# National Health Information Privacy

## Regulations Under the Health Insurance Portability and Accountability Act

Lawrence O. Gostin, JD, LLD

**Health information privacy is important in US society, but existing federal and state law does not offer adequate protection. The Department of Health and Human Services, under powers granted by the Health Insurance Portability and Accountability Act of 1996, recently issued a final rule providing systematic, nationwide health information privacy protection. The rule is extensive in its scope, applying to health plans, health care clearinghouses, and health care providers (hospitals, clinics, and health departments) who conduct financial transactions electronically ("covered entities"). The rule applies to personally identifiable information in any form, whether communicated electronically, on paper, or orally. The rule does not preempt state law that affords more stringent privacy protection; thus, the health care industry will have to comply with multiple layers of federal and state law. The rule affords patients rights to education about privacy safeguards, access to their medical records, and a process for correction of records. It also requires the patient's permission for disclosures of personal information.**

**While privacy is an important value, it may conflict with public responsibilities to use data for social goods. The rule has special provisions for disclosure of health information for research, public health, law enforcement, and commercial marketing. The privacy debate will continue in Congress and within the president's administration. The primary focus will be on the costs and burdens on health care providers, the ability of health care professionals to use and share full medical information when treating patients, the provision of patient care in a timely and efficient manner, and parents' access to information about the health of their children.**

*JAMA. 2001;285:3015-3021* www.jama.com

HEALTH INFORMATION PRIVACY HAS FUNDAMENTAL importance in US society. Public opinion surveys suggest that people feel a loss of privacy, with more than 80% of consumers saying they had "lost all control over their personal information."[1] Medical records contain intimate information about a person's physical and mental health, behaviors, and relationships. Intrusions into privacy can result in loss of trust, with an unwillingness to confide in health care professionals. Unauthorized disclosures of intimate information can cause embarrassment, stigma, and discrimination.

Public concern about erosion of privacy reflects marked changes in the health care system. First, there has been a transition from written to electronic records for many medical and financial transactions.[2,3] Computerization makes it efficient to acquire, manipulate, and disseminate vast amounts of information. Second, systematic flows of highly sensitive data are evident in the daily operation of employer-sponsored health plans, managed care organizations, hospitals, pharmacies, and laboratories. These data are used for numerous health-related purposes including clinical care, quality assurance, utilization review, reimbursement, research, and public health. The data are also used for many nonhealth-related purposes such as commercial marketing, litigation, and law enforcement.[4] Finally, advances in genetic sciences make it possible to reveal intimate details of patients and their families.[5] In the future, physicians likely will include more genetic data in medical records and investigators will increasingly use stored tissue samples for genetic research.[6]

The legal system has not adapted well to these changes in the health care system. Federal law contains few safeguards of health information privacy. The Privacy Act of 1974 protects only "systems of federal records," such as Medicare and Veterans Affairs data, but does not apply to the private sector.[7] Special protections are applicable to certain alcohol and drug treatment records,[8] research that qualifies for a certificate of confidentiality,[9,10] or research funded by the Agency for Healthcare Research and Quality.[11]

A large body of state and local medical privacy law exists, but the Department of Health and Human Services (HHS)[12] and independent scholars[13,14] characterize those safeguards as inadequate and highly variable. Often these laws apply specifically to state government records, not to privately held records. The strongest protection of privacy is often directed to specific areas of concern such as human immunodeficiency virus (HIV), mental illness, or genetics.

**Author Affiliation:** Center for Law and the Public's Health at Georgetown University Law Center, Washington, DC, and Johns Hopkins School of Public Health, Baltimore, Md.
**Corresponding Author and Reprints:** Lawrence O. Gostin, JD, LLD, Georgetown University Law Center, 600 New Jersey Ave NW, Washington, DC 20001-2075 (e-mail: gostin@law.georgetown.edu).
**Health Law and Ethics Section Editors:** Lawrence O. Gostin, JD, LLD, Center for Law and the Public's Health at Georgetown University Law Center, Washington, DC, and Baltimore, Md; Helene M. Cole, MD, Contributing Editor, *JAMA*.

Congress recognized the need for national health information privacy standards when it enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[15] Congress created a self-imposed deadline of August 21, 1999, to enact comprehensive health information privacy legislation under this act,[15] which required the secretary of HHS to promulgate privacy regulations if Congress failed to act by the deadline. Following the principles and policies laid out for privacy protection in 1997,[16] the secretary issued a proposed rule in November 1999.[17] The Department of HHS received more than 52 000 public comments on the proposed rule and the secretary issued a final rule late in President Clinton's term of office.[18] The Bush administration reopened the comment period[19] and received more than 24 000 additional comments.[20] President Bush set April 14, 2001, as the "effective date" for the rule, beginning a phase-in period requiring full compliance by April 14, 2003; small health plans must comply by April 14, 2004.[21]

The rule provides the first systematic nationwide privacy protection for health information. The HHS secretary has authority to investigate complaints and conduct compliance reviews.[22] Violations of the rule can result in civil and criminal penalties up to a $250 000 fine and 10 years in prison; however, HHS lacks statutory authority to grant a private right of action for patients to redress violations of privacy in the courts.

## Scope of the National Privacy Rule

The rule reaches virtually all those who use medical and financial information in the health care system, creating a national standard of privacy protection. Specifically, the rule applies to "covered entities," including[23]: (1) health plans, which provide or pay for the cost of medical care in the private (eg, health insurer or managed care organization) or public (eg, Medicaid, Medicare, or Veterans Affairs) sector; (2) health care clearinghouses, which process health information (eg, billing service); and (3) health care providers who conduct certain financial and administrative transactions (eg, billing and fund transfers) electronically. The rule even applies to sole practitioners who generate bills electronically.

The Health Insurance Portability and Accountability Act does not authorize HHS to regulate other entities that routinely handle sensitive medical information, such as life insurers and worker's compensation programs. Similarly, HIPAA does not authorize HHS directly to regulate the use and redisclosure of health information by the business associates of health care providers, such as lawyers, accountants, billing companies, and other contractors. Instead, the rule imposes a duty on covered entities to obtain satisfactory assurances that business associates will comply with privacy standards.[24] If the covered entity knows of a violation and takes no steps to correct it, that entity can be held responsible for violation of the rules.

It may be unfair to hold the health care industry accountable for privacy violations committed by its business associates. Ideally, health privacy law should regulate directly all those who receive health information, including agents and contractors. However, HHS had no other way to ensure that downstream users and processors respect consumer privacy.[25]

The rule applies only to personally identifiable information. The rule specifies 2 ways that a covered entity can determine that health information is nonidentifiable[26]: (1) if an expert applying scientific and statistical principles finds "that the risk is very small that the information could be used, alone or in combination with other reasonably available data, to identify an individual"; or (2) if the entity deletes from the record a list of identifiers such as name, geographic designators, dates, telephone and fax numbers, and Social Security numbers (the "safe harbor").[26]

The rule applies to identifiable information in any form, whether communicated electronically, on paper, or orally. For example, statements made over the telephone in the physician's office are covered, regardless of whether the data are recorded in the patient's record. The rule's coverage of nonelectronic records is controversial because HIPAA does not provide unambiguous authority to regulate written and oral communications. However, protecting health information only in electronic format would leave vast amounts of health communications unprotected by federal law. Further, limiting coverage to only data that at some point had been electronically maintained would be difficult to enforce.[27]

## The Right to Notice of Privacy Practices and Consumer Access to Medical Records

The rule affords patients the right to adequate notice of privacy and information practices. Providers and health plans must give patients a clear written explanation of allowable uses and disclosures of protected health information and patients' rights.[28] Adequate notice of privacy practices can build trust, enabling patients to feel informed about future data uses. Although not required under the rule, plans and providers should issue notices in "plain language," stating the expected uses that will be made of patient data.

The rule empowers patients to request confidential communications (eg, not by post or voice mail).[29] This right protects patients who do not want to alert household members of sensitive health problems, such as sexually transmitted diseases (STDs), substance abuse, and domestic violence.

Covered entities may disclose personal information to the individual and must do so when requested.[30] Patients have a right to inspect and obtain a copy of their records except for data compiled in reasonable anticipation of civil, criminal, or administrative proceedings, or if access is reasonably likely to endanger the life or safety of the person or others.[31] Patients also have a right to request amendments of the record; a covered entity may deny a request if it determines that the information in dispute is accurate and complete.[32] Finally, patients have a right to receive a history of disclosures, except to carry out treatment, payment, and

health care operations and for certain other purposes (eg, national security or intelligence).[33]

These provisions implement "fair information practices" adopted in federal[34] and state[35] privacy laws. Principles of fairness suggest that patients should have the right to notification of data uses, request confidential communications, gain access to personal data, request corrections of inaccurate or incomplete data, and understand to whom their data have been disclosed. The new standards suggest that health care institutions do not have exclusive control over medical records, but must give patients an opportunity to ensure their accuracy and monitor their use.

### Rights of Minors

The individual who is the subject of the protected health information is empowered to exercise all rights afforded under the rule, including the right of access to medical information. The rule also allows a personal representative to act on behalf of the individual in certain circumstances. The rule specifies that parents can be recognized as personal representatives of unemancipated minors.[36] The rule, however, generally does not permit parents to have access to health information if, under state law, the minor may lawfully consent to treatment. Several states permit competent minors to obtain medical treatment (eg, for STDs, contraception, abortion, or mental illness) without the parents' permission. The rule, moreover, provides that state laws that authorize or prohibit disclosures of information to parents are not preempted.

The right of parents to have access to health information concerning their children is politically charged. Parents have responsibility for their children's best interests and need to have access to health information to make informed judgments. Patient-physician confidentiality is equally important. If minors feel that their communications with physicians are not confidential, they may forgo diagnosis and treatment for sensitive health conditions. The rule currently defers to state law and policy judgments, but HHS Secretary Thompson stated that in subsequent guidelines or modifications "parents will have access to information about the health and well-being of their children, including information about mental health, substance abuse, or abortion."[20]

### Written Consent: Disclosure for Treatment, Payment, or Health Care Operations

Health care providers must obtain the individual's written consent prior to disclosure of health information for the "routine" uses of treatment, payment, or health care operations (eg, internal data gathering for quality assurance or utilization review).[37] There are certain exceptions, such as for treatment emergencies or if consent can be inferred from a patient who has difficulty communicating. The consent requirement for routine health-related purposes was not in the proposed rule. Written consent is controversial because it does not provide meaningful safeguards for patients, increases health care costs, and interferes with pharmacy practices.[38]

The consent model, as drafted, affords a safeguard in form, not substance. The patient could sign 1 consent form, in the first visit to a physician, authorizing all future disclosures for such purposes. The consent is not "informed" because most patients will be unaware of the contents of the record at the time they sign the form and, even if they are aware, the record will change over time. Nor will patients have a clear idea of the numerous uses that will be made of their records. The consent also is not truly voluntary because the rule specifically permits the provider to condition treatment, and the health plan to condition enrollment, on the signing of the consent.[39] Although the individual has the right to request restrictions on data uses, the covered entity is not obliged to agree to the request.[40] Thus, if patients desire treatment or reimbursement, they have no choice but to authorize disclosure.

Written consent also imposes significant costs and burdens on the health care industry. Providers will have pro forma obligations to obtain, and store, consent forms from every patient. Health care providers are also concerned that medical services may be delayed if consent forms have not been signed or cannot be located.[38]

Finally, written consents may interfere with pharmacy practices. A significant number of prescriptions are telephoned or faxed to pharmacists by physicians. The pharmacist then uses this information to dispense the prescription to the patient or person acting on his/her behalf. Requiring a written consent to be on file in advance may harm the patient-pharmacist relationship.

### Authorization: Disclosure for Purposes Not Related to Health Care

Covered entities may not use or disclose health information for purposes unrelated to health care (eg, employment, insurance, or mortgage eligibility) without explicit patient authorization. The rule has detailed standards for authorization for nonroutine uses or disclosures[41]: the authorization must contain a "specific and meaningful" description of the information and the name of the person or class of persons authorized to make the disclosure or use the information.

The authorization model for nonroutine uses of health information offers a valuable safeguard. It is informed because the covered entity must apprise the patient of the specific use to be made of the data. It is also voluntary because covered entities generally cannot condition treatment, payment, enrollment, or eligibility on a patient's agreement to disclose health information for nonroutine purposes.[42] The authorization rule addresses significant privacy problems in the health care system. Employer-sponsored health plans often gain access to health information about employees and can make adverse personnel decisions based on those data.[43]

Similarly, if personal data are disclosed to insurers, landlords, lenders, family, or friends, stigma and discrimination can result.

### Opportunity to Agree or Object: Relatives and Friends Involved in the Person's Care

Covered entities may disclose limited health information to a relative, personal friend, or designated person without written consent or authorization provided the patient is informed in advance and has the opportunity to agree to or prohibit the disclosure.[44] A covered entity may disclose only health information (1) directly relevant to the person's involvement with the patient's care or payment for care; or (2) to notify that person of the patient's location, general health condition, or death. Additionally, the rule permits disclosures if the patient is not present, is incapacitated, or in an emergency if the entity reasonably believes it is in the patient's best interests. In such cases, the entity may disclose only information directly relevant to the person's involvement in health care.

As discussed earlier, health care providers express concern that the rule will interfere with standard practices of sharing information for the patient's benefit. Many patients (particularly those who are sick, elderly, or in rural areas) rely on their family, friends, and caregivers to collect prescriptions, medical supplies, and test results. The rule, as written, appears to allow these practices to continue, but HHS will issue guidelines ensuring that patient care will not be hampered.

### The Minimum Disclosure Standard

Covered entities must limit health information disclosure to the minimum necessary to achieve the purposes of the use or disclosure.[45] The minimum disclosure standard is justified for many disclosure purposes, such as reimbursement. However, minimum disclosure could be harmful if health care professionals did not have full information for patient care. Confusingly, the minimum disclosure standard applies to information *used* for treatment, but not to information *disclosed* for treatment. Consequently, the rule may have the unintended effect of restricting full communication among teams of health care professionals in the course of treating patients. Future guidance should make clear that health care professionals should always have the complete medical record when treating and caring for patients.

### Privacy and Security Policies

Covered entities have detailed responsibilities for privacy and security and must[46] (1) designate a privacy official responsible for policies and procedures; (2) train members of the workforce; (3) adopt written procedures describing who has access to information, how it will be used, and the circumstances in which it will be disclosed; (4) ensure that business associates protect privacy; and (5) accept inquires or complaints from patients.

The rule gives the health care industry flexibility in devising policies and procedures, but ensures that covered entities have adequate plans and procedures in place to safeguard privacy and security. These privacy and security responsibilities, while important, may be burdensome for small businesses.

Notably, health plans must only accept complaints, but do not have to act on them or establish any particular grievance process. This leaves patients without an effective remedy at the plan level.

### Balancing Public Responsibility With Personal Privacy

Privacy, of course, is not the only important value in health policy. Health information can be used to accomplish many public goods.[47] Consequently, the rule permits disclosures of health information without individual consent, authorization, or the opportunity to agree or object under specified guidelines for national defense and security, prevention of abuse and neglect, identification of deceased persons or causes of death, judicial and administrative procedures, prevention of serious threats to health or safety, and oversight of the health care system (eg, inspections, disciplinary actions, and audits). The following discussion examines the tradeoffs between individual interests in privacy and social interests in particularly controversial areas, such as research, public health, law enforcement, and commercial marketing.

**Research.** All research should be subject to rigorous scientific and ethical review, which would build public trust. At present, federal regulations, known as the Common Rule,[48] apply only to federally funded studies and research conducted in anticipation of US Food and Drug Administration (FDA) approval, leaving most private research unregulated. The Common Rule requires institutional review board (IRB) approval but does not enunciate detailed privacy standards. Instead, a condition for IRB approval is that "when appropriate, there are adequate provisions to protect the privacy of subjects."[49] Furthermore, if consent is required, the investigator must provide the subject with "[a] statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained."[50]

The HIPAA rule is limited to safeguarding health information privacy and does not extend more broadly to human subjects research. Nevertheless, it closes gaps in privacy protection for records-based research. A covered entity may use or disclose protected health information for research without the person's permission, provided that it obtains a waiver from an IRB or privacy board.[51] Privacy boards must have members with varying backgrounds and appropriate competencies, including at least 1 member who is not affiliated with the covered entity or the research sponsor or investigator. The waiver criteria include findings that (1) the use or disclosure involves no more than minimal risk; (2) the research could not practicably be conducted without the waiver; (3) the privacy risks are reasonable in

relation to the anticipated benefits, if any, to individuals and the importance of the research; (4) a plan to destroy the identifiers exists unless there is a health or research justification for retaining them; and (5) there are written assurances that the data will not be reused or disclosed to others, except for research oversight or additional research that would also qualify for a waiver.

The waiver criteria seek a compromise between research and privacy interests.[52] Health services researchers, for example, often undertake statistical analyses of large databases obtained from varied sources. A requirement to obtain prior consent for tens of thousands of patients could be burdensome and result in biased samples due to self-selection.[53] Nevertheless, investigators should have to demonstrate that the research is scientifically rigorous and socially important, consent would be disproportionately costly or undermine the study design, and the research will not pose more than minimal privacy or other social risks. Additionally, members of IRBs and privacy boards should receive adequate training and resources to manage increasingly complex problems in human subjects research.

**Public Health.** A covered entity may disclose protected health information for the following public health activities without the person's permission[54]: (1) a public health authority authorized by law to collect information to prevent or control disease, injury, or disability (eg, reporting, surveillance, public health investigations, and public health interventions); (2) a public health authority or other agency authorized by law to receive reports of child abuse or neglect; (3) a person subject to the jurisdiction of the FDA to report adverse events, track and recall products, and conduct postmarketing surveillance; (4) a covered entity or public health agency authorized by law to notify persons who may have been exposed to, or may be at risk of, a communicable disease; and (5) an employer to conduct medical surveillance in the workplace, provided the person is notified.

A public health authority is defined widely as a federal, tribal, state, or local agency, or a person or entity acting under a grant of authority or contract with the agency.[55] The rule permits public health authorities to engage in routine reporting, surveillance, program evaluations, outbreak investigations, partner notification, and interventions without complying with federal privacy rules. Indeed, the rule expressly does not preempt state law for public health reporting, surveillance, investigation, or intervention.[56]

Government collection of sensitive health information (eg, named HIV reporting) raises privacy concerns. Yet, the rule leaves public health information unprotected, unless there are strong state laws. Scholarly reviews demonstrate that state privacy safeguards are often weak and fragmented.[13,14] Consequently, HHS funded the Public Health Information Privacy Project at Georgetown University Law Center[57,58] and urged states to consider adoption of a model law.[59] If the states do not enact strong legislation, the public will not have adequate protection of public health data.

**Law Enforcement.** A covered entity may disclose protected health information to a law enforcement official without the person's permission pursuant to a court order, subpoena, or some other legal order, such as a civil investigative demand or an administrative subpoena issued by government investigators.[60] Additionally, a covered entity may disclose limited information (eg, identification, type of injury, and time of treatment) in response to a law enforcement official's request for the purpose of identifying or locating a suspect, fugitive, witness, or missing person.

The disclosure of sensitive health information to law enforcement officials may weaken public trust in the health care system. The rule does not specify strong privacy standards for courts to apply when considering disclosure requests. Law enforcement officers, moreover, can gain access to medical records without a legal process, such as a warrant or court order issued by a neutral magistrate.

**Commercial Marketing.** A covered entity may use or disclose protected health information without the person's permission for marketing communications to that individual that occur in face-to-face encounters or concern products or services of nominal value.[61] Additionally, a covered entity may market health-related products and services of the covered entity or a third party if the communication identifies the covered entity as the party making the communication, discloses the fact that the covered entity is receiving remuneration, and contains instructions on how individuals may opt out of receiving future communications. If the covered entity targets persons based on their health status, it must first determine if the product or service will be beneficial and state why the individual has been targeted.

The preamble to the rule makes clear the broad powers given to the health care industry to use personally identifiable information for marketing: "The covered entity can engage in health-related marketing on behalf of a third party, presumably for a fee. Moreover, the covered entity could retain another party, through a business associate relationship, to conduct the actual health-related marketing, such as mailings or telemarketing, under the covered entity's name."[62]

The rule allows numerous covered entities to use or sell lists of patients without advance consent. The authority to market in a face-to-face encounter or for items of nominal value can involve products or services unrelated to health (eg, magazines, life insurance, or vacations). The face-to-face encounter does not necessarily have to involve a health care professional. For example, the provider's business associates could solicit patients at their homes. Further, the product or service of nominal value may involve a coupon for a low-priced product.

The conditions for marketing of health-related products and services offer limited protections. The communication must identify the covered entity as the party making the communication and prominently disclose whether the covered

entity is being paid. However, the covered entity may still endorse the product using its credibility as a provider. The covered entity also must determine that the product is beneficial and explain why the person has been targeted. Yet, the rule does not state who must make the determination of beneficial effects (eg, physician or administrator) or the standard of evidence (eg, a single study). The requirement to explain why the person has been targeted may prove upsetting because people may not want to be singled out for marketing based on their health status.

The provision allowing patients to opt out of receiving future marketing of health-related products is an important safeguard but is deficient in several respects. First, an opt out is not required for newsletters or general communications distributed to a broad cross-section of individuals. Second, patients have the burden of opting out. A more protective scheme would be to require patients to opt in if they wished to receive marketing communications. Third, patients may not opt out in advance, but only after receiving marketing communications. Fourth, covered entities are not obliged to provide toll-free telephone numbers, postpaid cards, or Web sites for opt outs. Finally, patients may have to opt out separately for all the health care entities to which they are associated (eg, health plans, providers, pharmacies, benefit managers, laboratories, and clinics).

### Preservation of Strong State Privacy Laws: The Preemption Debate

The Health Insurance Portability and Accountability Act does not permit HHS to preempt state health information privacy laws that have more stringent standards than those in the rule. Consequently, stronger state laws are preserved under the rule.[63] Federal and state privacy protections are cumulative; HHS sets a national "floor" of privacy safeguards, but permits states to provide additional protection. The failure to preempt state law has a dual effect. It allows consumers to take advantage of stronger privacy safeguards at the state level. For example, many states require "superconfidentiality" for HIV/AIDS, mental health, or genetic data. At the same time, it renders the health care industry liable for compliance with rules nationally as well as in each state and territory. The absence of uniformity means that entities that operate nationally or regionally have to comply with a myriad of different privacy standards, increasing costs and providing disincentives for electronic transfers of data across state lines.

### The Future of Health Information Privacy

Health information privacy has sparked intense political debate in Congress and the presidential administration involving 2 strongly held perspectives. Privacy advocates seek patient autonomy over personal information, including access to medical information and control over use and disclosure. On the other hand, the health care industry seeks less burdensome and costly procedures and freedom to use information for treatment, payment, research, and other health-related purposes. Department of HHS Secretary Thompson announced that he will issue guidelines for, and/or modifications of, the rule.[20] The secretary is authorized to modify the privacy standards during the first 12 months from the rule's effective date if "necessary . . . to permit compliance with the standard."[64]

The ongoing, and divisive, political debate will focus on a number of contentious areas. Should health care professionals be permitted to freely use, and share, full medical information with the health care team and specialists when treating patients? Should parents have access to medical information about their children? Do the written consent standards impose undue burdens on the health care industry? Will pharmacists be able to fill prescriptions with telephone authorization and serve their customers in a timely manner? Should the health care industry have to comply with nonuniform standards at the national and state level? But beyond these legitimate concerns lies the important reality that the United States has adopted the first national health information privacy standard in its history. Ensuring health information privacy is vital to respect the dignity of consumers and maintain trust in the health care system.


**REFERENCES**

**1.** Harris Equifax. Health information privacy. Available at: http://www.epic.org/privacy/medical/polls.html. Accessibility verified May 1, 2001.
**2.** Lowrance WW. *Privacy and Health Research: A Report to the US Secretary of Health and Human Services.* Washington, DC: Dept of Health and Human Services; 1997.
**3.** National Research Council. *For the Record: Protecting Electronic Health Information.* Washington, DC: National Academy Press; 1997.
**4.** Gostin LO. Personal privacy in the health care system: employer-sponsored insurance, managed care, and integrated delivery systems. *Kennedy Inst Ethics J.* 1997;7:361-376.
**5.** Botkin JR. Protecting the privacy of family members in survey and pedigree research. *JAMA.* 2001;285:207-211.
**6.** Gostin LO, Hodge JG. Genetics privacy and the law: an end to genetics exceptionalism. *Jurimetrics J.* 1998;40:21-58.
**7.** Privacy Act of 1974, 5 USC §552(a)(b) (1988).
**8.** 42 USC §290(dd)(2) (Supp V 1993).
**9.** Public Health Service Act §301(d), 42 USC §241(d) (amended 1988).
**10.** Office for Human Research Protections. *Privacy Protection for Research Subjects: Certificates of Confidentiality.* Washington, DC: Dept of Health and Human Services; 1978.
**11.** 42 USC §299(c)(3) (amended 1999).
**12.** Workgroup for Electronic Data Interchange. *Obstacles to EDI in the Current Health Care Infrastructure.* Washington, DC: Dept of Health and Human Services; 1992.
**13.** Gostin LO, Lazzarini Z, Neslund VS, Osterholm MT. The public health information infrastructure: a national review of the law on health information privacy. *JAMA.* 1996;275:1921-1927.
**14.** Institute for Health Care Research and Policy. *The State of Health Privacy: An Uneven Terrain.* Washington, DC: Georgetown University; 1999. Available at: http://www.healthprivacy.org. Accessibility verified May 2, 2001.
**15.** Health Insurance Portability and Accountability Act of 1996, 18 USC §264 (West 1994).
**16.** *Confidentiality of Individually Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996.* Washington, DC: Dept of Health and Human Services; 1997.
**17.** Proposed Standards for Privacy of Individually Identifiable Health Information, 64 *Federal Register* 59918 (November 3, 1999).
**18.** Department of Health and Human Services. Standards for Privacy of Individually Identifiable Health Information: Final Rule, 45 CFR §160-164.
**19.** 64 *Federal Register* 12738 (February 28, 2001).

**20.** The Department of Health and Human Services. *Statement by HHS Secretary Tommy G. Thompson Regarding the Patient Privacy Rule.* Washington, DC: April 12, 2001.
**21.** 64 *Federal Register* 12434 (February 26, 2001).
**22.** 45 CFR §160.300-160.312 (2001).
**23.** 45 CFR §164.104 (2001).
**24.** 45 CFR §164.502(e) (2001).
**25.** The White House. *President Clinton Issues Strong New Consumer Protections to Ensure the Privacy of Medical Records*. Washington, DC: December 20, 2000.
**26.** 45 CFR §164.514 (2001).
**27.** Health Privacy Project. *Comments on Final Standards for Privacy of Individually Identifiable Health Information.* Washington, DC: Georgetown University; 2001.
**28.** 45 CFR §164.520 (2001).
**29.** 45 CFR §164.522 (2001).
**30.** 45 CFR §164.502 (2001).
**31.** 45 CFR §164.524 (2001).
**32.** 45 CFR §164.526 (2001).
**33.** 45 CFR §164.528 (2001).
**34.** Privacy Act, 5 USC §552(a)(d).
**35.** Md Code Ann, [health-gen] §4-304(a).
**36.** 45 CFR §164.502(g) (2001).
**37.** 45 CFR §164.506 (2001).
**38.** Landers SJ. Physicians groups balking at privacy rule's extra burdens. *American Medical News.* May 7, 2001:1.
**39.** 45 CFR §164.506(b) (2001).
**40.** 45 CFR §§164.506(c)(4), 164.522(a) (2001).
**41.** 45 CFR §164.508 (2001).
**42.** 45 CFR §164.508(b)(4) (2001).
**43.** Starr P. Health and the right to privacy. *Am J Law Med.* 1999;25:193-201.
**44.** 45 CFR §164.510(b) (2001).
**45.** 45 CFR §164.502(b) (2001).
**46.** 45 CFR §164.530 (2001).
**47.** Gostin LO. *Public Health Law: Power, Duty, Restraint.* New York and Berkeley: Milbank Memorial Fund and University of California Press; 2000.
**48.** Protection of Human Subjects, 56 *Federal Register* 28003 (1991) (codified at 45 CFR §46).
**49.** Protection of Human Subjects, 45 CFR §46.111(a)(7).
**50.** 45 CFR §46.116(a)(5).
**51.** 45 CFR §164.512(i) (2001).
**52.** Institute of Medicine. *Protecting Data Privacy in Health Services Research.* Washington, DC: National Academy Press; 2001.
**53.** Gostin LO, Hadley J. Health services research: public benefits, personal privacy, and proprietary interests. *Ann Intern Med.* 1998;129:833-835.
**54.** 45 CFR §164.512(b) (2001).
**55.** 45 CFR §164.501 (2001).
**56.** 45 CFR §160.203(c) (2001).
**57.** Gostin LO, Hodge JG, Valdiserri RO. Informational privacy and the public's health: the model state public health privacy act. *Am J Public Health.* In press.
**58.** Model State Public Health Privacy Project. Available at: http://www.critpath.org/msphpa/privacy.htm. Accessibility verified May 2, 2001.
**59.** Centers for Disease Control and Prevention. Guidelines for national human immunodeficiency virus case surveillance. *MMWR Morb Mortal Wkly Rep.* 1999; 48:1-27.
**60.** 45 CFR §164.512(f) (2001).
**61.** 45 CFR §164.514(e) (2001).
**62.** Standards for Privacy of Individually Identifiable Health Information (Preamble), 64 *Federal Register* 82771 (45 CFR §160-164).
**63.** 45 CFR §160.203(b) (2001).
**64.** Health Insurance Portability and Accountability Act of 1996 §262 (1994).

> New opinions are always suspected, and usually opposed, without any other reason but because they are not already common.
> —John Locke (1632-1704)