There is a sacred realm of privacy for every man and woman where he makes his choices and decisions—a realm of his own essential rights and liberties into which the law, generally speaking, must not intrude.

—Geoffrey Fisher, Archbishop of Canterbury

Privacy

Rethinking Health Information Technology and Informed Consent

LAWRENCE O. GOSTIN

Above all values, Americans prize freedom—the right of individuals to control all aspects of their lives, including the personal and the economic. In many ways, both major political parties embrace individual freedom, with Democrats stressing personal freedom and Republicans economic liberty. What is often absent in political discourse around freedom, however, is the common good and an appreciation of when rigid adherence to individualism is inimical to collective welfare.

A core American value—privacy—is closely linked to freedom and clearly illustrates the tensions between the individual good and the collective good. Privacy is a foundational individual good that respects personal dignity and protects patients from embarrassment, stigma, and discrimination. Privacy is also a collective good that has societal value because it encourages individuals to participate in socially desirable activities such as biomedical research, health care quality assurance, and public health surveillance and response. Taken too far, however, privacy can seriously harm activities necessary for the public good. Privacy relating to medical records, for example, encourages individuals to access treatment and participate in research. However, if taken too far, it can thwart valuable societal activities such as quality assurance, cost-effectiveness studies, and epidemiological research if essential data are withheld from clinicians, risk managers, and researchers.

The prevailing model of privacy, both as formulated in theory and as enshrined in national policy, is doubly harmful. This model purports to safeguard privacy but actually fails to fully protect personal health information. At the same time, it significantly undermines socially valuable activities. President Obama's stimulus package, the American Recovery and Reinvestment Act (ARRA), authorizes $20 billion for health information technology, which is a cornerstone of the president's health care reform proposals. Unfortunately, ARRA and accompanying health care reform proposals do little to change the current privacy paradigm and, if anything, reinforce its flaws.

Privacy and Consent

With regard to health information, the most well-accepted definition of privacy is the right of individuals to control the collection, use, and disclosure of their personal medical information. Thus, individuals retain the right to strictly limit others' access to their personal data. Many scholars and policy-makers even assert that

Lawrence O. Gostin, JD, *is the O'Neill Professor of Global Health Law, Georgetown University; professor of public health, Johns Hopkins University; fellow, Centre for Socio-Legal Studies, Oxford University; and a Hastings Center Fellow.*

patients "own" everything to do with their body, including human tissue, DNA, future cell lines, and personal medical records.

The way modern laws and regulations assure these entitlements is to grant patients a right to fully informed consent. The Health Insurance Portability and Accountability Act, for example, adopts this model by giving patients the right to authorize most uses of their personally identifiable data.

Granting this right certainly makes sense when the data are to be used for purposes detrimental to the individual and society, such as discrimination in health care, employment, or insurance. However, it makes much less sense when each individual has the power to withhold information needed to achieve compelling public goods such as quality assurance, cost-effectiveness studies, medical records research, and public health investigations—even when potential harms to the individual are negligible.

The prevailing model of privacy fails to fully protect personal health information and significantly undermines socially valuable activities.

I propose an entirely different conception of privacy. Privacy should be understood as an individual's interest in avoiding embarrassing or harmful disclosures of personal information, while not significantly limiting equally valuable activities for the public's health, safety, and welfare. This conception allows that individuals have an interest in limiting access to personal data sought by insurers, employers, commercial marketers, and family or friends. But they would have a much-reduced interest in limiting the access of those engaged in highly beneficial, well-defined activities for the public's welfare.

This would require a fundamental shift in the way in which privacy is protected. Instead of relying chiefly on strict individual control of data by means of informed consent, it would erect meaningful privacy and security safeguards.

The Failure of Consent

Although consent is a dominant theme in law and ethics, in practice it fails to adequately protect personal privacy and is detrimental to valuable social activities. Multiple studies have demonstrated that patients do not read or understand complex privacy notices and consent forms, which are mostly designed to shield institutions from liability. Patients are also often asked to give consent when they are sick and incapable of making complicated decisions.

This means that consent is a poorly designed tool to prevent the most common causes of privacy invasion. Most professionals who access medical records—such as health care workers, health plan administrators, and lab technicians—are already authorized to do so. At the same time, many of the most visible and worrying privacy invasions occur due to security breaches, such as when data are left on laptops or databases with inadequate security.

Relying heavily on consent rather than on strong privacy and security assurances shifts the focus from meaningful safeguards to conceptual and often toothless ones. It provides patients with few real choices and burdens the health system with a new level of bureaucracy and expense. Furthermore, the prevailing model fails to safeguard personal health information both because it leaves gaps and because it is inconsistent.

The gaps in federal regulation leave many patients without protection against privacy invasions. Consider the "HIPAA Privacy Rule," which regulates "protected health information" held by "covered entities" such as health plans and health care providers. Personal data held by many entities that are not covered, such as pharmaceutical companies, remain unregulated. At the same time, the "Common Rule," which regulates human subjects research, applies principally to investigations supported by the federal government. Research carried out with private funding is often unregulated. This is in sharp contrast to most other countries, in which privacy regulations are not limited to particular health care transactions or funding sources, but instead apply to all health data.

Federal regulation and oversight of privacy is also inconsistent because of the marked and confusing differences between the Privacy and Common Rules. The standards for future consent, anonymized data, and recruiting patients vary under the two rules, leading to contrary results. There is no ethically principled reason for this patchwork of regulation.

Undermining Socially Beneficial Activities

A primary focus on consent is also harmful to the social good. Investigators report a diminished ability to recruit participants, obstacles in accessing stored tissue and genetic datasets, and increased complexity in IRB procedures, causing some hospitals and physicians to opt out of research. A universal requirement for consent, moreover, creates selection bias, which significantly limits the generalizability of results and leads to invalid conclusions.

Rigid understandings of privacy also hamper quality assurance and public health activities. There is a lack of clarity about whether privacy and research regulations apply to these vital activities. As a result, clinics, hospitals, and public health agen-

cies feel highly constrained when they seek access to or use personally identifiable health records.

The prevailing conceptualization of privacy as synonymous with strict individual control also defies common sense. We all have our own pet likes and dislikes, which is fine if each decision only affects the individual making it. However, allowing each person to make her own decisions in ways that disrupt the common good causes a deep social problem. Think of the consequences of granting individuals a virtual veto over each and every proposed use of their personal information for the foreseeable future. A patient might say, for example, that her information can be used for research on heart disease but not for research on AIDS or STDs. This effectively thwarts a great deal of health services research, and the same could be said for databases used for quality improvement or public health.

The perverse effects of privacy rules make life more difficult for investigators, physicians, and agency officials charged with carrying out research and public health activities. They undermine equally compelling individual and societal goods: scientific discovery, medical innovation, cost-effective health care, and methods of prevention that confront the nation's most pressing health problems. These are critical if health care reform is to succeed.

★ Policy Implications ★

What is urgently needed is a bold approach that would make federal regulations more effective in safeguarding privacy, more uniform and fairer in application, and less likely to impede socially beneficial activities. A new framework to the oversight of health records would emphasize data security, privacy, transparency, and accountability. Mandated security would include state-of-the-art systems with secure sign-on, encryption, and audit trails. Privacy safeguards would require that data be used only for well-defined and legitimate public purposes, with strict penalties for harmful disclosures. Security and privacy procedures would have to be transparent and actors held fully accountable. By focusing on fair informational practices, patients would gain strong privacy protection, with the assurance that their personal information would not be disclosed to their detriment and that data would be protected against security breaches.

To achieve public confidence, the new system would require careful ethical oversight focusing on measures to protect data privacy and security, harms that could result from data disclosure, and the potential public benefits. An alternative framework could also include a certification for entities that undertake large-scale data collection for defined health purposes or to link data from multiple sources for the purpose of providing more complete, anonymized datasets. Federal monitoring and enforcement would ensure regulatory compliance, and legal sanctions would prohibit unauthorized attempts to make donors of anonymized data identifiable again.

Information technology certainly will be a key component of national health care reform, but it will fail unless policy-makers safeguard privacy and facilitate responsible research, quality assurance, and public health. President Obama wants to achieve both cost-effective health care and strict privacy. But the stimulus package and his health care reform proposals do little to resolve the fundamental flaws of an antiquated model for safeguarding privacy. The success of health reform depends upon our ability to develop as rapidly and completely as possible our understanding of what works in health care, and an awareness that a false sense of privacy works against that urgent need. ★