Covered entities may also disclose health information in response to a subpoena or discovery request if the requester (1) reasonably attempts to inform the patient of the disclosure, or (2) reasonably at-
tempts to obtain a protective order to prohibit the recipients from using or disclosing the information for purposes other than the litigation.\(^{144}\) Instead of placing the burden on litigants seeking the information, the regulation requires that patients make objections to the court.

**Minors.** Disclosures to parents of unemancipated minors are exempted from consent requirements in multiple cases. If state law forbids or requires that parents be informed about their children's health conditions, the regulation allows state law to stand.\(^{145}\) While many states permit competent minors to receive medical treatment for potentially stigmatizing conditions without parental consent,\(^{146}\) states could pass laws requiring parents to be informed about their child's condition and treatment. Where no state law exists, the regulation allows parents to serve as personal representatives,\(^{147}\) who generally can act on behalf of the individual,\(^{148}\) with some restrictions.\(^{149}\) The Bush administration has suggested that it may modify the rule to increase parental access.\(^{150}\)

"**Significant Others** of Adults and Emancipated Minors.** Disclosures to "significant others" (i.e., family, friends, caretakers, or health care surrogates) of adults and emancipated minors are narrowly exempted. Covered entities may disclose limited health information to "significant others" without consent if the patient is informed in advance and has the opportunity to agree.\(^{151}\) The disclosed PHI must be (1) directly relevant to the person's involvement with the patient's care or payment for care,\(^{152}\) or (2) used to notify that person of the patient's location, general health condition, or

---

144. *Id.* § 164.512(e)(1)(ii)(B). The party requesting information must give the covered entity satisfactory assurances that the parties have agreed to a qualified protective order or that the requester has asked for a qualified protective order. *Id.* § 164.512(e)(1)(iv). The standard defines qualified protective order as one that prohibits the parties from using or disclosing PHI for any purpose other than litigation or proceeding for which the information was requested and requires the PHI's return to the covered entity or destruction at the end of the proceeding. *Id.* § 164.512(e)(1)(v)(A).

145. *Id.* § 160.202 (defining "more stringent").

146. See Gostin, *supra* note 82, at 3017.

147. 45 C.F.R. § 164.502(g)(1).

148. *Id.* § 164.502(g)(2).

149. If the minor consents to the health care service, the parent agrees to confidentiality between the provider and the minor, or the minor consents and does not wish the parent to be the personal representative, then the parent is not considered a personal representative. *Id.* § 164.502(g)(3).

150. Thompson Press Release, *supra* note 2, ¶ 10. ("[W]e will make it clear through guidelines or recommended modifications that . . . parents will have access to information about the health and well-being of their children, including information about mental health, substance abuse or abortion."). The July 2001 guidance indicated that the Secretary is still considering such action. See HHS, *Standards, supra* note 62 (indicating that Secretary Thompson is still considering actions to increase parental access).

151. 45 C.F.R. § 164.510(b)(1), (2). Disclosure is also permitted if the covered entity can reasonably infer from the circumstances that the patient does not object to disclosure. *Id.* § 164.510(b)(2)(iii).

152. *Id.* § 164.510(b)(1)(i).
death. In cases of incapacitation or emergency, disclosures to “significant others” may be made in the patient’s best interest when directly relevant to the entities’ involvement with the individual’s care.

**Public Health.** The health data privacy rule broadly exempts disclosures of PHI for routine public health activities. This includes disclosures: (1) where federal or state law authorizes public health authorities to collect PHI to prevent or control disease, injury, or disability, or to report child abuse or neglect; (2) to notify persons who may be at risk for or exposed to a communicable disease (e.g., partner notification provisions); and (3) concerning adverse events, tracks and recalls of products, and post-marketing surveillance by persons subject to the jurisdiction of the Food and Drug Administration. State reporting or other public health laws are not preempted by the rule even if they offer less privacy protections, thus leaving public health information privacy law to the states.

**Health Research.** Most federally funded human subject research is currently subject to federal regulations known as the Common Rule, which does not contain detailed privacy standards, but rather conditions IRB approval of research on whether “there are adequate provisions to protect the privacy of subjects.” Although the Common Rule is a helpful guide for protecting the privacy and other ethical interests of human research subjects, it does not apply to privately funded research. The health data privacy rule closes this gap between the public and private sectors by providing more detailed requirements than the Common Rule. A covered entity may only use or disclose PHI for research without the person’s permission if it obtains a waiver from an IRB or privacy board that finds

153. Id. § 164.510(b)(1)(ii).
154. Id. § 164.510(b)(3). The rule allows relatives and close personal friends to perform common care-taking duties such as picking up prescriptions, medical supplies, etc. Id.
155. Id. § 164.514(b)(2) (clarifying that all of the exceptions apply to uses of PHI as well as disclosures in the public health exemptions section).
156. See Gostin, supra note 82, at 3016.
157. Public health authority is expansively defined as a federal, tribal, state, or local agency, or a person or entity with a grant of authority or contract with the agency. 45 C.F.R. § 164.501 (defining “public health authority”).
158. Id. § 164.512(b)(1)(iv).
159. Id. § 164.512(b)(1)(ii)(A)–(D).
160. See id. § 160.203.
162. 45 C.F.R. § 46.111(a)(7). In the Common Rule, if consent is required, the researcher must provide the subject with “[a] statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained.” Id. § 46.116(a)(5). The Common Rule also applies to research conducted in anticipation of Food and Drug Administration approval.
163. See id. § 164.512(b)(1)(i). The privacy board must have members with varying backgrounds, appropriate professional competency, and no conflict of interest. Id. § 164.512(j)(1)(i)(B). At least one member must be unaffiliated with the covered entity and
that: (1) the use or disclosure involves no more than minimal risk; (2) the waiver will not adversely affect the privacy rights and welfare of the individual; (3) the research could not practicably be conducted without the waiver; (4) the privacy risks are reasonable in relation to the anticipated benefits to the individual, and in relation to the importance of the research; (5) a plan exists to protect the identifiable information from improper use and disclosure; (6) a plan to destroy the identifiers exists unless there is a health or research justification for retaining them; and (7) there are written assurances that the data will not be reused or disclosed to others, except for research that would also qualify for a waiver. Researchers must also show that PHI is necessary for the research, will not be disclosed to outsiders, and is sought solely to prepare for the research. While certain critics are concerned over the burdens imposed by the new requirements, the regulation fairly ensures that there are valid justifications for utilizing PHI for research without consent.

Commercial Marketing: In contrast to some of the other exceptions, which offer either greater or similar protections than the law currently provides, the exception for commercial marketing provides for less privacy protection by condoning the use or disclosure of PHI for commercial marketing without consent. PHI may be used or disclosed without consent for marketing communications to the individual that occur in face-to-face encounters (whether health related or not), concern products or services of nominal value, or concern health-related products and services of the covered entity or a third party. A covered entity may target persons based on their health status if the product or service may benefit them. However, commercial communications must identify the covered entity, disclose whether the entity is receiving remuneration for the communication or sale, and instruct individuals on how they can opt out of receiving future communications. If a covered entity targets persons based on their health

---

164. Id. § 164.512(i)(2)(ii)(A)-(H).
166. See, e.g., Barnes & Krauss, supra note 165, at 1031 (arguing that IRBs are ill-prepared to make the assessments now required of them by the health data privacy regulation); Jocelyn Kaiser, Researchers Say Rules Are Too Restrictive, 294 Science 2070 (2001); J. Kulynych & D. Korn, The Effect of the New Federal Medical-Privacy Rule on Research, 346 New Eng. J. Med. 201 (2002).
168. See id. ¶ 7.
170. Id. § 164.514(e)(3)(ii)(A).
status, it must predetermine whether the product or service may benefit those persons and indicate why they have been selected. 171

V. CONCLUSION

The systematic electronic collection, use, and disclosure of individually identifiable health information are essential to achieving several important communal goals. Public health authorities and health researchers require health data to perform accurate, beneficial studies, and shape effective interventions and treatments. The exchange of electronic data can improve clinical outcomes, prevent fraud and abuse, and help consumers make informed choices about their health care. With these benefits, however, come significant threats to individual privacy and civil liberties, including discrimination and autonomy violations from unwarranted disclosures to health insurers, employers, and governmental agencies.

Through its health information privacy rule, HHS seeks to provide a national standard that balances individual interests in health information privacy with society’s interests in accomplishing various communal goals. The rule provides expansive, new protections for health data privacy and security. In many ways, it improves existing privacy protections by creating an equitable, even field in which information can be responsibly exchanged. At the same time, the rule fails to provide a sufficient floor of protection for the use and disclosure of all health information. Limited by congressional authorization under HIPAA, HHS at times trades personal privacy for public (e.g., public health exception) and nonpublic goods (e.g., commercial marketing exception). Reaching a final balance between individual and communal uses of health data may require additional authorization from Congress, or, alternatively, new federal legislation. For now, the regulation represents a new standard in an age of increasing threats to individual interests in protecting the privacy of their health data.

171. Id. § 164.514(e)(3)(ii)(A)-(B)