

Reprogramming the Hippocratic Oath: A Historical Examination of Early Medical Informatics and Privacy

Jeffrey R. Yost

.....

Abstract

Recent advances in genetics, the accelerating possibilities of securing and processing medical data, and the near ubiquity of computer medical databases and networked connections have combined to heighten the focus on privacy as one of the most fundamental ethical issues in medicine. Over the past decade considerable attention has been given to medical databases and privacy by journalists, policy makers, and others, yet very little is known of the origin and structuring of the privacy issue in early medical computing. Drawing on the Willis H. Ware Papers at the Charles Babbage Institute, medical journals, conference transcripts, government documents, and other primary and secondary sources, the following survey examines medical information systems and privacy from the early 1960s to the present. It documents the obscurity of the issue in the late 1960s; confusion and inaction in the 1970s and 1980s; and renewed focus, policy debate, and attempts at legislation in the 1990s. The paper concentrates on the place of medical information systems and privacy within the larger debate that was emerging on computers and privacy and new possibilities in epidemiology and public health.

The idea of privacy has had a complex history that began long before its relatively recent ascent into the public arena of legislation, adjudication, and widespread media and political debate. Prior to erupting onto the scene as the foundation for controversial court decisions in the United States on birth control (*Griswold v. Connecticut*, 1965), abortion rights (*Roe v. Wade*, 1973), and other personal, political, and social issues of the 1960s, 1970s, and beyond, privacy had led a relatively sedate life of varying form but continuing presence across time, place, and culture. In the United States, as in the rest of the world, much of this long history remains unexplored. Early writings on privacy

concentrated on legal issues and the growing threats made possible by advances in information technology. This tradition began in the late 1960s and gained momentum with Arthur Miller's influential book *The Assault on Privacy: Computers, Data Banks, and Dossiers* (1971). David Flaherty's monograph *Privacy in Colonial New England, 1630–1776* (1972) and Hannah Arendt's celebrated study of public and private life, *The Human Condition* (1958), stand as notable exceptions that analyze cultural aspects of privacy. Charles Sykes's *The End of Privacy: Personal Rights in the Surveillance Society* (1999), however, is representative of most privacy literature—focusing on privacy as a critical right and its invasion by government as a fundamental problem. Throughout the past three decades, as attention to privacy has escalated in response to the proliferation of computers and networking, the expanding literature on the topic has retained a fairly narrow focus on defining and interpreting legal rights.

The following essay extends beyond the strictly legal domain of data banks and privacy by broadening the mode of analysis to include social and ideological components, while at the same time concentrating on a single realm: medical computing during its formative decade (the late 1960s to the late 1970s). The centrality of the issue of computerized medical records and privacy over the past five years, after decades of public and legislative neglect, only heightens the importance of gaining a clearer grasp of its infancy and early adolescence and the opportunities, challenges, and constraints posed by such a history.

The story to be told about protecting medical

records is quite different from that associated with protecting nonmedical records, such as financial records, which have been the subject of greater public and legislative focus. The history of medical data and privacy includes several significant topics: public opinion and the level of trust in medical care providers and institutions, the background and work of the leaders who raised the medical computing privacy issue, and the influence of the broader dialogue on data banks and privacy. I will explore elements of these topics, but first I will lay a foundation by providing a brief overview of the history of technology and privacy and an outline of the emergence of medical computing.

Evolving Cultural and Legal Conceptions of Technology and Privacy

Despite the absence of a direct discussion of privacy in the U.S. Constitution, many Americans perceive privacy as a right no less fundamental than any explicit in the Bill of Rights. The earliest articulation of a legal right to privacy was made by Louis Brandeis and Samuel Warren in a landmark *Harvard Law Review* article of 1890. Based primarily on torts, they argued for protection of not only property but also thoughts, sentiments, and emotions (Warren & Brandeis, 1890). Over the past several decades the Fourteenth Amendment (protecting life, liberty, and property) and torts have provided the legal basis for a number of piecemeal state privacy laws. Some of these came in direct response to new technologies, such as New York State's law resulting from the use and abuse of the handheld camera by journalists in the late nineteenth century (Mensel, 1991; *Corliss v. E. W. Walker*, 1893).

During the middle third of the twentieth century the relationship between technology and privacy often took the form of government intelligence and law enforcement creating and using new surveillance tools as they concomitantly developed devices of countersurveillance (Westin, 1967). More recently, these activities have been mirrored by attempts primarily within but also outside of government to develop ever more complex computer encryption devices, alongside attempts to program code-breaking software.

The Advent and Early Development of Medical Computing

Digital computing developed out of World War II research to help calculate ballistic trajectories and further other scientific and engineering projects. While com-

puting applications in the physical sciences were becoming increasingly common in the 1950s, use of these machines in the biological and medical sciences was typically absent. By the late 1950s, however, Robert Ledley, Lee Lusted, and several other physicians worked with computer specialists to pioneer computer applications in medicine. Ledley, a young dentist, had been stationed at the National Bureau of Standards (NBS) during the Korean War and greatly benefited from the knowledge of a number of NBS scientists in using the Standards Eastern Automatic Computer (SEAC). Later in the decade Ledley took a position at George Washington University and teamed up with National Institutes of Health physician Lee Lusted to develop computerized diagnostic systems (Yost, 2002; Collen, 1974; Ledley, 1965; Lusted, 1968).

In their diagnostic systems Boolean logic was used to compare individual patient records with growing databases of medical histories. Computing centers at universities were frequently tapped to process information, as only a small number of hospitals and laboratories invested in mainframe computers in the early to mid-1960s. The increased use of time-sharing and the success of minicomputers by the late 1960s led to the acceleration of computer installations in medical laboratories, clinics, and hospitals (Yost, 2002).

Networking and the formation of large databases, coupled with the widespread exchange of medical information, became more common in the late 1960s. At this time the role of computers began to grow from discrete diagnostic tools into systems fundamental to the practice of public health and epidemiology. Hospitals and other medical institutions also increasingly used computers for administrative purposes by the late 1960s. Soon thereafter the term *medical informatics* came into common usage in the United States to refer to the application of computers in medical care, research, and administration—everything from patient health records and computer diagnostic tools to billing and human resource management systems.

The large-scale adoption of computers in medicine was far from smooth, however, as a number of physicians and those outside the profession argued the diagnostic limitations of these machines (Agalides & Swisher, 1964; Hubbard, 1972). Nearly all critiques of medical databases and hospital information systems were couched in terms of their performance and cost, and the issue of privacy remained conspicuously absent during much of the 1960s. This situation continued into the first half of

the 1970s, while cutting-edge diagnostic medical computing became linked in part to research on expert systems (a database coupled with a heuristic-based inference engine that draws meaning from data) and the new field of knowledge engineering. Stanford computer scientist and expert system pioneer Edward Feigenbaum worked with Stanford University School of Medicine's Edward Shortliffe to develop what is credited as the first medical diagnostic expert system, MYCIN, in the early 1970s (Blum & Duncan, 1990).

Literature on privacy issues in medical journals and scientific conferences during the 1960s, however, was quite rare. There were a few short articles and "letters to the editor" appearing at the end of the decade, but they did not precipitate a discussion, let alone an ongoing debate. Each year there were hundreds of articles on medical computing and many conferences on the topic, but very few of these even mentioned privacy (Yost, 2002).

Given this dearth of attention, a two-day 1969 conference on medical-computing privacy at the medical school of the State University of New York at Buffalo stands out. The participants were almost all local professionals, ranging from physicians, medical researchers, and hospital administrators to computer technicians, lawyers, and medical librarians. Physicians, who made up the majority of the speakers and participants, offered a wide range of opinions. Many doctors and hospital administrators expressed fears of "Big Brother," seeing the government as the greatest potential abuser. Some saw little benefit of computers in medicine and emphasized the machines' depersonalization of health care; others argued an ethical obligation to reap the societal benefits of medical computing applications (*Right to Privacy*, 1969).

Physicians at the conference favoring the growth of medical informatics emphasized the need for greater cooperation between doctors and computer specialists, both to develop the field and to ensure that systems were set up better, with proper safeguards to protect against unauthorized access. Several of those present, including Elemer Gabrieli, repeatedly stressed the need for a new professional, a "privacy administrator" (*Right to Privacy*, 1969), and expressed some doubt whether medical records librarians could, as a group, assume this role, which would require competence in programming lan-

guages, security, and legal matters. One discussant from the medical records library field, Margaret Beard, took issue with this, emphasizing her profession's current base of relevant knowledge and skills and desire to address the difficulties that lay ahead:

We feel that the role of the medical record librarian is changing drastically and that we will be able to meet the challenge. . . . What we offer are specialized skills based on vast experience in the field of medical records. This experience can serve as the crucial link between medicine and machine or, if you will, physician and engineer. (*Right to Privacy*, 1969)¹

Overall, the presentations and discussion at the conference reflected an exploration of a new issue in which opinions were being formed based on limited experience, and there was much uncertainty of the different knowledge and skills that people from various professions might bring to the difficult questions of medical computing and privacy. The local nature of the conference did not result in a discussion of local systems or problems but instead promoted an often ill-informed dialogue on the national "privacy problem" with a focus on medical informatics. The conference appeared to make no impact, and there is no evidence that it provided momentum for follow-up research. Instead, much of the meaningful early analyses and emerging national leadership on the general issue of computers and privacy (which tended to focus nearly exclusively on government databases of records on individuals), and the more specific question of medical informatics privacy (an issue that by the very nature of our health care system involved many private-sector concerns), came from a research corporation with close ties to the federal government, the RAND Corporation.

One reason that the conference probably had little impact and that there were not others around this time was the uncertainty and lack of standardization in the field of medical computing to talk about it effectively in broad terms (Blum & Duncan, 1990). Also in 1969, but after the conference, a physician, L. L. Weed, proposed the first computer record format that took hold at a substantial number of institutions: Problem Oriented Medical Information System (PROMIS). In the end, however, PROMIS came under severe criticism, as

¹ While there has been some historical research on library applications of computing technology, including analysis of MEDLINE and other systems, there is a complete absence of scholarly literature on the role of librarians in hospitals and laboratories in maintaining collections of medical records.

many physicians found the eight steps it took to make a medical decision too cumbersome (Tange, Hasman, Robbe, & Shouten, 1997). Three years later the first systems that would stand the test of time were developed and implemented. In 1972 the Regenstrief Medical Record System (RMRS) was created, a popular system that could monitor situations and remind physicians of actions that should or should not be taken (Tange et al., 1997). By 1975 the famed HELP medical record system was installed for the first time at the Latter Day Saints Hospital in Salt Lake City, Utah. Its fundamental feature was providing decision support. It had standardized preformatted screens on which controlled medical vocabulary was entered. Among its applications was the direction of respiratory therapy for intensive-care patients (Tange et al., 1997). With such software systems as RMRS and HELP medical computing was quickly gaining a foothold in a number of hospitals and medical research centers. Networking between installations was also becoming increasingly common in the 1970s. Given these developments, computers facilitated the recording, maintenance, and sharing of far more patient information than ever before for medical care and administration. Related to these growing databases, a small but increasing concern about privacy and medical records began to appear at the national level.

The RAND Corporation, Willis Ware, and Early Leadership in Medical Informatics Privacy Issues

Communications scholar Philip Agre, in the introduction to *Technology and Privacy: The New Landscape* (1997), wrote of “tectonic shifts” in nearly all aspects of the technology (particularly computing) and privacy policy debate since the 1980s. One of the key shifts he identified was the emergence of a generation of technologically sophisticated privacy advocates. While he is undoubtedly correct that a far greater number of Americans have some basic knowledge about computers and more experience using them than in the previous generation, he ignores the fact that the earliest significant advocates for examining data-security issues and ensuring privacy came from the computing field during the mid- to late 1960s. Some new components to the privacy debate have been added with the proliferation of personal computers and networking over the past quarter century. With the focus of the debate on government intrusions, however, the best way to characterize it during this span of time is by continuity rather than change. This focus has

often diverted attention away from perceived and real privacy invasions by corporations and other organizations and individuals. The concentration on government, at least at first glance, is also ironic given the fact that the computer specialists leading the way on the privacy issue were from the quasigovernmental, Department of Defense–sponsored RAND Corporation.

During the 1960s RAND’s computer center had been one of the first industrial computer installations in the country to research and implement data-security procedures. In March 1967 RAND scientists Paul Baran, Paul Armer, and Willis Ware led the first focused effort by a federation of computer societies (American Federation of Information Processing Societies) to try to come to a consensus on policy regarding security and privacy. Ware, an electrical engineer who had joined RAND in the early 1950s, chaired the session and presented a paper on the similarities and differences between security and privacy (Turn, 1972).

In a report published in 1967 by the RAND Corporation, Baran turned specifically to the medical field and rephrased the Hippocratic oath in light of computing technology. Baran was the inventor of packet switching, the most important technology of the ARPANET-Internet. The Hippocratic oath, formulated in the fifth century B.C., has long been identified as a professional ethical pledge by physicians to maintain the privacy of their patients. With regard to mental health records Baran posed the question: “How can anyone meet this [privacy] obligation in a future era of amoral computers, which may or may not be discreet, serving both as servants and middlemen?” (Baran, 1967)

Baran speculated that file systems, the proliferation of storage services, economic pressures to centralize, and the future growth of time-shared data would combine with concomitant trends in health care, such as the rise of widespread health insurance plans, medical specialization, and more on-line patient monitoring in hospitals, to extend greatly the problem of maintaining privacy. His report raised significant questions but offered few policy alternatives; it did not appear to have a significant initial impact in either the medical or computing communities outside of RAND. At RAND, however, Baran’s report marked one of the first forays into computer privacy issues and the first on medical informatics privacy, a topic to which other scientists at the corporation soon gravitated. Of particular note was RAND’s Willis Ware, who would soon make computer privacy

issues the focus of his professional work within and outside of RAND. Ware had worked in the late 1940s with John von Neumann and others at Princeton University's Institute for Advanced Study (IAS) in developing and using the computer (Baran, 1967; Ware, 1970, 1971, 1973, 1975, 1976, 1977, 1981).

Simultaneous with RAND's privacy research, the issue also garnered attention in legal circles during the mid- to late 1960s. The 1965 ruling on a landmark birth-control case, *Griswold v. Connecticut*; the work of the Special Committee on Science and Law of the Association of the Bar of the City of New York, which resulted in Alan Westin's *Privacy and Freedom* in 1967; and Arthur Miller's project at the University of Michigan Law School (the basis for *The Assault on Privacy* in 1971) all contributed momentum. Even more influential to public awareness of the computer privacy issue was the congressional and public debate over President Lyndon B. Johnson's proposal for a National Data Center in 1967 (Westin, 1967; Miller, 1971; Sykes, 1999). The center, which would have combined the databases of twenty federal agencies, came under attack from the media and public and was abandoned. Four years later Arthur Miller, reflecting on the National Data Center proposal, argued that far larger data banks of personal information were already used by the executive branch (Miller, 1971; Sykes, 1999).

The debate over the National Data Center and Miller's widely read book were the two most significant developments fueling the early debate on the right to privacy. Each centered the discussion on intrusions by the federal government. Miller, Westin, and other legal scholars studying privacy, in contrast to Baran and his RAND colleagues, did not give significant attention to medical informatics privacy, at least in part because the subject mainly concerned hospitals and other institutions in the private sector.

Of the RAND scientists, Willis Ware had the longest and most sustained focus on privacy issues in medical informatics. Following on the momentum for the privacy issue generated by the conference in 1967, late that year Ware became the chair of the newly established Defense Science Board Task Force on Data Security. He also served as chair on several other Department of Defense science advisory boards on security and privacy in the late 1960s. This experience led to his leadership roles on the two most important privacy policy federal advisory groups of the 1970s: the Automated Personal Data System (APDS) Committee and the Privacy Protection Study Commission (PPSC).

Department of Health, Education, and Welfare Committee on Automated Personal Data Systems

In 1972 Elliot Richardson, secretary of the Department of Health, Education, and Welfare (HEW), established the APDS Committee. He acted in the context of the short-lived discussion over a National Data Center, increasing use of Social Security numbers as personal identifiers, and more broadly, growing public concern about unregulated applications of computer technology to the government's acquisition, storage, and dissemination of data on U.S. citizens. Specifically Richardson took the lead in forming such a committee because HEW maintained Social Security records. The government's use of Social Security numbers as an identifier, however, was just a point of departure, as the APDS Committee took it upon itself to examine a broad range of privacy issues both within and outside of government.

The APDS Committee was composed of such computer experts as Joseph Weizenbaum, of MIT's computer science department, and Arthur Miller, as well as prominent individuals with backgrounds in business, academe, medicine, law, and government. The committee also included students, a police officer, and a homemaker to lend perspective to public opinion on privacy issues. This diverse group of roughly two-dozen members conducted nine multiday meetings in the first half of 1972 and early 1973. Willis Ware, an influential member of the committee from the start, replaced Frances Grommers, a physician from Harvard University's School of Public Health, as chair at the beginning of 1973.

From the start the APDS Committee examined many different issues and brought in a varied group of experts. The committee's privacy research, discussion, and testimony, however, fell within several broad realms: education, insurance, finance, and medicine. The group gave particular attention to the latter two areas. Several years before the committee was formed, the Fair Credit Reporting Act had been passed to allow individuals to access and correct mistakes of their credit history. While the APDS Committee often discussed financial records privacy, the consecutive chairs, Grommers and Ware, showed particular interest in medical records privacy.

In the late 1960s and 1970s, however, public interest in protecting the privacy of financial records dwarfed public concerns for medical privacy. Legislation, media attention, and anecdotal testimony in front of the APDS Committee support the prevalence of this prioritization.

Such sources also indicate that most patients had a significant trust in their physicians. By 2000, however, the discrepancy in public interest and attention between these two areas of privacy concerns substantially narrowed.

The growing public and political focus on medical informatics privacy is at least in part a result of the increased use of medical records by agents who are not physicians, such as insurance companies, employers, and pharmaceutical firms. Increasingly, medical information was bought, sold, and traded by such individuals and organizations. In light of these developments, by the last years of the twentieth century public and political focus on medical informatics privacy had grown to match that of protecting the confidentiality of financial records (Gallup Organization, 2000; Ware, 1972–1977a, 1972–1977b).

Despite the lack of public or media attention, by the start of 1973 Ware maintained and even heightened the focus on medical records privacy. Extensive documentation and testimony were gathered on the creation, dissemination, and use of medical records. While there was no clear consensus, public health physicians were leery of regulations that might inhibit the broad collection of useful public health data. In general, physicians did not view privacy as something new in the era of medical computing but rather as a continuation of their oath to protect patient privacy. A minority, however, recognized that the playing field had changed dramatically in the era of computers, and the scale and scope of opportunities for abuse of patient health data had grown. Some physicians testified in favor of safeguards; however, most doctors did not see health privacy as a significant problem (Ware, 1972–1977a).

By March 1973 the APDS Committee concluded its regular meetings, and in July it published its findings in a report submitted to Caspar Weinberger, the new secretary of HEW, titled *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education, and Welfare* (Automated Personal Data Systems Committee, 1973). This three-hundred-page report offered glimpses into the committee's exhibits, testimony, and discussions but largely abandoned the subject area focus (finance, education, insurance, and medicine) of the meetings in favor of broad generalizations on privacy. The report also concentrated on several important issues that had been with the committee from the start, such as the costs and benefits of using Social Security numbers as standard

identifiers (Ware, 1972–1977a). The committee recommendations to achieve “information fairness” included developing a code to protect against secret personal-data record-keeping systems, providing a means for individuals to investigate what information is being kept on them, and giving an opportunity for people to correct false information in their personal records. These general ideas became the basis for the Federal Privacy Act of 1974 (Privacy Act, 1974; Ware, 1972–1977a).

The Privacy Act of 1974 provided significant protections against certain areas of federal government-controlled medical data systems. Federal hospitals, such as Veterans Affairs hospitals, fell under the jurisdiction of the legislation, and thus patients had some rights with regard to the inspection and correction of records. The Privacy Act, however, did nothing with regard to private systems, including many maintained by hospitals and medical research centers. As deliberations of the APDS Committee during 1972 and 1973 repeatedly indicated, medical records privacy issues were unique. Discussions recognized that privacy protection rules could have important costs (as well as benefits), such as the potential harm that could arise from individuals seeing their own medical records and public health benefits from large medical record data banks.

In short the APDS Committee's final report did not reflect the many complex technological and administrative issues explored throughout the committee's long deliberations. In turn, the Privacy Act left wide parameters for interpretation, but some areas, such as nongovernmental medical records systems, were untouched by the 1974 legislation. This was not a failure on the part of Ware's committee but rather a calculated effort to get some important federal legislation in place and begin work on the more complicated issues of specific areas. Ware recognized that his committee's report and even the Privacy Act were works in progress. The Privacy Act, following a recommendation from the ADPS Committee, called for a continuing commission, the Privacy Protection Study Commission, or PPSC, to explore further certain areas of information systems, particularly those made up of medical records (Privacy Act, 1974).

The Privacy Protection Study Commission and Continuing Privacy Work

Ware became the vice chair of the PPSC and was instrumental in the group's continuing and significant focus on medical records data and privacy. Between 1974 and 1976 this commission did more to explore

impartially the many complex issues and competing concerns regarding medical informatics privacy than any previous group (Ware, 1972–1977b).²

In contrast to its reaction to the APDS Committee, in 1976 the American Medical Association, or AMA (an organization representing 215,000 physicians at the time), came out with a position paper for the PPSC that was presented by one of the association's board of trustees members, Joseph Boyle. Boyle's paper emphasized new threats posed to patients' privacy in the era of computerization. Nevertheless, it placed the responsibility for these problems in the hands of third parties and patients, stating that often these third parties had been authorized by the patients to receive medical information. While the AMA argued that some legislation would be helpful, it believed that such legislation should be decided at the state rather than federal level and that general provisions of the Privacy Act of 1974 should not be extended to private hospitals and other repositories of medical records. Boyle emphasized that such a requirement would interfere with the delivery of quality medical care by preventing the free flow of information between doctors, patients, and medical care organizations (Ware, 1972–1977b). While state legislation was advocated in the paper, this may have been merely a diversion to shift focus away from more stringent federal legislation, as no specifics on state laws were in the AMA report.

Not surprisingly, a presentation by the American Public Health Association (APHA), an organization of fifty thousand public health care providers, took an even stronger position against application of the Privacy Act to private-sector medicine. Lester Breslow, representing the APHA, told the PPSC that an exploration of means to maintain anonymity made sense, but any regulation of the exchange of information between medical institutions would result in negative impacts to epidemiological research and overall public health (Ware, 1972–1977b).

Ware's work on the PPSC also led him to publish several RAND reports on the medical records privacy issue and the difficulties in getting legislation passed. These reports contained primarily anecdotal material of cases where employees and managers almost immediately knew workers' physical or mental health assessments by physicians. While there was not necessarily direct elec-

tronic access to the records by employers, the computerization of medical information, coupled with the growth of employer-paid health insurance, created an environment where patient data was far more dispersed and accessible than in previous decades, when it only existed in paper form in physicians' file cabinets (Ware, 1975, 1977).

In general, the PPSC and Ware's related work identified some of the complex issues and competing concerns with regard to medical records data banks and privacy. This work failed to reach a concrete conclusion, however, and in many respects was limited by both the rapidly evolving types of medical record applications and the political environment. The PPSC devoted the latter part of its final report on the "Medical Records Project" to address an anticipated national movement toward a federalized health insurance pool under the Carter administration. In some respects the short history of medical computing offered little guidance to a rapidly changing contemporary environment and hindered the ambitious efforts of the PPSC (Ware, 1972–1977b).

Renewed Efforts to Ensure Medical Privacy

Following the work by the PPSC, President Jimmy Carter made a major push for privacy legislation that would have given individuals greater control over their own health data. These efforts, however, fell largely on deaf ears in Congress. The issue was not a high-level concern of the subsequent presidential administrations of Ronald Reagan and George Bush. As use of computers by physicians became increasingly ubiquitous in the 1990s (Freudenheim, 2001), public and journalistic attention on the medical privacy issue increased. The rhetoric of the debate, however, continued to be at the extremes.

In 1994 the Institute of Medicine wrote a report titled *Health Data in the Information Age: Use, Disclosure, and Privacy*. The report came out strongly against a regulation prohibiting widespread access to records that might be used in research and health care. While it supported a federal law to preempt any state or local medical privacy laws, it favored extremely weak federal legislation that would in some states supersede stronger local laws. Overall, the report offered little policy guidance to the many complicated issues it raised. The report differed from the AMA and APHA responses to

² The PPSC, however, did benefit from a draft report of a research project of legal scholar Alan Westin, titled *Computers, Health Records and Citizen Rights* (Ware, 1972–1977b).

the PPCS in the 1970s in form by advocating federal, not state, information privacy legislation but not in overall intent since it too opposed strong regulation.

The advent of the World Wide Web in the early to mid-1990s further accelerated the scale and scope of computer-based medical records systems. In 1996 the health care industry invested an estimated \$10 billion to \$15 billion in information technology (National Research Council, 1997). Public and media attention to potential misuse of medical records by both authorized and unauthorized individuals inside and outside of the medical profession grew. An increasing number of physicians became active in examining problems and potential solutions.

In 1995 the National Library of Medicine, the National Institutes of Health, the Massachusetts Health Data Consortium, and the National Research Council's Computer Science and Telecommunications Board initiated a study to define existing and potential future problems and to make policy recommendations regarding the protection of electronic health information. In 1997 this joint panel, composed primarily of physicians, recommended a number of new or more stringent technological procedures and organizational practices. The former consisted of greater use of authentication codes, physical security, and disaster recovery; protection of remote access points; and encryption of patient-identifiable information transmitted over public networks. Recommended organizational practices included development and enforcement of more explicit security and confidentiality policies, establishment of chief information security officers as well as security and confidentiality committees, and patient access to audit logs (National Research Council, 1997). This latter issue resonated deeply with some individuals and politicians who believed that the power of patients was increasingly being eroded in an era of widespread dissemination of health care through health maintenance organizations. These organizations often have demanded patient information on a wide scale to analyze the outcome and costs of different medical treatment plans and procedures (National Research Council, 1977). With the Clinton administration's focus on a patient bill of rights during his second term, the possibility for legislation to address medical records privacy appeared likely.

President Bill Clinton developed and proposed the first elaborate national standards for protecting patient privacy rights as part of the Health Insurance Portability and Accountability Act of 1996. Clinton's final ver-

sion of the privacy provision rules (called the Standards for Privacy of Individually Identifiable Health Information), scheduled to take effect on 14 April 2001, would have given patients greater rights to view, correct, and control disbursement of their medical data. Donna Shalala, the secretary of Health and Human Services under Clinton, described the task as "staggeringly complex." Clinton characterized the rules as the "most sweeping privacy protection ever written" (Shalala, 2002; Pear, 2001a, 2001c).

President George W. Bush, while not blocking the legislation, engaged in delay tactics and has revised the rules to provide far less information rights to patients. Bush's secretary of Health and Human Services, Tommy Thompson, has led the charge on the issue. Although he resolutely maintains Bush's commitment to medical privacy protection, he emphasizes the need to prevent unintended consequences that disrupt routine operations, overburden industry, and run the risk of harming patients or health care (Pear, 2001c). Behind the strong lobby of many sectors of the medical industry, the latter concerns seemingly have won out as Thompson announced Bush's proposal to rescind Clinton's key provision that doctors and hospitals would need to gain patient permission before disseminating records for the purpose of reimbursement or treatment (Pear, 2001b, 2002; Toner, 2001).

In effect, Clinton's introduction of sweeping new legislation just prior to leaving office and Bush's readiness to abandon key elements of it in light of potential burdens on the health care and related industries seem to be just one more chapter of discourse at the extremes and a reluctance to engage in a meaningful dialogue on costs and benefits. The Bush administration has been cautious about ignoring consumer patient privacy concerns, but nevertheless it supports the health care industry's position (Pear, 2001a). While the passage of Clinton's legislation in diluted form under the Bush administration does offer modest new hope toward better balancing of conflicting interests, the need for diverse and inclusive research and dialogue on the issue is more clear than ever. Computerized medical record information systems have been very beneficial to public health and epidemiology, as well as understanding and attacking skyrocketing medical care costs. Such systems can also inform doctors of prior conditions, allergies, and other pertinent medical information that a new patient forgets to disclose. Losses in patient privacy, however, have resulted, and a complex set of administrative

(e.g., appropriate patient identifiers, tight procedures on access, strict punishment for violations, proper positioning of computer monitors, and training programs on privacy issues) and technical (e.g., advanced encryption, close monitoring of access, and creation of audit trails of network use) solutions need to be used wisely to balance conflicting interests. Open debate has not occurred because entrenched and well-financed insurance lobbyists and privacy advocacy groups look at health records issues from the opposite ends of the spectrum. In essence, recent developments remind us that with rare exception (the National Research Council Study conducted in 1995 and 1996) such a dialogue has been nonexistent ever since the early work of the RAND Corporation and Willis Ware's leadership on the issue for the APDS Committee and the PPSC more than a quarter of a century ago.

References

- Agalides, E., & Swisher, S. (1964). The limitations in biological and medical data acquisition and processing. In K. Enslein (Ed.), *Data acquisition and processing in biology and medicine: Volume 3* (pp. 223–242). New York: Macmillan.
- Agre, P., & Rotenberg, M. (Eds.). (1997). *Technology and privacy: The new landscape*. Cambridge, MA: MIT Press.
- Arendt, H. (1958). *The human condition*. Chicago: University of Chicago Press.
- Automated Personal Data Systems Committee. (1973, July). *Records, computers, and the rights of citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education, and Welfare* (DHEW publication no. OS 73-94). Washington, DC: U.S. Government Printing Office.
- Baran, P. (1967). *Remarks on the question of privacy raised by the automation of mental health records*. Santa Monica, CA: RAND Corporation.
- Blum, B. I., & Duncan, K. (Eds.). (1990). *A history of medical informatics*. Reading, MA: Addison-Wesley.
- Collen, M. F. (1974). *Hospital computer systems*. New York: John Wiley & Sons.
- Corliss v. E. W. Walker*, Col., 57 Fed 434, C.C.D., 1893.
- Flaherty, D. (1972). *Privacy in colonial New England, 1630–1776*. Charlottesville: University of Virginia Press.
- Freudenheim, M. (2001, 8 January). Digital doctoring. *New York Times*, pp. C1, C4.
- Gallup Organization. (2000). *Public attitudes toward medical privacy*. Princeton, NJ: Gallup Organization. [Submitted to the Institute for Health Freedom].
- Griswold v. Connecticut*, 381 U.A. 479, 1965.
- Hubbard, H. C. (1972). Hazards of medical computing. *Lancet*, 2(7775), 489–500.
- Institute of Medicine. (1994). *Health data in the information age: Use, disclosure, and privacy*. Washington, DC: National Academy Press.
- Ledley, R. S. (1965). *The use of computers in biology and medicine*. New York: McGraw-Hill.
- Lusted, L. B. (1968). *Introduction to medical decision-making*. Springfield, IL: Charles C. Thomas.
- Mensel, R. E. (1991, March). "Kodakers lying in wait": Amateur photography and the right to privacy in New York, 1885–1915. *American Quarterly*, 43, 24–45.
- Miller, A. (1971). *The assault on privacy: Computers, data banks, and dossiers*. Ann Arbor: University of Michigan Press.
- National Research Council, Computer Science and Telecommunication Board. (1997). *For the record: Protecting electronic health information*. Washington, DC: National Academy Press.
- Pear, R. (2001a, 13 April). Bush accepts rules to protect privacy of medical records. *New York Times*, p. A1.
- Pear, R. (2001b, 12 February). Medical industry lobbies to rein in new privacy rules. *New York Times*, p. A1.
- Pear, R. (2001c, 27 February). Health secretary delays medical records protections. *New York Times*, p. A18.
- Pear, R. (2002, 22 March). Bush acts to drop core privacy rule on medical data. *New York Times*, p. A1.
- Privacy Act, 5 U.S.C. 552a (1974).
- Right to privacy and medical computing: Transactions of the convergence on the use of computers in clinical medicine*. (1969). Buffalo: State University of New York at Buffalo.
- Roe v. Wade*, 410 U.S. 113, 1973.
- Shalala, D. E. (2002, 30 March). A loss of medical privacy. *New York Times*, p. A27.
- Sykes, C. J. (1999). *The end of privacy: Personal rights in the surveillance society*. New York: St. Martin's Press.
- Tange, H. J., Hasman, A., Robbe, P. F., & Shouten, H. C. (1997). Medical narratives in electronic medical records. *International Journal of Medical Informatics*, 46, 7–29.
- Toner, R. (2001, 20 June). Debate on patients' rights sends lobbyists into battle. *New York Times*, p. 1.
- Turn, R. (1972). *A brief history of computer privacy/security research at RAND*. Santa Monica, CA: RAND Corporation.
- Ware, W. H. (1970). *Computer data banks and security controls*. Santa Monica, CA: RAND Corporation.
- Ware, W. H. (1971). *Computers in society's future*. Santa Monica, CA: RAND Corporation.
- Ware, W. H. (1973). *Data banks, privacy, and society*. Santa Monica, CA: RAND Corporation.
- Ware, W. H. (1975). *Legislative issues surrounding the confidentiality of health records*. Santa Monica, CA: RAND Corporation.
- Ware, W. H. (1976). *State of the Privacy Act: An overview of*

- technological and social science developments*. Santa Monica, CA: RAND Corporation.
- Ware, W. H. (1977). *Privacy and patient rights*. Santa Monica, CA: RAND Corporation.
- Ware, W. H. (1981, 19 January). Oral history, conducted by Nancy Stern, Santa Monica, CA. Charles Babbage Institute, University of Minnesota.
- Ware, Willis H. Papers. (1972–1977a). Automated Personal Data Systems (APDS) records, 1972–1973, Proceedings of committee meetings, CBI 40. Charles Babbage Institute, University of Minnesota.
- Ware, Willis H. Papers. (1972–1977b). Privacy Protection Study Commission (PPSC) records, 1975–1977, meeting transcripts, CBI 40. Charles Babbage Institute, University of Minnesota.
- Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4, 193–200.
- Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.
- Yost, J. R. (2002). *A bibliographic guide to scientific computing, 1945–1975*. Westport, CT: Greenwood Press.

