Journal of Contemporary Health Law & Policy (1985-2015)

Volume 18 | Issue 3 Article 11

2002

Health Records Privacy and Confidentiality: Pending Questions

Gerald S. Schatz

HEALTH RECORDS PRIVACY AND CONFIDENTIALITY: PENDING QUESTIONS

Gerald S. Schatz[*]

"Privacy" and "confidentiality" of medical data and records in health care and biomedical research on human subjects are the stuff of myth and illusion, often more symbolic than substantive. Let me begin with some definitions and my perspective, then mention some emerging technologies and point to some important, lingering questions.

As I use these terms: The right to privacy refers to the right of the person to be left alone in ordinary circumstances, to be free from arbitrary intrusion into one's affairs by government and by other persons. As against government, privacy may be a constitutional or statutory protection. In the United States, to the extent that privacy protections exist, they are enforceable in the courts in civil litigation and due process claims. Confidentiality refers to safeguarding privacy. Records may be subject to varying degrees of confidentiality in order to protect the privacy of the persons who are the subjects of those records. Medical, health and biomedical, as used here, include behavioral and social science and social services. Technology is used here in the anthropological sense, to refer broadly to how we work in a cultural and societal context. This is especially important. Ultimately, people, not organizations or machines, are the requestors, suppliers, processors, manipulators, users, buyers and sellers of information. People are the devisors of systems for processing information.

First, let me provide some perspective. After my wife emerged from the cancer ward of a local hospital, that institution's contract fund-raiser called and asked how her stay went on the cancer floor. A few weeks later, she began getting targeted mail from the funeral industry. Today, the credit card industry sends her offer after offer, praising her creditworthiness and promising huge credit lines. Alas, she has been dead for nine months. The

---

[*] Of the District of Columbia Bar. Mr. Schatz teaches Biomedical Ethics Law at the Graduate School of the Foundation for Advanced Education in the Sciences, Inc., and in September 2002 became a visiting scholar at the Center for Clinical Bioethics, Georgetown University Medical Center. He has been a public member of the Institutional Review Board of the National Institute of Child Health and Human Development, and he is a public member of the Hematopoietic Progenitor Cell Standards Program Unit of the American Association of Blood Banks.

business world that would exploit health and medical records is neither monolithic, nor invariably smart.

More perspective, the Hippocratic Oath obliges the physician to protect the patient's privacy—including the privacy of the patient's house—but only in part. The Oath bars the physician's disclosure only of what ought not to be divulged from the physician-patient relationship. What ought to be divulged is, in the Oath, a societal matter. The standard of care, so to speak, does not include absolute confidentiality, although many physicians believe, or dearly wish, to the contrary. The myths of absolute privacy of the patient or biomedical research subject persist, as do myths concerning the right and obligation of a caregiver or researcher to protect the patient's or subject's privacy and to safeguard the health record. Of course, there are readily acknowledged departures–chiefly for public health and child safety and to interact with other persons and entities in the patient's behalf. The cherished medical obligation of confidentiality has both ethical and legal roots and is in continuing tension with societal demands. In the United States, courts long ago cut deeply into the doctor-patient privilege. The United States Government and state governments long have had access to health records in connection with health-care subsidy, public benefit programs, schools, clinics, prisons, public and private occupational safety and health, public hospitals and biomedical research–including behavioral and social research. Law enforcement agencies are establishing DNA databanks. The world's financial and business structures and their regulation have changed. A large firm may be involved simultaneously in banking insurance, and other businesses, all in addition to its involvement in employee health benefits and occupational health. At the same time, that firm may be subject to multiple regulatory structures in each of several countries and in several jurisdictions of federal states. Far smaller, independent firms may be involved in some aspects of processing medical information.

Increasingly and dramatically, payment for health care in the United States has shifted away from classic insurance and toward a combination of government-subsidized facilities and care, government insurance, and managed care in which insurance firms administer not so much their own money as employers' benefit funds, employee premiums, and business arrangements include drug company tie-ins. Information on the patient's condition and treatment joins the financial record.

Accordingly, much may depend upon the uses and misuses of the health record. Efficient use of information technologies in diagnosis, therapy, prophylaxis, and research and development redounds to the benefit of

patients, the public and insurance providers, as does efficient administration of health benefit and public health programs.

But the easy availability of private information also lends itself to invidious discrimination. For example social stigma or Kafkaesque denials of mortgages or employment to qualified applicants whose health records mark them as health insurance risks. Similarly, the easy and un-policed acquisition and sharing of personal data lends itself to targeted marketing, which some may deem a service and which others may deem an un-consented exploitation. Accordingly, the need to protect the privacy of patients and research subjects and to protect the confidentiality of their health records is a deeply felt, continuing concern of patients, research subjects, ethicists, and healthcare professionals.

Legislation and regulation reflect the pendency of these concerns. These concerns are not new. The National Research Council Computer Science and Engineering Board sought in its report *Databanks in a Free Society* to clarify the interrelationships of responsibility, confidentiality, and technology: "It is the increased feasibility of data sharing, and not any significant changes in either privacy or due-process interests, that will be the most important effect of advances in computer technology" in these regards. Clear implications then, in the Board's view, included extending "the zones of personal and group freedom from compulsory data collection," providing "greater rights of access by individuals to the records maintained about them," providing greater rights to contest those records, questioning the need for data collection case by case, and abolishing some old files altogether." The criteria for data collection would be demonstrable of a need to know and share. Why was the data being sought? What uses would be made of it, and by whom? The report by the Computer Science and Engineering Board was published in 1972. These questions persist.

The emerging technologies of interest in this respect are, first of all, organizational changes. Persons, subject to no health professional ethical strictures have become negotiators, gatekeepers, processors, exploiters, and vendors of patients' secrets. Research subjects and medical patients are not negotiators in the international trade harmonization arena.

In ordinary, non-exotic health care, the use of the contract of adhesion with respect to personal data is increasingly common. Some have characterized it as "sign or die."

The emerging Internet technologies, including web-based medicine and pharmacies; email; malicious coding; data-mining; and computer-based private investigations all acquire and share personal data. Among the

problematic emerging technologies, anticipated in that report twenty-nine years ago, is a black market in personal data.

Pharmacogenomics, tailoring drugs to individuals, is an area of great interest in medical research and development, but poses considerable danger to health privacy absent adequate controls over acquisition, verification, and sharing of personal information.

Genetic testing and disease prediction increase the severity of consequences of breaches of confidentiality.

Tissue banking, cross-linkage studies, and longitudinal studies pose difficult problems. Further, in some U.S. hospitals, patients are pressured to provide tissue samples for use in the biotechnology industry. Over several years, a great deal of tissue has been acquired in the course of research, and by cross-linking with medical records it has become possible to infer relationships between genetics and medical conditions expressed later in life. Finding and tracking the individual subjects may raise issues of unconsented invasions of privacy. Again, the consequences of information leaks here can be severe for the individual patient and confidentiality should not be a cover for violation of rights. However, that shield may have to be penetrated in limited circumstances; for example to ascertain that the taking of tissues did not come from coercive circumstances.

Behavioral genetics, whether based on actual genetics or on family background, behavioral genetics and related social research, may be particularly troubling. Many proponents of research in this area see it as the search for a key to finding the predictors of behavior to facilitate timely and effective interventions. Studies of children deemed by researchers to be "at risk" for behavioral problems fall into this category. Often, these studies target slum school populations and involve school personnel. Misuse and leaks of personal information from these studies can be devastating in their effects. Students may be labeled and channeled into ostensibly remedial or preventive programs without due process of law. Predictions of antisocial behavior may become self-fulfilling prophecies. The predictions may come to haunt these children in law enforcement proceedings and in searches for employment. The law enforcement and security industry has been trying to sell the District of Columbia Government a schoolchildren's identity card system. The card would include health information. The processing system and facilities would be managed by the D.C. Department of Motor Vehicles.

This is a troubling set of factual challenges, the more complicated both in the United States and Europe because of complex and seemingly comprehensive regulatory structures. Notwithstanding the structure and

content of regulation, the big questions remain: Why is the data sought? How will it be used? By whom? What rights does the subject of the data have?

The European Union's Directive 95/46/EC, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, requires member states to legislate privacy protections that begin with personal privacy as the default position, is more protective than U.S. legislation and regulation on confidentiality of personal records. The directive's efficacy remains open to question, however. Thus, the draft Charter of Fundamental Rights of the European Union provides in Article 8 for "Protection of Personal Data" that instrument leaves open the question of remedy.

For all their gaps, these European developments have left U.S. international companies scrambling to conform their personal data practices to requirements in the European Union. This has been no simple task, inasmuch as those same companies must conform to U.S. requirements that do not make privacy and confidentiality the default position. Rather, Gramm-Leach-Bliley, the Financial Services Modernization Act, seems comprehensive as to consumer privacy but permits a great deal of data sharing unless consumers opt out. Recent regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 seem comprehensive at first glance, and were announced by the Department of Health and Human Services on December 20, 2000, as "Protecting the Privacy of Patients' Health Information." The HIPAA regulation is a records management regulation. Neither HIPAA nor the regulation addresses comprehensively the big questions such as; Why require the data? Who will use the data, and for what purpose? The HIPAA regulation spells out certain requirements for health records management, and it partly limits data sharing. The Continuing Legal Education industry in the United States has gone to work to train lawyers in HIPAA compliance counseling. Perhaps more because of fear of government inquiry than because of the rule itself, there are good-faith efforts to comply–although I doubt that the rule will withstand judicial scrutiny or last long in its present form.

The thirty-one-page rule and its 338-page preamble constitute a wonderful exercise for teaching administrative law. Consider: Does the preamble correctly state its constitutional and statutory authority? Does the preamble make sense? Notwithstanding whether it makes sense, is it consistent with legal authority? Does the rule respond to an intelligible principle in the legislation? That requires in turn that one look at the legislation for an intelligible principle, and that is a difficult task. How is

the rule designed to work in practice? It does not appear that any thought has been given to how the rule would actually work in practice. What protections does the rule provide and for whom? Who is exempted from the rule's obligations? Law enforcement agencies and any public body that wants to make an inquiry with an administrative subpoena or data request is exempted from the rule's obligations. Who is exempted from the rule's protections? Approximately eight million Americans who are either prisoners or detainees. Detainees are people who have been arrested but who have not been tried. Under what circumstances is the rule superceded by more protective state law? The default is to the federal requirement. How does the rule apply to various Federal and state entities? These issues are effectively unaddressed. When is full compliance expected? At least two years from the effective date of the rule. What right of remedy is provided? None. What mechanism for enforcement is provided? None. Yet these are basic tests for the efficacy of any administrative rule in American law. Now with these questions in mind, look again at the rule.

These are basic tests for efficacy. With these questions in mind, look at the rule. It mandates certain health records management procedures, but its exemptions are many and its enforcement provisions are empty. Some of its interlaced paragraphs give, while others take back. Nevertheless, the good-faith compliers will try to reorganize and reprogram their data management to meet the requirements of the HIPAA and Gramm-Leach-Bliley rules, and the transnational firms will try to adapt to the various European national implementations of the E.U. privacy directive. Well before HIPAA, some U.S. health management organizations and healthcare institutions instituted exemplary data-confidentiality measures. That's expensive, it's not easy, and it is not the national pattern.

In several of the United States there are miscellaneous anti-discrimination statutes. Tort law still exists, and there are Federal statutes that address discrimination. However, whether in the United States or elsewhere, legislation and regulation notwithstanding, vindication of rights is slow and expensive. There remain those nagging big questions. Are we captive of emerging technologies? Consider these extracts from that National Research Council report:

"Our task is to see that appropriate safeguards for the individual's rights to privacy, confidentiality, and due process are embedded in every major record system . . ."

". . . What is collected, for what purposes, with whom information is shared, and what opportunities individuals have to see and contest records are all matters of policy choice, not technological determinism."

We "cannot escape . . . social or moral responsibilities by murmuring feebly that 'the Machine made me do it.'"

That report has been around for more almost three decades. The issues that it raised still await ethical, efficacious answers.