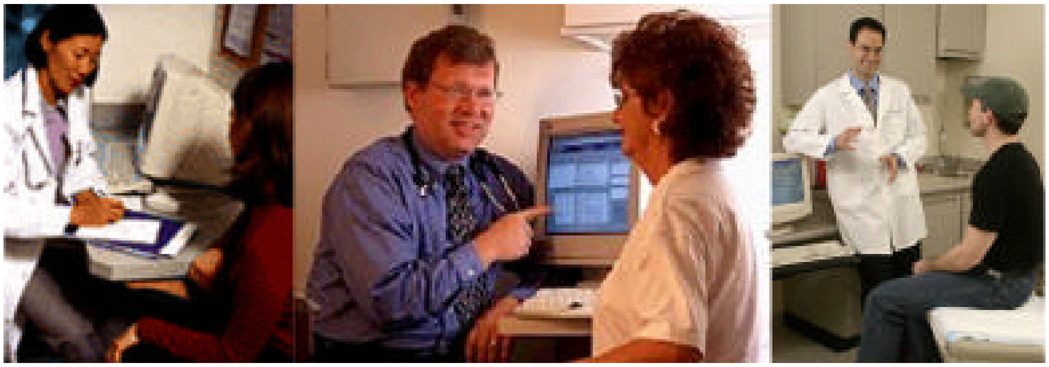
Building Privacy by Design In Health Data Systems



A Report By
The Program on Information Technology, Health Records and Privacy
of the Center for Social and Legal Research

Prepared by:
Dr. Alan F. Westin and Vivian van Gelder

August 2005

Contact Information: Tel. 201-996-1154 Fax 201-996-0488
email: ctrslr@aol.com Dr. Westin's direct email: alanrp@aol.com

CONTENTS

EXECUTIVE SUMMARY

Background: The Program on Information Technology, Health Records and Privacy

This Report is the first in a series of studies by a new program at our Center for Social and Legal Research – The Program on Information Technology, Health Records, and Privacy.

We prepared this report because we believe that this decade will see fundamental changes in the ways that personal medical records and health information are collected, used for health care services and payments, and transferred for use in other important organizational processes of our society. The Electronic Health Records (EHR) and health data networking efforts currently underway suggest that these changes will be implemented in the near term, and at a rapid rate.

However, based on historical experience, we also believe that unless the privacy and data security aspects of this transforming shift are addressed now, at the "front end", this entire venture could be compromised - if not stillborn - because of potential public resistance to computerization without adequate privacy safeguards.

A History and Analysis of IT Efforts and Privacy Issues in U.S. Health Care, 1960s to the Present

The concept of health data computerization and networking has a long and venerable history – a history that contains valuable precedents and a wealth of knowledge that can be applied to today's efforts in this area.

From its first appearance in 1960, to the present day, there have been three identifiable waves, or phases, of efforts to develop and implement health IT: 1960-1979; 1980-2000; and 2001-Present. In the first two of these phases:

- IT failed to achieve the significant penetration, coordination and positive effects in health care that occurred in other major sectors of U.S. business and governmental life.

- Survey research found that the public was generally comfortable with the handling of their health information by doctors and hospitals, but was deeply worried about how their personal medical information was being accessed and used in other sectors, for secondary purposes such as insurance, employment, licensing, research, law enforcement, public health, and media activities.

- A series of detailed technology-privacy impact assessments were carried out by various government, private, and academic projects. These described the potential but still unrealized benefits of IT applications for the health sector; analyzed the impediments for adopting IT applications; confirmed the critical aspects of privacy protection for patient trust and self-disclosure in health encounters; documented the absence of an adequate legal structure for health care privacy; and called for the development of an adequate legal framework of privacy rules in preparation for planned major IT roll outs in the health sector.

· Proposals for health care privacy laws were offered but not adopted, either as federal rules or comprehensive state laws, despite these recommendations. Generally, the failure to create a comprehensive legal structure to protect health privacy was a function of U.S. interest group and political processes, and the sectoral rather than comprehensive approach of the U.S. toward national privacy legislation.

What is New About the Current IT Efforts in Health Care

Since 2001, a number of developments have significantly altered the health IT implementation landscape, including:

- the arrival of more powerful, reliable and cost-effective hardware and software tools to support EHR and data network proposals in health care settings;

- a greater readiness among health care professionals and staffs to embrace and use information technology to manage their daily workflow;

- the emergence of a broad consensus among all of the key policy players that clear and strong privacy standards must be identified and adopted as part of any EHR and data network national program;

- an explosion in 2004-2005 of incidents involving leakage and compromise of personal medical records from health providers, against a national backdrop of rapidly rising identity theft and fraud - creating an environment in which 2005 surveys show the public almost evenly divided on whether the benefits of further computerization and networking in health care are likely to outweigh their potential risks to privacy.

What Needs to be Done

In this new environment, our Program believes that those leading the current efforts to digitize and network health records must act now to incorporate appropriate, responsive privacy protections in the design of those records and networks.

The technology-privacy impact assessments undertaken in previous eras provide extremely valuable tools for a “Privacy by Design” approach to current system development. Although these assessments dealt with earlier technologies, their techniques and methodologies – along with many of their insights - remain pertinent today.

Drawing on this long tradition of health information technology-privacy impact assessments, we argue that a Privacy by Design approach should:

- conduct detailed empirical research into how current and planned EHR and network applications affect the scope of data collection, the use and confidential handling of personal data within the care settings, the handling of payments and administrative oversight, and provision of personal health data to secondary users, in order to test whether the assumed benefits of these applications are being realized, and whether they enhance patient knowledge and use of privacy rights.

- conduct surveys of patient populations and the public to track perceptions of the benefits of EHR operations for patient care, and of organizational privacy and data security practices, using online and other survey techniques that permit collection of valuable narrative accounts;

- apply the prevailing U.S. Fair Information Practices standards to the new EHR and networking programs, going beyond the HIPAA Privacy Rule in several key areas;

- develop a strong multi-strategy approach to assuring greater data security in an EHR environment (while recognizing that total security can never be assured);

- monitor any changes in access by secondary-user organizations to computerized medical records, and open policy debates about increased controls or limits where any such changes breach acceptable privacy or equality standards.

In order to assure a hearing for alternative values and judgments, we believe that there should be multiple assessments performed along these lines by a variety of governmental, academic, industry, and public-interest organizations.

Conclusions

We recognize that balancing privacy with public disclosure and societal protection interests is a complex and difficult process – especially in the health care field – and that merely calling attention to the importance of protecting privacy will not ensure that it is done appropriately or well. We have tried to spell out in this Report both the principles and the processes that we see as needed to mount an effective Privacy by Design effort for EHR and data networking programs.

Accompanying that Privacy by Design effort should be a major educational campaign to inform the public about EHR developments and their key privacy and data security choices, along with creative efforts to involve the public in EHR privacy assessments and policy developments at local and national levels.

PREFACE

The Program on Information Technology, Health Records and Privacy

The Program on Information Technology, Health Records and Privacy was initiated in January, 2005. A description of its activities to date, its available materials, and its Staff appears in the Appendix to this document.

Creation of the Program reflects my sense – as someone who has worked on issues of health care and privacy since the late 1960s – that this decade will see fundamental changes in the U.S. health care information system. However, if patient and public acceptance of EHR and data networking programs is to be achieved, the privacy and data security aspects of this transforming shift must be addressed now – at the front end of IT application efforts.

With this perspective, our Program commissioned and developed a national public opinion survey in February, conducted by Harris Interactive, on public attitudes toward EHR programs and Privacy. I reported the survey findings in testimony in February before various HHS committees and presented our analysis of privacy issues in the EHR context at conferences this spring, such as the AHRQ Annual Meeting in June.

This Report

In February, we began preparing this Report, which is now in is Third Draft and ready to publish.

While my colleague, Vivian van Gelder, and I have signed off on this report in early September, 2005, we are aware that hardly a week goes by without important new developments, studies, and debates over EHR and Networking initiatives. Therefore, we plan to update this first Program Report on a regular basis, and make the updating available to all interested parties on our Center's main web site -– www. privacyexchange.org

Therefore, we invite readers of this to give us reactions, criticisms, and suggestions, and we promise to use valuable inputs in our updates.

ALAN F. WESTIN
Program Director

I. INTRODUCTION: PRIVACY AND THE "DECADE OF HEALTH NETWORKING"

On April 27, 2004, President George W. Bush signed Executive Order 13335, "Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator." Launching a proposed "Decade of Health Networking", the Executive Order urges that electronic health records be made available for every American within ten years, and envisions the development of a "nationwide interoperable health information technology infrastructure" that would make these records available to health care providers, public health agencies and health researchers nationwide.

While – as this paper will show -- the concept of health data networking has a venerable history, much of the present effort is driven by a growing sense among observers and experts that, over a decade after the failure of the Clinton Health Security Plan, the American system of health care delivery is rapidly approaching crisis point. Health care costs are spiraling out of control,[1] while a "huge and growing" number of Americans have limited access to care[2] whose quality has, in any case, been described as "substandard"[3]. (Medical errors are, for example, now believed to be the third leading cause of death in the United States.)[4]

These developments have not escaped the notice of the American public: a 2004 survey showed that up to 55% of American adults are dissatisfied with the quality of health care they receive, up from 44% in 2000; four in ten believed that health care quality had declined over the previous five years.[5] Increasingly, the automation and linkage of health records, fragments of which are currently quarantined in "silos" across a decentralized health system of unparalleled complexity, is thought to present a promising way to "avoid dangerous medical mistakes, reduce costs, and improve care"[6] – an outcome also foreseen by one in two Americans, who believe that, after better

[1] The U.S. has the world's most expensive health care system, with spending currently at 15% of GDP - more than double the OECD average. See U.E. Reinhardt, P.S. Hussey, G.F. Anderson, "U.S. Health Care Spending In An International Context," Health Affairs, May/June 2004, Vol. 23(3):10

[2] In 2003, some 45 million Americans (including 8 million children) were without health insurance for all or part of the year. See DeNavas-Walt, Proctor, and Mills, U.S. Census Bureau, Current Population Reports, P60-226, *Income, Poverty, and Health Insurance Coverage in the United States: 2003*, U.S. Government Printing Office, Washington, DC, 2004

[3] National Coalition on Health Care, *Building a Better Health Care System: Specifications for Reform* (Washington, D.C., July 2004). The U.S. now ranks toward the bottom among OECD countries on leading health indicators such as disability-adjusted life expectancy and infant mortality. See Bureau of Labor Education of the University of Maine, "The U.S. health care system: Best in the world, or just the most expensive?", 2001 (available at http://dll.umaine.edu/ble/U.S.)

[4] B Starfield, "Is US Health Really the Best in the World?" Journal of the American Medical Association, Jul 26, 2000; 284(4):483-5

[5] Kaiser Family Foundation, Agency for Healthcare Research and Quality, and Harvard School of Public Health, *The National Survey on Consumers' Experiences With Patient Safety and Quality Information*, published November 17, 2004

[6] President's State of the Union Address, January 20, 2004

communication and quality control, greater use of computerized medical records would reduce preventable medical errors.[7]

In the year that has passed since Executive Order 13335, the momentum for creation of a nationwide patient records network has increased rapidly. Experimental health records networks have recently been proposed or launched by private sector groups and companies. Both houses of Congress have produced a number of bipartisan bills aimed at creating a supportive environment for health record networking. The position of National Coordinator for Health Information Technology has been created within the Department of Health and Human Services, and in June 2005, HHS launched the American Health Information Community, a public-private collaborative body charged with setting standards for health records interoperability.

This surge in momentum comes after over a decade of stalled efforts to get a nationwide health records network off the ground, a task made Herculean by the very low rate of patient record computerization in hospitals and doctors' offices. Surveys show that up to 87% of hospitals and between 72% and 86% of physician practices were still operating with paper-based patient record systems in 2002.[8] In addition, those patient data systems that *are* in current use are not deployed in a coordinated way; the typical American hospital, for example, is said to have "more than 200 different information system applications, few of which work together".[9] As such, wholesale computerization and networking of medical records would represent a very significant change in the way that health data is currently handled in the United States.

Clearly, a change of this magnitude will have significant implications for the protection of patient privacy, and indeed at present there is virtually unanimous agreement that preserving privacy in a fully networked health data system is of the utmost importance. But it will be difficult, if not impossible, to create appropriate privacy protections without first identifying the changes wrought by networking on patient data handling in real-world settings. Having done so, it will then be possible to assess the impact of these changes on patient privacy, and to consider whether existing laws and policies are likely to be adequate to address any adverse impacts.

We submit that the potentially serious impacts of health data networking on individual privacy cannot be meaningfully addressed in the absence of such a process. Without a careful and deliberate assessment, the development of privacy protections must proceed in an ad hoc, reactive manner incapable of addressing unexpected results, and ultimately requiring much expensive and difficult "retrofitting". In fact, because the concept of automated and networked health data has a long history, there already exists a valuable body of research on the impacts of information technology on individual health privacy. This paper will draw on this body of research, and will suggest ways in which it

[7] Kaiser Family Foundation et. al. *id*.
[8] "E-records vital to health strategy", Federal Computer Weekly, August 2, 2004
[9] Microsoft Healthcare and Life Sciences Division, "Electronic Health Records Solutions for Healthcare Providers"

might profitably be adapted to the present effort to create a nationwide network of patient data in the United States.

II. HEALTH NETWORKING AND PRIVACY IN HISTORICAL CONTEXT

The concept of a fully automated and networked system of patient information can be traced back more than four decades, to the dawn of the modern computer age. The forty-five years since health data automation and networking was first proposed can be divided into three major phases. The first of these comprises roughly the period between 1960 and 1979, when automation was first proposed and Congress considered and then abandoned a national health scheme. The second encompasses the two decades from 1980 through 2000, when networking technology reached full maturity in the context of yet another failed proposal for national health reform. The third consists of the period since 2001, during which a consensus has emerged that, since national health reform is unlikely in the near term, health IT implementation depends on collaboration between the private and public sectors.

The steady growth and application of health information technologies during the first two phases was accompanied by exhaustive and in-depth assessments by researchers of their actual effects on the use and disclosure of personal health information, along with public reactions to these new health data use patterns. These studies provided valuable guidance to policymakers seeking to determine whether existing laws and regulations properly addressed the privacy implications of technology-driven changes in personal health data handling. Many of the issues identified by these studies remain urgent and pressing even today, and as a result, many of the policy proposals they put forward continue to be relevant to the current environment.

A. Phase One: 1960 – 1979

(1) Technology and practice

With the arrival of third generation computers and remote access terminals, and the invention and refinement of the integrated circuit chip, the computer emerged during the decade of the 1960s as a feasible tool for data processing and storage. The invention of the Intel 4004 microprocessor in 1971 and the commercial release of “personal computers” by IBM and Apple ushered in the era of desktop computing, though they never became widespread during this period. Most computing power was deployed via large, expensive mainframes owned by governments, universities and large businesses. Although the capability and diffusion of information technology was limited during this period, nonetheless its capacity to effect revolutionary change in many of the foundational structures of society – including the delivery of health care - was widely recognized and debated.

The concept of an electronic health information network emerged very early, with the 1960 publication by Drs. R.S. Ledley and L.B. Lusted of what is generally considered to be the seminal paper in the field of medical informatics.[10] In that paper, the authors envisioned a "network of connected computers communicating with hospitals and physicians within a geographic area, all receiving, processing and transmitting medical information as required"[11] to support care provision, including computer-aided diagnosis, as well as clinical research. That same year, the National Institutes of Health established a Health Advisory Committee on Computers in Research, and a number of leading colleges and universities began to offer "Life Sciences Computer Resources" programs of study.[12]

Another landmark was the 1969 proposal by Dr. Lawrence L. Weed and his associates at the University of Vermont College of Medicine of the first computer health record format. The Problem-Oriented Medical Record consisted of a set of standard inputs intended to enable an interoperable electronic patient record with built-in clinical decision support, and forming part of a computer-based Problem-Oriented Medical Record System (PROMIS).[13] PROMIS was quickly followed by other computerized health record formats with clinical decision-support functions, such as the Regenstrief Medical Record System and the University of Utah's HELP (Health Evaluation through Logical Processing) program.[14]

The advancing potential for automated management of patient information spurred the launch of a number of computerized patient data-processing projects during this period in health care facilities across the nation.[15] These included Harvard Community Health Plan's COSTAR (Computer Stored Ambulatory Record) System, which began in 1971 and was extensively deployed at nearby Massachusetts General Hospital; and similar projects at Yale-New Haven Medical Center, Emory University's Grady Memorial Hospital, Johns Hopkins Hospital in Baltimore, and at California's pioneering pre-paid group practice, Kaiser Permanente.

(2) The assessments

· *(a) 1972: Databanks in a Free Society*

Among the earliest empirical assessments of the extent and effects of computing on health care was a landmark study undertaken in the early 1970s by Alan F. Westin and Michael A. Baker as part of the National Academy of Sciences Project on Computer Databanks. One section of Westin and Baker's 1972 report, *Databanks in a Free Society: Computers, Record-Keeping and Privacy*, assessed medical record-keeping practices at

[10] "The use of electronic computers in medical data processing: aids in diagnosis, current information retrieval, and medical record keeping," IEEE Transactions in Medical Electronics (1960), Volume 7, 31

[11] MF Collen, *Informatics: A History of Medical Informatics in the United States: 1950 to 1990*, American Medical Informatics Association, Bethesda, MD, 1995; at 149

[12] R Jenders, R Sideli, G Hripcsak, "Introduction to Medical Informatics" Columbia University, 1998

[13] M Collen, *Id.*

[14] JR Yost, "Reprogramming the Hippocratic Oath: A Historical Examination of Early Medical Informatics and Privacy", in *The History and Heritage of Scientific and Technological Information Systems* (Information Today for Chemical Heritage Foundation and American Society of Information Science, New Medford, New Jersey 2004), 49

[15] Collen, *id*, at 184

American hospitals, health insurance companies, local and state government health agencies, employee medical departments in private companies and public agencies, and medical services in schools and universities.

Westin and Baker found that that the high costs associated with digital data storage were retarding the computerization of full patient records, with their reliance on space-consuming narrative data. Physician reluctance to invest extra time in learning to operate a new data entry system was also a factor in low rates of computerization. As a result, in the health sector in general, computerization had advanced furthest in non-narrative medical records not compiled by physicians, such as "hospital accounting and billing operations," and "laboratory reporting, patient admissions and scheduling".[16] The study found that computerization in these areas had not significantly altered existing patterns of health data processing.

This was the case even in pioneering institutions such as the pre-paid Kaiser Permanente Health Care Program, which at the time was running a pilot program to test the feasibility of real-time computer record creation, through the integrated storage of patient data that Kaiser was already digitally recording and storing. Included in Kaiser's prototype electronic health records were "hospital and clinical diagnoses, results of all laboratory tests, X ray, pathology and electrocardiographic examinations, and data concerning all drugs dispensed or administered." Even so, Westin and Baker found that "the computer medical record system [had] had a small impact so far on [Kaiser's] general record keeping practices."[17]

However, the study also found that, while progress on digitizing medical records had been slow, certain trends in the health care field were likely to create pressures for computerization in the future. These trends were already raising questions among health professionals about "what kinds of protections exist or should exist in medical data systems" to maintain the confidentiality of patient records.[18] Professionals noted that confidentiality in existing manual records was particularly difficult to protect when those records "passed into the hands of nonmedical institutions" for purposes such as "insurance underwriting and claims processing, hospital accreditation and other regulatory and law-enforcement activities, and for health department monitoring of communicable diseases".[19] Unlike health care providers, most of these non-medical users were not subject to any legal requirement to preserve the confidentiality of patient data.

Westin and Baker found that these concerns needed to be addressed in order to protect patient record confidentiality as computerization progressed. They noted that, in the absence of "new laws, public protests, or pressures from within," organizations tended to retain existing policies and practices as they moved to computerize their health record systems. As a result, there was little incentive for those who had not dealt with confidentiality issues within their manual record systems to do so during the

[16] AF Westin and MA Baker, *Databanks in a Free Society* (1972), at 204
[17] *Id*, at 209
[18] *Id*, at 204
[19] *Id*, at 204

computerization process. Westin and Baker therefore called for an immediate public "re-examination" of data policies "without regard to whether the storage and processing medium was manual or automated." After that, "special rules" could be formulated for the protection of confidentiality in automated files.

· *(b) 1976: Computers, Health Records and Citizen Rights*

In 1974, the earliest specific study of the impact of computers on patient privacy was launched by the National Bureau of Standards and the National Association for Computing Machinery, under the direction of Alan F. Westin. The 1976 report of the study, *Computers, Health Records and Citizen Rights*, exhaustively documented patterns of record-keeping about people in health care field prior to automation, and undertook case studies of health data computerization in six organizations to observe the effects of health data computerization on these patterns and, subsequently, on citizen rights. The study then considered effective ways to protect the confidentiality of patient data in the light of these empirical findings.

The study used an innovative "three-zone" schema to identify and assess patterns of health data processing. Zone 1 encompasses the context of Direct Patient Care, in which medical records are created when a patient seeks health care, and in which "the cycle of medical record-keeping usually begins". Zone 2 comprises Supporting and Administrative Activities, including government and private service payers and professional and government quality care reviewers. Finally, Zone 3 consists of Secondary Use of personal health data by Social Users, such as employers, life insurers, licensing authorities, the judicial process, the media, public health reporting, law enforcement, medical research and social welfare programs .

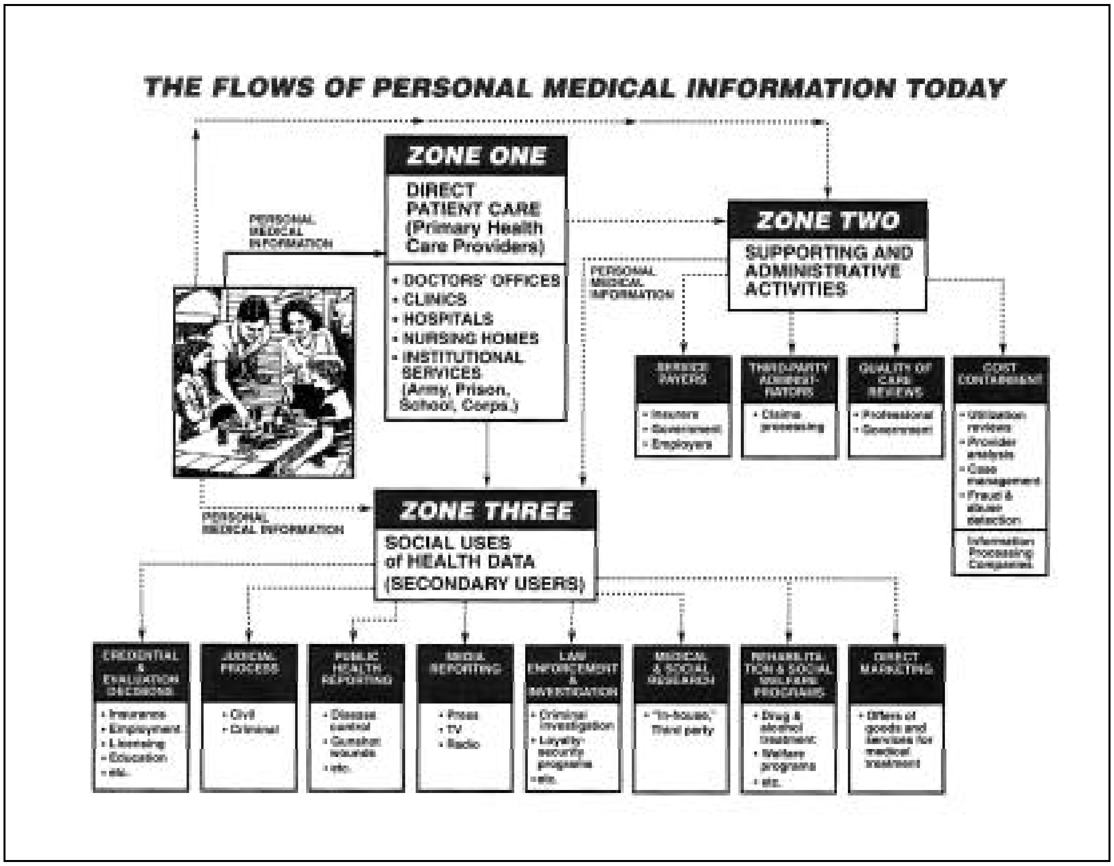

THE FLOWS OF PERSONAL MEDICAL INFORMATION TODAY
ZONE ONE
DIRECT PATIENT CARE (Primary Health Care Providers)
• DOCTORS' OFFICES
• CLINICS
• HOSPITALS
• NURSING HOMES
• INSTITUTIONAL SERVICES (Army, Prison, School, Corps.)
PERSONAL MEDICAL INFORMATION
ZONE TWO
SUPPORTING AND ADMINISTRATIVE ACTIVITIES
SERVICE PAYERS
• Insurers
• Government
• Employers
THIRD-PARTY ADMINISTRATORS
• Claims processing
QUALITY OF CARE REVIEWS
• Professional
• Government
COST CONTAINMENT
• Utilization reviews
• Provider analysis
• Case management
• Fraud & abuse detection
Information Processing Companies
PERSONAL MEDICAL INFORMATION
ZONE THREE
SOCIAL USES of HEALTH DATA (SECONDARY USERS)
PERSONAL MEDICAL INFORMATION
CREDENTIAL & EVALUATION DECISIONS
• Insurance
• Employment
• Licensing
• Education
• etc.
JUDICIAL PROCESS
• Civil
• Criminal
PUBLIC HEALTH REPORTING
• Disease control
• Gunshot wounds
• etc.
MEDIA REPORTING
• Press
• TV
• Radio
LAW ENFORCEMENT & INVESTIGATION
• Criminal investigation
• Loyalty-security programs
• etc.
MEDICAL & SOCIAL RESEARCH
• "In-house," Third party
REHABILITATION & SOCIAL WELFARE PROGRAMS
• Drug & alcohol treatment
• Welfare programs
• etc.
DIRECT MARKETING
• Offers of goods and services for medical treatment

Figure 1: The Three Zones of Personal Health Information Use

The 1976 study began with a zone-by-zone assessment of the pressures on confidentiality of patient data within existing manual record systems. It found significant pressures on health record privacy in all three zones, with Zone 3 or "secondary" uses of health information raising "the sharpest clash between society's interest in protecting medical confidentiality and its interest in a wide variety of other important functions."[20] The study then turned to assess the likely effects of automation on these existing pressures. It found that, while computerization in the health sector had "not been as extensive as in fields such as banking, law enforcement or taxation," it was "growing steadily in use and sophistication", and for this reason warranted a detailed evaluation.[21]

To this end, the study evaluated real-world experiences in automating patient data at six public and private sector institutions drawn from each of three "zones" of health data. Four of these were Zone 1 users: the L.A. County Medical Center, the Martin Luther King Jr. Medical Center (Bronx, NY), the Kaiser Permanente Medical Program, and the U.S. Indian Health Service. One, the Mutual of Omaha Insurance Company, was

[20] *Computers, Health Records and Citizen Rights* (1976), at 60
[21] *Id*, at xi

a Zone 2 health insurer, while the remaining entity - the Multi-State Information Service, a public system of automated psychiatric patient records – fell into Zone 3.

The study found that the effects of automation on confidentiality were largely dependent on choices made by the automating organization, rather than on the technology itself.[22] Organizations "for the most part [were] simply carrying over into computerized files the same practices pursued with manual records",[23] so that those that did not have existing strong privacy policies did not introduce them during the automation process, absent external pressures (such as patient protest, provider concern, media interest or legislative or regulatory requirements) to do so. As a result, many automation efforts were going ahead without sufficient consultation with patient and provider groups, leading to the creation of "ambiguous and ill-defined systems that leave people uncertain and fearful about their capacity to control the circulation" of their health data.[24]

Because computerized medical records were "more detailed, more centralized, more permanent, [and] more easily-transmissible" than manual records, the study predicted that existing "flawed policies and procedures", where they persisted, were very likely to be "seriously inadequate" for managing patient privacy issues in the computer era. The study concluded that "no single law, judicial ruling, regulatory action, or organizational policy can hope to deal with the tremendously varied and complex issues of citizen rights in health record-keeping; it will take a mosaic of policy actions, over time, to do what is needed". It set out twelve basic principles that should apply to the "management of data systems in the health field":

- A public notice and privacy impact statement should be issued and filed with an appropriate public authority whenever an automated health database is created;

- "Socially acceptable standards of relevance and propriety" in the collection of personal data in each of the three zones of health data use should be established, through "public discussion and appropriate policy setting mechanisms";

- Individuals should be given a "clearly written account of how their (health) information will be used", along with the procedures to be followed when other uses for that information are contemplated;

- Authorization forms used for releases of health data should be narrowly and specifically tailored, describe the data to be released in detail, limit the release in time, and require voluntary and informed consent;

- Individuals should be assured a general right of access to their health information (with an absolute right to know what information will be released for non-health purposes);

[22] *Id*, at xii
[23] *Id*, at 117
[24] *Id*, at 245

- Health data should be kept accurate, up-to-date and complete;
- Data security measures appropriate for the protection of highly sensitive personal information should be employed;

- Database-using staff should be required to undergo orientation and training in handling automated health data in such a way as to protect citizens' rights;

- A patients' rights handbook should be produced and distributed for each automated health data system, and an independent and accessible patients' rights representative appointed;

- Policy measures should be taken to ensure that health privacy considerations are not misapplied in order to reduce public access to government information (e.g., under FOI obligations); and

- Special measures should be implemented to ensure that health care quality assessments and clinical research can be performed without infringing on citizens' rights.

The study also developed a Voluntary Fair Information Practices Code which was sent by NBS to every hospital in the nation. Elements of the Code were adopted by many hospitals in the 1970's and 80's, while efforts to enact a federal health privacy law were being pursued (*see below*).

- ***(c) 1977: Personal Privacy in an Information Society***

In 1977, Congress appointed the Privacy Protection Study Commission, with Dr Alan Westin as its chief consultant, to inventory the standards and procedures in force nationwide for the protection of personal information in "data banks, automatic data processing programs, and information systems of governmental, regional, and private organizations," with a view to assessing whether the application of the Privacy Act of 1974 should be extended beyond the Federal Executive branch.

The Committee reviewed the previous findings on changing patterns of health data use, and reached "six basic conclusions":

1. That medical records now contained more information and were available to more users than ever before;

2. That social and economic pressures had "greatly diluted" the "control medical-care providers once exercised over information in medical records";

3. That, due to the increasing importance to both the individual and society of Zone 2 and Zone 3 access to medical-record information, the "comparative insulation of medical records from collateral uses . . . cannot be entirely restored";

4. That because access to an increasing number of vital social benefits was conditioned on the provision of health data, the concept of "freely given" consent to disclosure of medical record information had "less and less meaning";

5. That despite its growing impact on their fundamental rights, patients continued to lack the right to see, copy or check the accuracy, timeliness or completeness of information in their medical records;

6. That steps could and should be taken to (a) improve the accuracy, timeliness and completeness of medical record information; (b) improve the patient's awareness of the content and uses of his or her medical record information; and (c) to control the amount, type and conditions under which such information was disclosed to others.

On the basis of these conclusions, the Committee proposed a set of fourteen recommendations aimed at "minimizing intrusiveness, maximizing fairness, and creating a legitimate, enforceable expectation of confidentiality", with emphasis outside, rather than inside, the medical-care relationship (i.e. in Zones 2 and 3, rather than in Zone 1).

The Committee's proposals included the creation of a patient right to access, correct, and supplement his or her medical record data; obligations to safeguard against unauthorized medical record disclosure; a prohibition on disclosure of health data without patient authorization, except under certainly narrowly defined circumstances; an obligation to account to the patient for all disclosures of his or her health information; and the creation of a criminal offense of obtaining medical records through deception or false pretences.

(3) Public perceptions of health privacy issues

In 1978, Louis Harris & Associates and Dr. Alan Westin undertook the first detailed national survey of attitudes towards privacy. *The Dimensions of Privacy* measured American attitudes toward privacy across a broad spectrum of contexts, including the handling of personal health information by doctors and hospitals.[25]

The survey found that doctors were rated the least intrusive of the eighteen organizations and individuals on which attitudes were tested. Only 11% of Americans felt that doctors asked for too much personal information, while 84% felt that doctors appropriated limited their demands for such information to what was strictly necessary. (Hospitals were twice as likely to be criticized, with a rate of intrusiveness – 24% - equal to that attributed to local police.)

Doctors (and hospitals) were also the least criticized of all eighteen groups and individuals tested regarding their efforts to keep patients' information confidential; only 17% felt that doctors "should be doing more" to protect confidentiality, while 75% felt

[25] *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy,* Conducted for Sentry Associates by Louis Harris & Associates and Dr. Alan F. Westin (1978)

that they were already “doing enough”. Some 23% felt that hospitals could do more to protect their information, while 66% considered that their efforts were sufficient. (Interestingly, 30% of doctors themselves felt that the profession could make improvements in this area.)

The survey identified strong support for the passage of Congressional legislation to protect medical and health privacy, with 65% of respondents agreeing that the passage of such legislation was “important”. In addition, there was strong public support for a legal right of access to one’s medical record, with 91% of respondents agreeing that patients should have a legal right to see their health records held by doctors and hospitals.

(4) Developments in health privacy regulation

That health care would in future be provided centrally by government-run programs seemed highly likely in the 1970s. Medicare and Medicaid had both been launched in 1965, and in 1973, President Richard M. Nixon said “comprehensive health insurance is an idea whose time has come.” The creation of government databases in other areas (such as the FBI’s National Criminal Information Network, in 1971) suggested that a national health system would be accompanied by vast government-operated computer databases of patient information.

At the same time, the political turmoil of the late 1960s and early 1970s had created unprecedented levels of public distrust of government, and the concept of government databases of personal information generally raised strong concerns. In 1972, in an attempt to address these concerns, the Secretary of the federal Department of Health, Education and Welfare (the precursor to today’s HHS) established an Advisory Committee on Automated Personal Data Systems in an effort to address “growing public concern about unregulated applications of computer technology to the government’s acquisition, storage, and dissemination of data on U.S. citizens.”[26]

The Committee’s July 1973 report on the “impact of computer-based record keeping on private and public matters” found that “under current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices.”[27] It recommended Federal legislation to enact an enforceable Code of Fair Information Practices that would apply to “all automated personal data systems.” The Code consisted of five principles:

- There must be no personal data record keeping systems whose very existence is secret.

- There must be a way for an individual to find out what information about him is in a record and how it is used.

[26] JR Yost, *id*, at 50
[27] Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens*: *Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973)

- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

- There must be a way for an individual to correct or amend a record of identifiable information about him.

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

These principles were incorporated into the Federal Privacy Act, which was passed in 1974, The Act applied only to the federal public sector; it did not regulate state activity, nor automated personal data processing by private sector persons or bodies.

Following the 1977 report of the Privacy Protection Study Committee, President Jimmy Carter pressed for the passage of comprehensive Federal health data privacy legislation that would apply beyond the federal public sector.[28] In 1980 Congress considered the *Federal Privacy of Medical Information Act.* The bill would have applied health data handling rules to "medical care facilities such as hospitals and clinics," but would not have extended to individual practitioners. It was opposed by both the American Medical Association and the American Hospital Association, which preferred that the issue be left to the states rather than legislated at the Federal level.[29] After Congress failed to pass the bill, the momentum for passing a comprehensive national health data privacy law faded. It would not be revived for over a decade.

B. Phase Two: 1980 - 2000

(1) Technology and practice

During the 1980s, the personal computer became a common business tool; by the end of the decade, individual desktop computers could be linked together in Local Area Networks. The decade of the 1990s witnessed a technological explosion that resulted in the World Wide Web, increasing access to e-mail, wireless handheld computing, and the spread of large-scale "data mining". These technological advances led to rapid networking within industry sectors such as finance, and laid the basis for an explosion in electronic commerce. They also provided the basic structure for a nationwide system of electronic health data, but for a variety of non-technical reasons, automation and networking proceeded much more slowly in the health sector than in other sectors during the period.

[28] J Yost, *id*.

[29] R Gellman, "Politics, Policy, and Technology: Perspectives on Proposals for Federal Health Confidentiality Legislation in the United States," paper presented at *Visions for Privacy in the 21st Century: A Search for Solutions*, Victoria, British Columbia, May 9 - 11, 1996

The prospects for widespread health data automation and networking looked bright in the early 1990s, when the Institute of Medicine (IOM) of the National Academy of Sciences published a highly influential report, "The Computer-Based Patient Record: An Essential Technology for Health Care".[30] The report noted the "lack of diffusion of information management technologies in the health care sector," and called on the health sector to "adopt the computer-based patient record as the standard for medical and all other records related to patient care."[31] The report found that automated records could potentially enhance quality and reduce costs by supporting a variety of uses within and between all three Zones, such as in-hospital and ambulatory health care delivery, management and review of care, reimbursement of care, research, education, accreditation and policymaking.

In order to promote the development of an automated health record system, the IOM proposed the establishment of a Computer-based Patient Record Institute to draft "uniform national standards for data and security", and to create "model legislation and regulations to facilitate the implementation and dissemination" of automated health records. In 1992, acting on the IOM's recommendations, the Department of Health and Human Services launched the Computer-based Patient Records Institute. The CPRI called for the "development of a nationwide electronic health care information network by 1996".[32] To this end, in 1992 and 1993, the industry-based Workgroup for Electronic Data Interchange (WEDI) worked on technical standards for supporting "an integrated system of electronic communication networks that would allow any entity within the health care system to exchange information and process transactions with any other entity in the industry".[33]

The concept of a sector-wide information network was subsequently incorporated into President Clinton's 1993 Health Security Plan for national health care reform. The Plan proposed the creation of a uniform standards-based national health data network, tied to an electronic "health security card" for every American.[34] However, the President's health plan was defeated in 1994 and was not revived. Following the plan's collapse, a market-driven, profit-based approach to health care delivery took over by default.[35] This approach (especially in its managed care form) emphasized stringent controls on spiraling health care costs, and in tandem with alarming data about a dramatic decline in the quality of delivered care, increased the amount of data about individual patient care collected by Zone 2 payers and quality assessors from Zone 1 providers.

[30] RS Dick, EB Steen, DE Detmer (Eds.), *The Computer-Based Patient Record: An Essential Technology for Health Care*, Committee on Improving the Patient Record, Division of Health Care Services, Institute of Medicine (National Academy Press, Washington, D.C. 1991; Revised Edition 1997

[31] *Id*, at 50

[32] *Initiatives Toward the Electronic Health Care System of the Future* (USDHHS Report), Washington, D.C., 1992

[33] See U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information, OTA-TCT-576* (Washington, DC: U.S. Government Printing Office, September 1993).

[34] Massachusetts Health Data Consortium, "Health Care EDI Legislation: A Historical Perspective"

[35] M Angell, *The American health care system revisited*, New England Journal of Medicine, Jan 7, 1999.Vol. 340, Issue 1, at 48

Other developments during the latter half of the decade also had significant effects on the management of personal health information in the United States. The new market focus included efforts to encourage patients to see themselves as consumers of health care "products", and in 1997, the Food and Drug Administration (FDA), lifted a long-standing moratorium on direct-to-consumer advertising by drug companies. The shift to "health care consumerism" brought existing consumer marketing techniques into the health sector, encouraging the creation of consumer profiles and providing greater incentives to share patient data among the three Zones of health data handling.

While the attempt to build a national health information network had failed, health sector IT use grew steadily (if at uneven rates) during the period, and its operation remained essentially unregulated following the most recent failure to pass Federal health privacy legislation. Perhaps unsurprisingly, this drew a response during the latter part of the period by a growing community of self-described "privacy advocates," composed of both general-interest groups with a longtime privacy focus (such as consumer rights and civil liberties groups), and new organizations focused on the interaction of technology with individuals rights (such as the Electronic Privacy Information Center, the Electronic Freedom Foundation, and the Center for Democracy and Technology).

This broad coalition arose in response to the privacy impacts of two main trends: the growing warehousing of personal data and the use of data mining to create extremely fine-grained consumer profiles for marketing purposes; and the explosion of electronic personal information sharing via the Internet. The impact of these developments on health data handling constituted a major area of interest and action for these groups. While not always successful in having these impacts legislatively addressed, these advocates were increasingly able to bring them to public attention by sharing reports they had collected of intrusive business and government data handling practices with the national media, and through participation in key legislative and regulatory proceedings.

(2) The assessments

- ***(a) 1993: Protecting Privacy in Computerized Medical Information***

In 1993, the Federal Office of Technology Assessment (OTA) released a report that analyzed the privacy implications of the Institute of Medicine's 1991 proposal to computerize health records. The OTA identified the privacy issues arising from health data computerization; examined the current state of the law dealing with privacy in medical information; and examined legislative, policy and technological models for protecting electronic medical record privacy.

The OTA observed that "computerization can reduce some concerns about privacy in patient data and worsen in others; but it also raises new problems" related to the computer's ability to easily gather, store, exchange and transmit very large amounts of patient information. Among these was the likelihood that increased automation would "prompt increased demands for use of medical information beyond the traditional uses",[36] essentially those in Zone 3. These were the uses identified as long ago as 1976 as raising the "sharpest clash" between health privacy and other socially useful functions.

The OTA reviewed the "patchwork" of State and Federal laws of varying "nature and quality" that had sprung up in the absence of a comprehensive Federal health privacy law, and found that it did "not provide consistent, comprehensive protection for privacy in health care information, whether it exists in a paper or computerized environment." The group warned that the current legal environment was "inadequate to guide the health care industry with respect to obligations to protect the privacy of medical information in a computerized environment."

It urged comprehensive Federal legislation that would: establish strong civil and criminal penalties for "improper possession, brokering, disclosure, or sale" of health care information (broadly defined); provide patients with appropriate rights to access, correct, amend and delete information in their health records; require informed patient consent for disclosure of health information; require the application of technology to track flows of health information; and to finally "establish protocols for access to health care information by secondary users, and determine their rights and responsibilities in the information they access."

· ***(b) 1994: Health Data in the Information Age***

Concurrently with the OTA's study, the Institute of Medicine set out to examine the impact on health information use patterns of regional health data networks, experimental versions of which were being launched in communities across the country. These prototype networks were seen as building blocks for a possible future nationwide system of patient data exchange.

For its 1994 report, *Health Data in the Information Age*, the IOM assessed networks under development in Memphis, Tennessee; Cleveland, Ohio; Des Moines, Iowa; Seattle, Washington; and Albany and Rochester, New York. After exploring the likely users and uses of such networks, the study concluded that health data networking was likely to create significant concerns about patient privacy. It would do so because it facilitated secondary use of patient data; accumulated valuable personal data which would likely create "new demands for access"; linked previous unlinked data items using a unique identifier; and created a large pool of detailed data ideal for use in medical research (a use found to be objectionable to a majority of Americans in the 1993 Harris/Equifax survey).[37]

The IOM then assessed the relevance of existing constitutional, statutory and common law to health data networks and the ability of these laws to address the potential

[36] U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information, OTA-TCT-576* (Washington, DC: U.S. Government Printing Office, September 1993), at 18

[37] MS Donaldson ad KN Lohr, *Health Data in the Information Age*, National Academy Press, Washington, D.C., 1994, at 162

patient privacy concerns they had identified. Because the new health data networks could not properly be categorized as providers, payers, quality assurance organizations, consumer reporting agencies or insurance support organization – but instead combined many or all of these functions – the IOM concluded that “most of [the existing] body of law is unlikely to apply” to them[38] (though certain laws would apply to those who *supplied* data to such networks).[39] As a result, the IOM concluded that “policymakers will [come] under pressure to develop effective privacy protection safeguards” for health data networks.

After canvassing a range of options for such safeguards, the IOM recommended the passage of Federal preemptive legislation that would establish a uniform confidentiality requirement for all who handled health data, and which would specify a Code of Fair Health Information Practices that would appropriately balance patient privacy with socially valuable uses of health data.[40] It also suggested that individual health data networks be required to appoint a Data Protection Board with policy and compliance oversight responsibilities;[41] and that individual consent be required for all disclosures of health data from networks, except in certain narrowly defined circumstances.[42]

· *(c) 1997: Protecting Electronic Health Information*

In 1995, with “expenditures on information technology for health care growing rapidly,” the National Research Council established a committee to “observe and assess existing technical and non-technical mechanisms for protecting the privacy and maintaining the security of health care information systems.”[43] To do so, the Committee on Maintaining Privacy and Security In Health Care Applications of the National Information Infrastructure made site visits to six (unnamed) organizational users of health IT systems, including “a large, urban hospital; a tightly integrated health care system; a second tightly integrated health care system affiliated with a community health information network; a more loosely affiliated provider network; a state health care system; and a large insurer.”[44]

The Committee found that “protection of electronic health information held by individual organizations requires a combination of technical and organizational practices,”[45] and it recommended a set of combined security practices “for immediate implementation”. These included technical measures to prevent both external intrusion and unauthorized disclosures by insiders, such as user authentication, access controls and audit trails; and organizational steps such as the appointment of information security officers, staff training and discipline programs, and the creation of clear data use and

[38] *Id*, at 172
[39] *Id*, at 179
[40] *Id*, at 190
[41] *Id*, at 194
[42] *Id*, at 202
[43] *For The Record: Protecting Electronic Health Information (1997),* at viii
[44] *Id*, at x
[45] *Id*, at 4

handling policies.[46] It urged the Federal government to assist the industry in creating the infrastructure necessary to implement these measures, including the updating of technical privacy and security standards.

The Committee also found, however, that, while improving institutional protections for privacy and security was urgent and vital, doing so would not address *systemic* concerns "that stem from the widespread and relatively unregulated dissemination of information among institutions in the health care industry, including providers, payers, researchers and oversight agencies."[47] According to the Committee, these systemic concerns could "be addressed only through initiatives at a national level that delineate and enforce standards for the appropriate uses of health information."[48]

Going beyond its immediate terms of reference, the Committee urged the Federal government to "work with industry to promote and encourage an informed public debate to determine an appropriate balance between the privacy concerns of patients and the information needs of various users of health information".[49] It also recommended that "organizations that collect, analyze, or disseminate health information should adopt a set of fair information practices similar to those contained in the Federal Privacy Act of 1974."[50] Finally, the Committee proposed the creation by the Department of Health and Human Services, in cooperation with the Office of Consumer Affairs, of an official "privacy ombudsman" accessible to patients with concerns and complaints.[51]

(3) Public perceptions of health privacy issues

· *(a) The early 1990s*

At the beginning of the decade, a survey by Louis Harris & Associates and Dr. Alan Westin found that health information privacy was an issue of very high concern among Americans. While only 25% of Americans fell into the "high concern" category for issues of privacy generally, this rose to 48% in relation to personal health data.[52] At the time of the survey, health care reform issues were occupying center stage in the nation's political discourse, and – as in the 1970s – there appeared to be a real possibility that health records would, in future, be processed in the context of a national health system.

Attitudes toward uses and users of patient data. In 1993, most Americans (87%) trusted their health care providers to protect the confidentiality of their medical information, but were increasingly concerned about access to and use of that information

[46] *Id*, at 8
[47] *Id*, at 2
[48] *Id*, at 5
[49] *Id*, at 180
[50] *Id*, at 181
[51] *Id*, at 184
[52] *Health Information Privacy Survey 1993: a national opinion survey conducted for Equifax, Inc. by Louis Harris & Associates and Dr. Alan Westin*

outside of the direct care context. These concerns were highest in relation to Zone 3 uses and users of medical information:

- Four in ten Americans (41%) were concerned that medical claims data processed within a workplace health plan might be seen by their employer and adversely affect their job opportunities or job status.

- Six in ten (60%) felt that the use of their medical records for the purpose of pharmaceutical direct mail advertising was unacceptable.

- Almost seven in ten (66%) said that hospitals should not use medical record information to solicit donations from patients (a Zone 3 use by a Zone 1 user).

- There was surprisingly strong concern over the use of even de-identified medical record information for the purpose of health research – 64% of Americans wanted to be asked for permission before such records could be used in research. More than half (56%) wanted their consent sought each time a researcher requested access to their de-identified record.

Attitudes toward automation of medical data processing. The survey found significant levels of unease about the use of computers to process health data. Half of all Americans (50%) were concerned that their health care providers had automated functions such as accounting and lab data. One major area of concern was in the rate of data error: majorities of respondents felt that automation had increased errors in health care service charges (75%) and in medical conditions recorded in patient files (60%). Automation was also strongly felt to contribute to an increase in access to personal health data for non-health uses: more than six in ten Americans (64%) felt computer-processed health data was more likely to be "given to people who aren't supposed to see it", while three in four (75%) were concerned that "a computerized health care information system will come to be used for many non-health purposes".

Attitudes toward health data privacy regulation and enforcement. Finally, the survey found that large majorities of the American public favored comprehensive federal health data privacy legislation. A very large majority (96%) wanted a law that classified all personal medical information as sensitive and imposed penalties for its unauthorized disclosure. The same percentage thought such a law should also include rules "spelling out who has access to medical records and what information could be obtained." A similarly large group (95%) supported a legal right for patients to access, correct and supplement their health records. Almost nine in ten (86%) favored the creation of an independent National Medical Privacy Board to "hold hearings, issue regulations, and enforce standards" for health privacy.

- ***(b) The late 1990s***

By the end of the decade, surveys showed that Americans' concerns about both privacy generally, and health privacy specifically, had risen significantly. In 1999, 48%

nationwide described themselves as "very concerned" about invasion of personal privacy, and 79% believed it had become more difficult in recent years to keep personal information private and confidential.[53] A year later, 78% said that privacy of personal health information was "very important".[54] The rise was perhaps unsurprising in the context of a decade in which various health sector trends had resulted in a great increased in health data collection, use and sharing, and in an environment of growing public attention to the issue of data security in computer networks.

Attitudes toward uses and users of patient data. Trust in health care providers to maintain the privacy of personal health data remained high, with anywhere from six[55] to nine[56] in ten Americans expressing confidence in the ability of doctors, hospitals and other health care professionals to protect confidentiality. Confidence in users outside of Zone 1 was much lower; in 2000, only 42% trusted insurance companies to protect their health privacy; a slightly lower proportion (35%) trusted managed care companies to maintain confidentiality.[57]

Surveys during this period also showed a strong desire among Americans for greater control over the disclosure of their medical information. In 2000, more than eight in ten (84%) said that they were concerned that their personal health information "might be made available to others without their consent."[58] Majorities of varying sizes were opposed to medical record access without consent by banks (95%), government agencies (92%), police or lawyers (88%), employers (84%), insurance companies (82%), medical doctors (71%), local and state health departments (71%), medical researchers (67%), and pharmacists (59%).

Even with consent, certain uses and users of health data were considered more acceptable than others. In 1999, majorities were willing to consent to health record access by health researchers at universities (64%) and government institutions (58%) conducting a study about a medical condition by which they were affected. Conversely, majorities said that they would not consent to health record access by drug companies for marketing purposes (70%); by hospitals seeking enrollees for preventative health programs (60%); by employers as part of the job application process (61%); or by health insurance plans for marketing purposes (56%).

Attitudes toward automation and networking of medical data processing. At the end of the decade, levels of concern about personal health data automation remained high. In 1999, 54% of Americans agreed that "the shift from paper record keeping

[53] Princeton Research Associates/California HealthCare Foundation, *Medical Privacy and Confidentiality Survey*, October 1999

[54] Gallup/Institute for Health Freedom, *Public Attitudes Toward Medical Privacy*, September 2000

[55] Princeton Research Associates/California HealthCare Foundation, *id*

[56] Gallup/MedicAlert Foundation, *Most Americans Shun Using Internet for Personal Health Information*, 2000

[57] *Id*.

[58] *Id*.

systems to electronic or computer-based systems" had "made it more difficult to keep personal medical information private and confidential".[59]

As Americans increasingly turned to the Internet for medical and health information (71% of Americans used the Internet to search for health-related information in 1998, rising to 74% in 1999),[60] their concerns over automation were now joined by a growing fear about the potential impacts of storing and exchanging personal medical information via networks. In 2000, only 7% were "very willing" to store or transmit personal health information on the Internet.[61] Online medical record keeping – even under conditions of restricted access – was considered the greatest threat to privacy on the Internet, with users more concerned that websites storing health data would share it with others without permission than they were about hackers gaining unauthorized access to their health data online (75% and 59% respectively).[62]

Americans were overwhelmingly (88%) opposed to the idea of a compulsory national computerized database of patient records, and a strong majority (95%) wanted to be asked for permission to have automated health records included in a national database. Even then, most felt that certain information should never be circulated within such a database; only 4% said they were comfortable with the inclusion of "personal information told a doctor in confidence and entered into their medical records."[63]

(4) Developments in health privacy regulation

- ***(a) HIPAA and the Health Privacy Rule***

The decade of the 1990s was marked by repeated attempts to pass comprehensive Federal health privacy legislation that would address many of the outstanding concerns identified in technology assessments and surveys of the public. The Health Security Act of 1993 would have included restrictions on disclosure of health information without patient consent, established patient rights of notification, access and correction, and required the development within three years of passage of a comprehensive, stand-alone Federal privacy health privacy law incorporating an enforceable Code of Fair Information Practices.

Between 1995 and 1997, a number of relevant bills were introduced (and reintroduced) into Congress, including the Medical Records Confidentiality Act; the Fair Health Information Practices Act; and the Medical Privacy in the Age of New Technologies Act. All of these efforts failed. Senator Robert Bennett (R-UT), a skilled practitioner of legislative compromises, who with Senator Patrick Leahy (D-VT) led the effort in the mid-1990s to enact health privacy legislation, has commented that the intransigence of key stakeholders across the spectrum of involved interests torpedoed all

[59] Medical Privacy and Confidentiality Survey, California HealthCare Foundation, 1999
[60] Harris Interactive, "Cyberchondriacs Update," May 1, 2002
[61] Gallup/MedicAlert, *id*.
[62] California Health Care Foundation, *Ethics Survey Of Consumer Attitudes About Health Web Sites,* 2000
[63] Gallup/Institute for Health Freedom, *id.*

efforts to craft a law. He called it one of the most disappointing experiences of his legislative career.

Finally, a provision requiring Congress to enact a comprehensive health privacy law by 1999 was inserted (at the twelfth hour) into the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Act provided that if Congress failed to pass such a law within the designated period, the Secretary of Health and Human Services was required to draft a health privacy regulation within the following six months. Congress was unable to agree on a comprehensive law before the deadline, and in December 2000 President Clinton issued regulatory Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164) drafted by the Secretary of Health and Human Services.

Finalized in December 2000 (and amended in 2002), the HIPAA Privacy Rule comprises the nation’s first Federal health privacy regulation. The Rule addresses some, but by no means all, of the health privacy concerns identified over the decades by the technology assessments reviewed above, and shown by successive surveys to be held by majorities of the American public. For example, the Rule guarantees a right of patient access to health records; requires notice to patients of how their health information will be used and disclosed; and allows patients to track the circulation of their medical information through the “accounting of disclosures” requirement. The Rule also promotes the development of a privacy-protective environment inside health data-handling organizations through requirements to appoint a privacy officer, train staff and implement formal privacy safeguards.

However, the Rule applies only to a subset of all organizations that handle personal health information, and excludes many of those (mainly in Zone 3) whose operations are of most concern to a majority of Americans. Consent is not required for use or disclosure of personal health information for purposes of “treatment, payment of health operations”, broadly defined. Perhaps most controversially, marketing uses – shown by surveys to be among the most objectionable to Americans – are only lightly regulated (and these regulations were further loosened when the Rule was amended in 2002). Covered organizations are free to share patient data with “business associates”, as long as these entities undertake to abide by the requirements of the Rule.

While the Rule includes both civil and criminal penalties, there is no right of individual enforcement, and HHS, rather than an independent body, is responsible for oversight. Finally, the Rule does not preempt existing state health privacy laws that are more stringent, leaving much of the existing “patchwork” of health information privacy law in place.

· *(b) State legislative actions*

During this period, in the absence of Congressional action, the individual States increasingly took action to pass legislation regulating the processing of health data and establishing patient rights in relation to health data in a variety of contexts. In the main, these laws established different obligations and requirements on different holders and users of health information, rather than establishing across-the-board rules for all health data processing.[64] The majority of State laws were not intended to implement comprehensive health privacy protection schemes, and few were designed to maintain pace with technological developments in health information processing. They were by no means uniform, creating a situation in which health data handling obligations varied widely from State to State.

By 1999, thirty-three states granted patients a right of access to their hospital records; 13 assured a right of access to HMO records; and 16 legislated for a right to access health insurance records. Others had created patient rights to amend and supplement their medical records, especially those held by health insurers. A number of States passed laws restricting the disclosure and re-disclosure of patient information without consent. By the end of the period, almost all States had laws to restrict the use of information about specific health conditions carrying particular stigma, such as mental illness, communicable diseases, HIV/AIDS and cancer. Most of these State laws provided penalties for breach and remedies for violations of health privacy interests, such as the ability to bring private lawsuits to recover compensation.

· *(c) Equality limits on health information uses*

It was during this period that laws first appeared to restrict the collection of otherwise relevant personal information, especially for the purpose of carrying out Zone 3 functions. These laws were based on a consensus that had developed in the 1970s that rejected “previously widespread racial, religious, political and gender discrimination patterns embedded in many existing organizational record systems”.[65] The passage of these laws constituted a recognition that the added cost of excluding potentially relevant personal information was outweighed by society’s interest in equal protection. While not based specifically on an argument from privacy interests, these laws had privacy effects, in the sense that they reduced the handling of certain (often sensitive) information about people in the Zone 3 contexts that surveys showed were of most concern to Americans.

In the 1990s, these laws increasingly included prohibitions on the collection of certain otherwise relevant personal health information. The most notable of these were passed against the backdrop of the widely publicized Human Genome Project, the international collaborative scientific effort to “decode” the human genome. After the project had advanced to a stage that raised the possibility of using genetic information to determine future health risks, some 32 States passed legislation prohibiting the requirement of genetic data for health insurance, employment, or as a conclusive factor in life insurance. Although Congress did not act during this period, President Clinton signed in February 2000 Executive Order 13145 -- To Prohibit Discrimination in Federal Employment Based on Genetic Information.

[64] This and the following details are drawn from J Goldman et. al., *The State of Health Privacy: An Uneven Terrain (A Comprehensive Survey of State Health Privacy Statutes),* Health Privacy Project, 8 August 1999

[65] AF Westin, “Social and Political Dimensions of Privacy,” Journal of Social Issues, Vol. 59, No. 2, 2003, 431 at 436

C. Phase Three: 2001 to the present

(1) Technology and practice

While political and industry-based developments had sapped the momentum, the impetus for patient data automation and networking continued to increase after the turn of the millennium. When the Institute of Medicine reported in 2000 that medical and medication errors were the third leading cause of death in the United States (just behind heart disease and cancer),[66] one of the culprits was found in a health sector "relatively untouched by the revolution in information technology that has been transforming nearly every other aspect of society."[67] The IOM urged "a renewed national commitment to building a [nationwide health] information infrastructure," with a view to eliminating "most handwritten clinical data by the end of the decade".[68]

The IOM's call was echoed in February 2001 by the President's Information Technology Advisory Committee, whose Panel on Transforming Health Care reported that the lack of a "broadly disseminated and accepted national vision for information technology in health care" was a central and continuing obstacle to the development of a nationwide health data network.[69] In November 2001, the National Committee on Vital and Health Statistics (NCVHS) called on the Department of Health and Human Services to adopt "a key leadership role" in a "dynamic, nationwide, collaborative venture" that would engage all stakeholders, including Federal, state and local governments; healthcare providers; health plans and purchasers; standards development organizations; the information technology industry; consumer and patient advocacy groups; community groups; and academic and research organizations.[70]

In June 2002, the Markle Foundation launched "Connecting for Health", which brought together over 100 representatives drawn from all segments of the health community, in what has become the leading private-sector collaborative working to accelerate the development of "electronic connectivity in healthcare." The group rapidly began working to create consensus standards for health data interoperability and to identify exemplary privacy and security practices for health data networking, with its

[66] LT Kohn, JM Corrigan, and MS Donaldson, (Eds.), *To Err is Human: Building a Safer Health System*, Committee on Quality of Health Care in America, Institute Of Medicine (National Academy Press,_ Washington, D.C. 2000)

[67] *Crossing The Quality Chasm: A New Health System for the 21st Century*, Committee on Quality of Health Care in America, Institute Of Medicine (National Academy Press, Washington, D.C., 2001), at 5

[68] *Id*, at 17

[69] President's Information Technology Advisory Committee, Panel on Transforming Health Care, *Transforming Health Care Through Information Technology: Report to the President*, February 2001

[70] National Committee on Vital and Health Statistics, *Information for Health: A Strategy for Building the National Health Information Infrastructure*, Washington, D.C., November 15, 2001

ultimate goal the promotion of greater patient participation in care through the provision of secure access to electronic health records.[71]

At the same time, several Federal agencies were working to establish intra-governmental standards for health data networking. In 2003, the Consolidated Health Informatics Initiative of the Departments of Defense, Health and Human Services and Veterans' Affairs created uniform standards for the electronic exchange of clinical information between the three agencies. Also in 2003, the Secretary of Health and Human Services directed the IOM and the international data standards body Health Level 7 to design a standard for electronic health records to be used in federally coordinated demonstration projects.

In April 2004, President George W. Bush signed Executive Order 13335, creating a new HHS-based Office of National Coordinator for Health Information Technology with responsibility for "develop[ing], maintain[ing], and direct[ing] the implementation of a strategic plan to guide the nationwide implementation of interoperable health information technology in both the public and private health care sectors that will reduce medical errors, improve quality, and produce greater value for health care expenditures."[72]

The ONCHIT is required to coordinate the efforts of various government departments and agencies, as well as to "coordinate outreach and consultation" by those departments and agencies with "public and private parties of interest, including consumers, providers, payers, and administrators." The Department of Health and Human Services thus now serves officially in the "key leadership role" envisioned for it in 2001 by the National Committee on Vital and Health Statistics. Following the May 6, 2004 appointment of Dr. David Brailer as the first National Coordinator, the Office has moved swiftly to broker collaborative public-private efforts to develop a national health information network.

In July 2004, the National Coordinator released a Framework for Strategic Action,[73] setting out four major goals for the new collaborative health information technology effort. These included: encouraging and assisting providers to adopt electronic health records; interconnecting providers by "fostering regional information exchanges and linking EHRs via a national health information network", personalizing care by creating Personal Health Records, and using information technology to improve public health surveillance and health care quality assessment systems, as well as clinical research.

[71] "Markle Foundation Launches Initiative to Promote Adoption of Key Clinical Health Information Standards; Connecting for Health Convenes Leaders to Promote Adoption of Information Standards to Improve Healthcare while Protecting Privacy," Press Release, June 21, 2002

[72] *Executive Order 13335 of April 27, 2004: Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator*, Federal Register Vol. 69, No. 84, April 30, 2004

[73] Office of the National Coordinator for Health Information Technology, *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care*

In November 2004 the National Coordinator issued a "Request for Information on the Development and Adoption of a National Health Information Network",[74] inviting stakeholders to provide input on "possible methods by which widespread interoperability and health information exchange could be deployed and operated on a sustainable basis." The RFI attracted over 500 responses from hospitals and health care providers, payers, potential IT vendors, health IT standards bodies, and civil liberties and patients' rights groups. In June 2005, incoming Health and Human Services Secretary Mike Leavitt announced the formation of an American Health Information Community that will create an official foundation for the emerging public-private collaborative. A 17-member public-private collaborative body, AHIC will be charged with creating uniform technical and compliance certification standards for the networked electronic health records.[75]

In addition, efforts are now underway in Congress to provide a legislative basis – as well as public funding -- for national health data networking. May 2005 saw the introduction of the 21st Century Health Information Act of 2005 (HR 2234) into the House with bipartisan support. The bill would fund government-accredited regional health data sharing organizations, and would provide financial aid and technical assistance for physicians purchasing IT systems in order to participating in regional health data sharing projects.

In June, Senators Hillary Clinton (D-NY) and William Frist (R-TN) cosponsored Senate Bill 1262, which aims "to reduce healthcare costs, improve efficiency, and improve healthcare quality through the development of a nation-wide interoperable health information technology system." Additional health IT promotion bills were introduced during June by Senators Chris Dodd (D-CT), Debbie Stabenow (D-MI) and Olympia Snowe (R-ME), Michael Enzi (R-WY), and Edward Kennedy (D-MA), and Charles Grassley (R-IA) and Max Baucus (D-MT).

(2) The assessments

Since 2003, a wide range of reports and studies have assessed various technical, organizational, economic and social obstacles to and implications of creating a nationwide electronic health record network. For example, in 2003, Dr. David Brailer, the current National Coordinator for Health Information Technology, and colleague Emi Terasawa issued a report on "Use and Adoption of Computer-Based Patient Records" on behalf of the California Health Care Foundation. 2004 saw the release of a large number of reports identifying remaining obstacles to health record networking, including reviews by the Cap Gemini consulting group,[76] the Government Accountability Office (GAO),[77] and the National Health Policy Forum of George Washington University.[78] Detailed

[74] Federal Register, Vol. 69, No. 219, November 15, 2004

[75] M.L. Baker, "HHS Launches Health IT Collaborative," eWEEK, June 6, 2005

[76] Cap Gemini, *Health Information Technology and the Electronic Health Record: Implications for Healthcare Organizations*, 2004

[77] Government Accountability Office, *HHS's Efforts to Promote Health Information Technology and Legal Barriers to Its Adoption*, August 13, 2004

[78] L Sprague, "Electronic Health Records: How Close? How Far to Go?" NPHF Issue Brief, No. 800, September 29, 2004

assessments of the technical and economic feasibility of the proposed network continue to appear in 2005.

While many of these reports have identified privacy and security as among the central elements that must be addressed before a national electronic health records network becomes a reality, only a few have specifically addressed as such a networked system's implications for privacy. Among those that have focused on privacy are the 2003 report of the Markle Foundation's Connecting for Health Privacy and Security Working Group, which surveyed fourteen sites operating various types of electronic health data programs in order to identify "promising and noteworthy" privacy practices. A 2005 report by the collaborative introduced the concept of a Record Locator Service, a novel mechanism for protecting patient privacy by linking patient data in disparate localized databases, rather than creating a centrally-stored and "total" electronic health record .[79]

While these reports and studies introduce valuable mechanisms for protecting patient privacy in electronic health record systems, they are not analogues for the in-depth, sector-wide technology impact assessments undertaken in previous eras. As such, a full assessment of the impact of networked EHR systems on health data circulation and patient rights is yet to be undertaken.

(3) Public views and legal rules

· *(a) Public perceptions of privacy in electronic health data networks*

Current surveys show that, at this early stage, the American public can best be described as ambivalent about electronic health records and networks. On the one hand, majorities agree that such developments have the potential to make the improvements claimed for them, such as increasing their participation in their own care, and reducing medical errors, waste and some administrative costs. On the other hand, similar majorities view the expansion of health data networking (whether within the newly launched scheme or outside of it) with great concern for its potential impact on their privacy.

For example, a 2003 survey by the Connecting for Health collaborative found that between 50% and 70% of Americans believed that having personal health records online would have positive effects on their health care, with support highest among those already using e-health services and those suffering from chronic illnesses. Respondents were most comfortable with consenting to access by doctors to an online medical record (79%), and least comfortable with allowing insurers similar access (23%). However, concern about the privacy and security of online medical records was almost universal (91%).[80]

[79] Connecting for Health Working Group on Accurately Linking Information for Health Care Quality and Safety, *Linking Health Care Information: Proposed Methods For Improving Care And Protecting Privacy,* February 2005

[80] Connecting for Health, "Americans Want Benefits Of Personal Health Records," 2003

A 2004 Harris Poll found that two in five adults were keeping a personal health or family record containing "the results of all [their] medicals tests and details about prescriptions, vaccinations, treatments, known allergies and other health care information."[81] Of those who were not, 84% agreed that it was a good idea for a variety of reasons. However, of those who kept such records, only 13% kept them on computer, with only 1% storing them on a health record website such as (the now-defunct) "MyDocOnline.com". Of the remaining 86% of record-keepers, six in ten indicated that they were unlikely to move their records either onto a computer or the Internet. By far the strongest reasons for this reluctance were "serious concerns" over privacy (68%) and security (66%).

· *(b) Adequacy of the legal and policy environment*

As outlined above, the current regulatory environment is characterized by the operation of the HIPAA Privacy Rule, single-issue federal health confidentiality laws and regulations, and a patchwork of state health privacy laws.[82]

There are already serious concerns about the ability of this framework to sufficiently address privacy concerns about health data handling in the existing partially automated and networked environment. It is clear that some of these concerns – most notably those related to the security of digital information – may in fact be resolved by the application of appropriate technologies. Others, however, are not related to the record format, but rather to systemic health data handling practices such as widespread health data sharing without meaningful consent. As previous assessments have demonstrated, a regulatory environment that leaves these practices unaddressed will result in their unchanged incorporation in and facilitation by developing technologies.

In addition, because of its restrictive application, the Rule may not apply to the new structures required to create a national health information network. For example, the move to create and store personal health records using trusted non-medical record keepers acting as the patient's own agent would not be covered by the Rule, as these record-keepers do not fall within the Rule's definition of "covered entities". The same is true of regional health data exchanges, which are intended to function as the backbone of a larger national system – just as it was when the Institute of Medicine investigated early prototypes in 1994.

There are, of course, formidable obstacles to revisiting the current regulatory framework. Even in its current, much-criticized format, the HIPAA Privacy Rule is the

[81] Harris Interactive, "Two in Five Adults Keep Personal or Family Health Records and Almost Everybody Thinks This Is a Good Idea," The Harris Poll Health Care News, Vol. 4, Iss. 13, August 10, 2004

[82] For a valuable summary of the current complex legal environment within which efforts to expand information technology programs will have to unfold, see S. Rosenbaum and M.W. Painter, Assessing Legal Implications of Using Health Data to Improve Health Care Quality and Eliminate Health Care Disparities, George Washington University Medical Center and The Robert Wood Johnson Foundation, GQ/SPHHS, July, 2005.

result of several decades of political struggle, and any proposals for further changes will, without doubt, be met with strong opposition. However, it is becoming clear that many aspects of the Rule may actually impede the creation of a national system of interoperable electronic health records. For example, the Rule's non-preemptive status creates a very serious – some believe insurmountable – state-laws obstacle to the viability of a national health information network.[83].

These structural impediments are already opening up the Rule and the wider regulatory environment for review. As noted above, the Department of Health and Human Services recently issued a Request for Proposals for solutions that would "address state and business privacy and security practices that may pose challenges to interoperable health information exchange." This is clearly also the appropriate time to consider fully addressing and resolving some of the outstanding systemic privacy issues unaddressed by the current environment.

Already, there appears to be support in some quarters for a such a review; for example, in May 2005, Congressman Dana Rohrbacher (R-CA) proposed an amendment to HIPAA that would reverse the 2002 relaxation of restrictions on marketing use of health data, and would require meaningful patient consent to be obtained for all uses and disclosures of personal health information except for the purposes of (1) dispensing a prescription or (2) providing treatment in a situation in which it is impractical to seek the patient's consent (such as a medical emergency).[84]

In addition, privacy standard-setting has been mandated in at least three of the four e-health bills that have been introduced in Congress. The Frist-Clinton bill[85] would create an Electronic Health Information Standards Development Working Group that would work on standards for protecting privacy, among other things, and would also require a study on harmonizing State health privacy laws and practices. The Kennedy-Murphy bill[86] would provide grants for the development of regional health information technology plans tied to the provision in those plans of a certain level of patient control over health records, and compliance with the HIPAA Privacy Rule. And the Dodd bill[87] would create within the Office of the President an Office of Health Information Technology charged, among other things, with developing standards to "ensure the privacy and confidentiality of medical records".

III. A PRIVACY BY DESIGN PROGRAM FOR THIS DECADE

A. What is new about the recent developments

(1) The technology

[83] Federation of American Hospitals, "Response to Request for Information," January 18, 2005
[84] "The Medical Independence, Privacy, and Innovation Act of 2005, " H.R.2599
[85] Senate Bill 1262, "The Health Technology to Enhance Quality Act of 2005"
[86] House Bill 2234, "The 21st Century Health Information Act of 2005"
[87] Senate Bill 1223, "The Information Technology for Health Care Quality Act of 2005"

While the technology needed to create and network electronic patient records has been available for some time, the basic standards vital to the operation of a network among a great variety of far-flung systems have been conspicuously absent. The proliferation of vendors and products in the absence of basic uniform standards for electronic health record formats and data exchange have, until now, prevented the spread of networks outside of single institutions or regional data exchanges.

The current environment is marked by a consensus among almost all potential designers, installers, operators and users that such standards must be established and enforced in order to create wider networks, and by a willingness to engage in collaborative development of such standards. As such, the creation of a workable nationwide network appears more likely now than at any time since the technology for creating such a network became reliable and affordable.

In addition, new information technologies are emerging that may, in future, become central components of a national health data network. One of these is the radio frequency identification device (RFID), whose potential to track patients, medical equipment and drugs may greatly reduce high rates of medical error caused, in part, by high patient volume and system complexity. Already a small number of institutions and systems, such as the Veterans Affairs hospital system and Partners HealthCare of Massachusetts, are experimenting with RFID projects that use scanners to match tagged patients to the correct tagged prescription drugs. These projects have reduced medication error rates by between 24% and 50%.[88]

In addition, developments in clinical and pharmacological research may, in future, significantly alter the amount and nature of information collected from patients and shared among health and related professionals via electronic personal health records. With recent advances in biotechnology making the widespread extraction of human genomic data increasingly feasible, those at the cutting edge envision the use of genetic data in development of tailored medical treatments - and even in the creation of drugs tailored to an individual's genetic profile.[89] While "pharmacogenomics" is, at this stage, only an emerging field (and one not entirely supported by the mainstream pharmaceutical industry)[90], many experts see the paradigm shift in drug treatment it represents as an inevitability.

(2) The Federal role

During the 1970s and again in the 1990s, proposals to create nationally integrated health record systems were put forward by successive Federal governments as components of broader health sector reform. Within these reform plans, nationwide health information databases were envisioned as being either centrally operated or standardized by the Federal government. When these plans failed, information technology went forward in the health sector nonetheless, but in the absence of a central

[88] AA Wright and IT Katz, "Bar Coding for Patient Safety," N Engl J Med 353;4, at 329
[89] See, for example, "Custom Care", Informationweek.com, October 18, 2004
[90] "The New New Pharmacogenomics", M Branca, Bio-IT World, September 9, 2002

authority or standard-setter, IT development proceeded in an ad hoc manner, leading to the wide variation in EHR and networking readiness that exists today.

The Federal government's commitment to collaborate with the private sector in the development of a public-private network project, outside of a wider health system reform plan, thus sets current efforts apart from previous attempts. The private sector has sought, and the Federal government has now agreed to provide, central leadership in the development of the standards whose absence, until now, has prevented greater integration of existing health databases. Congress has also proposed Federal grants to organizations for assistance with development and implementation of health record database technology.

The Federal government has even proposed to share its own tested EHR technology – the Vista electronic health records software used in both the Medicare and Veterans Affairs environments – with doctors free of charge.[91] In its current forrn, Federal engagement both increases the chances of success for EHR and networking development, and raises strong concerns about the extent of public sector access to personal medical information. This is particularly so in the context of prolific media reporting on controversial Federal programs (such as the "TIA" and "trusted traveler" programs) to draw on both public and private sector data sources to create profiles of millions of Americans for the purpose of deterring further terrorist attacks.

(3) Conditions in the health sector

In previous eras, occupational resistance was a key factor in preventing the spread of information technologies through the health sector. Apart from those who were early adopters of technology, many physicians of the 1970s and 1980s were not yet comfortable with computers and were resistant to the time-consuming work of inputting patient data into a database in accordance with pre-set constraints. In addition, some were wary of the potential effects of computer-aided diagnosis – an oft-mentioned benefit of computerized patient records - on professional autonomy and status.

The current generation of physicians and providers is now extensively "wired" and resistance to computer use appears to be much less of a factor in the development of electronic health records systems than it was previously. While concerns over technological impacts on professional autonomy continue, the potential of information technology to enhance the patient-physician relationship is much more plausible than it was in previous eras. In addition, the changing nature of American society and American medical practice in recent years has led many providers to see information technologies as essential tools in managing patient care. Among the more important changes have been:

A rise in chronic illness. Whereas in the immediate postwar period, the majority of health care was provided in a hospital setting and dealt with acute episodes of illness,

[91] "U.S. Will Offer Doctors Free Electronic Records System," New York Times, July 21, 2005

in recent years there has been a dramatic rise in chronic illnesses like diabetes, heart disease, hypertension and asthma within the American population. Care provision has thus shifted from an event-based in-patient model to an ongoing ambulatory care paradigm. This shift has both increased the need for health care providers to follow their patients' health status over time and made it more difficult to do so. In addition, sicker patients are taking more prescription drugs than ever before, making it imperative for their providers to track potentially fatal or harmful pharmaceutical interactions.

Increased labor market instability. A substantial increase in the instability of the labor market has permitted or required many Americans to move more often for employment purposes, making the establishment of long-term patient-provider relationships impossible. Even within the same geographical area, employment changes frequently lead to a change in insurance coverage, requiring patients to find alternative providers in a new network. Rising insurance costs have led many employers during this period to begin switching insurers periodically, meaning that even when employment is stable, access to a particular care provider is not guaranteed. All of these events have made it difficult for many individuals to steadily build a comprehensive longitudinal health record with a single provider.

Increased specialization in health care delivery. The United States now has one of the developed world's lowest ratios of primary care providers to specialists, witnessing a dramatic drop in the supply of medical school graduates to family and general internal medicine programs (and a sharp rise in subspecialty physician training) since 1997.[92] The result has been that health data about a specific individual are increasingly maintained in separate locations by specialist providers who often are not affiliated, and is not routinely communicated between those providers.

A growing volume of clinical research data. There is ample evidence that health care providers are finding it increasingly difficult to keep up with the growing volume of clinical research findings, leading to major disparities between regions and institutions in the quality of care delivered to patients. Research has shown that it takes an average of 17 years for findings from basic health research to be widely adopted among practitioners,[93] perhaps because (as research has also shown) physicians have less time than ever before to spend reading and digesting relevant medical journal information.[94]

As a result of changed provider attitudes and the growth of strong imperatives for technological management of patient information, the occupational culture now appears less likely to present a significant obstacle to the development of a networked health record system than was the case in earlier periods. Rather, it appears that the most

[92] RL Phillips, B Starfield, "Why Does a U.S. Primary Care Physician Workforce Crisis Matter?" American Family Physician, Vol. 68 No.8, October 15, 2003, at 1494

[93] Balas EA, Boren SA. "Managing clinical knowledge for healthcare improvement," Yearbook of medical informatics, National Library of Medicine, 2000: 65-70

[94] See, for example, D Burke et. al., "Reading Habits of Physical Medicine and Rehabilitation Resident Physicians," American Journal of Physical Medicine & Rehabilitation. 83 (7):551-559, July 2004

significant remaining barriers to adoption of EHRs and creation of EHR networks are financial and legal.

(4) The Legal Environment

The existence of a massive federal/state/private IT promotion effort in the current environment may well provide a new opportunity to privacy advocates, who are better organized than ever before, to press for the adoption of more stringent legislative or regulatory health privacy standards.

In this context, it is important to note that national privacy legislation in the U.S. has traditionally been made on a sector by sector basis, with enforcement by sectoral regulatory agencies and private lawsuits, rather than EU-style, with a comprehensive code for the entire private domain and an overall national data protection agency.

What is even more important to understand is when and how federal privacy laws in major industry sectors are enacted at all. With a few exceptions, such as the Electronic Communications Privacy Act and the Children's Online Privacy Protection Act (COPPA), private-sector privacy laws have been passed not as stand-alone legislation to ameliorate privacy harms, but rather as "privacy inserts" to larger industry re-organization or revised industry operations legislation that Congress is ready to enact.

Put another way, privacy protections have generally been tradeoffs by which privacy-oriented interest groups accept larger industry reforms or changes on condition that some privacy protections are included. This has been the case with both the financial services and health care sectors in the U.S. Efforts to enact federal financial or health privacy laws were proposed but rejected in the 1974-1995 period, under industry opposition, weak advocacy resources, and insufficient political rewards for mainstream legislators.

However, when Congress took up the industry-sponsored Financial Modernization legislation in the mid to late 1990s, by which legally separated banking, insurance, and investment firms would be able to join in conglomerates and cross-market their services, privacy advocates were able to make the insertion of privacy rules a condition for passage of the Financial Modernization (Gramm-Leach-Bliley) Act of 1999.

In the health area, after defeats for stand-alone health privacy laws in the 1970s, 1980s, and early 1990s, the addition by Congress of health privacy provisions was made a condition of passage of the Health Insurance Portability and Accounting Act of 1996. (This was later delegated by Congress to be written by the Department of Health and Human Services, in 2000) and, with Bush Administration modifications, issued in 2002 and put into force in 2003.)

The point of these observations is that the current collaborative federal/state/private IT promotion effort presents again the "pay-your-privacy-toll" political opportunity. Seen in this crass political light, what is noteworthy is that the privacy toll-takers are now quite substantial and well organized. That they will collect a privacy toll is not really in issue; the question is what this toll will be, how well it will be formulated in the new IT-driven health care system; and then how effectively these new IT-environment privacy rules will operate and be enforced.

(5) New Data Security Threats

Prior to 2003, concern among Americans over leakage of personal data from business and government data systems was only a minor concern. In 2003-2005, however, two developments changed this condition dramatically:

- First, an epidemic of leaks, hacks, and thefts of personal data involving tens of millions of consumers took place in 2003-2005 - which, because of a California law requiring notification to victims of such breaches, generated explosive coverage in the national news scene

- Second, 20% of American adults, representing 44 million individuals, reported that they had personally been the victim of an ID theft, as a result of having their data leaked or captured by ID thieves, for a cost that the FTC estimated at $9 billion yearly. ID theft became the number one consumer concern.

Personal information in medical files was by no means untouched by these data security failings, and compromises of medical record information were also widely publicized. More than 50 health data breaches were reported in 2003-2005, including ID theft uses of data stolen by health care employees, family members, or hackers. In 2005 alone:

- Medical files on 57,000 patients of Blue Cross Blue Shield of Arizona were stolen from a managed-care company processing these records on back-up tapes; the records contained, in addition to personal identifiers, treatment histories and physicians visited.[95]

- A break-in at a San Jose, California Medical Group provided thieves with two laptops containing names, addresses, Social Security numbers, and medical information on 185,000 patients.[96]

- Eleven defendants were indicted in May, 2005 in Chicago for stealing the patient records of more than 100 patients at two medical practice groups and using identifying information in the records to make withdrawals of moneys from the patients' bank accounts. The thefts were carried out by two employees of the medical practices.[97]

[95] July 14, 2005; California Healthcare Foundation.
[96] The Mercury News, April 12, 2005.
[97] U.S. Department of Justice Press Release, May 12, 2005.

- Kaiser Permanente in Northern California informed over 150 patients that a former employee had posted their names, addresses, telephone numbers, a medical record number, and some lab results on the Internet.[98]

- About 3,000 detailed patient hospital statements from the Cleveland Clinic fell off a delivery truck and were blown by the wind across downtown streets, where they were picked up by pedestrians.[99]

- A clerk at the Dana-Farber Cancer clinic in Boston was convicted for accessing patient records and using the personal information to buy cell phones and other merchandise charged to the patients' accounts.[100]

- The U.S. Navy reported that an identity theft ring in Baltimore stole patient records from a large medical testing company, and used the information to buy expensive automobiles, building supplies, and other merchandise.[101]

- Hundreds of patients' medical records from a medical practice were discarded in July 2005 in two boxes left at a Pittsburgh elementary school dumpster site, contrary to legal requirements under state and federal law that such records had to be burned, shredded, or otherwise have their contents made unreadable. . The story in the Pittsburgh Tribune-Review described similar incidents of improper disposal of medical records and breaches of confidentiality requirements in 2005 in Arizona and Florida.[102]

- Medical records on 42,000 students, faculty members, and staff from the Wardenburg Health Center of the University of Colorado were captured by hackers from a University computer server. The University warned the victims that "possible fraud and identity theft" might be involved.[103]

This steady flow of medical-record disclosures or thefts in 2004-2005 has communicated a sharp message to the American public: assurances of the confidentiality and security of patient health data cannot be relied on fully. (Evidence that these data security lapses or compromises is already affecting attitudes of large public majorities is reported in the next section.)

(6) Overall Public Perceptions

In February 2005 our IT, Health Records and Privacy Program undertook the first assessment of American attitudes toward interoperable electronic health records. We collaborated with Harris Interactive in a survey of over 1,000 adult Americans

[98] BNA Reports, March 21, 2005
[99] Associated Press, April 6, 2005.
[100] Boston Globe, June 3, 2005.
[101] Associated Press, March 31, 2005.
[102] Pittsburgh Tribune-Review, July 15, 2005.
[103] United Press International, Boulder, Colorado, July 22, 2005.

nationwide on the issue of electronic health data processing. *How the Public Sees Health Records and an EHR System* found that, with only 29% of Americans aware that real work is being undertaken right now on the development of a national health information network, they held strong fears concerning the security of the system and its potential to further increase non-consensual health data sharing and further erode their control over their medical information.

Seven in ten (70%) fear that, in a fully automated and networked system, "sensitive personal medical-record information might be leaked because of weak data security" (with 38% "very concerned"). A similar proportion (69%) was worried that strong data security protections would not be installed in a new system (with 34% "very concerned). The survey showed that fears related to computer errors in medical records persist, with 65% believing that further computerization will increase rather than decrease medical errors. The same proportion predicted that many people are likely to withhold sensitive but vital information from their health care providers because of fears related to its computerization.

Unsurprisingly, the survey found existing concerns relating to the sharing of personal health data applied strongly to health data networking. Almost seven in ten (69%) were concerned that "there could be more sharing of your medical information without your knowledge" (with 42% of those "very concerned" about this potential). Significantly, more than eight in ten respondents (82%) believed that consumer privacy tools should be built into any such system at its inception, with almost half (45%) believing this to be "very important".

These strong concerns persist in what the survey also showed is a generally favorable attitude toward the HIPAA Privacy Rule; almost seven in ten respondents to the survey (67%) agreed that the Rule had increased their "confidence that their personal medical information is being handled today in what they feel is a proper way." However, only 23% said their confidence had been increased "a great deal," while a much larger 44% chose "only somewhat," suggesting that this confidence may result from the mere *existence* of a Federal health privacy regulation – something surveys show the American public has favored since at least 1978.

That such regulation continues to be considered vital can been seen in the finding that 62% of respondents feared that HIPAA protections would be watered down in the name of enhancing the efficiency of the proposed network system.

After describing the new program and then measuring the various concerns about it, the survey posed a "tie-breaker" question. Survey participants were asked to response to the following statement: "Supporters of the new patient Electronic Medical Record system say that strong privacy and data security regulations will be applied. Critics worry that these will not be applied or will not be sufficient. Overall, do you feel that the expected benefits to patients and society of this patient Electronic Medical Record system outweigh potential risks to privacy, or do you feel that the privacy risks outweigh the expected benefits?"

The public divided equally on this fundamental question, with 48% saying the benefits outweigh risks to privacy, 47% saying the privacy risks outweigh the expected benefits, and the deciding 4% describing themselves as unsure. This outcome suggests that half the American public does not feel today that an EHR program is worth the risks to privacy that they perceive as accompanying this development.

Subsequent surveys have confirmed these findings. For example, a March 2005 Harris Interactive/Wall Street Journal Online poll on electronic medical records found wide understanding among Americans of the potential benefits of EHR, such as error and cost reduction and minimization of duplication and wastage in diagnosis and treatment. But it also found high levels of privacy concern, with 67% of respondents agreeing (27% strongly) that "the use of electronic medical records makes it more difficult to ensure patients' privacy".[104]

B. What Needs To Be Done

(1) Empirical Studies of Current EHR Programs

In order to assess both the institutional-level and system-wide effects of EHR and IT applications, new assessments must involve the study of a variety of organizational settings in which such applications are being developed and implemented. Each should be assessed separately, since the patient-organizational and privacy-relationships vary among these settings. But from each sub-set analysis can come a "total system" problems-and-potential-solutions evaluation.

To this end, an empirical assessment must begin by creating a taxonomy of institutions and organizations that are already implementing EHR systems. Any such taxonomy should include the following major contexts in which electronic health record and network experiments and demonstration projects are currently unfolding:

- Single entities (like the Mayo Clinic, the Cleveland Clinic Foundation and the University of California – San Francisco);
- Large, vertically-integrated health organizations (such as Kaiser Permanente's KP Health Connect system);
- Regional, multi-organization contexts (such as the health data exchange operated by the Massachusetts e-Health Collaborative/MAeHC);
- Specific health populations (such as those served by the Department of Veterans' Affairs My Health*e*Vet program, and Yale-New Haven Hospital's ERICCA Project - Electronic Records to Improve Care for Children with Asthma);

[104] K Gullo, "Many Nationwide Believe in the Potential Benefits of Electronic Medical Records and are Interested in Online Communication with Physicians," Wall Street Journal Health Care Poll Newsletter, Volume 4, Issue 4, March 2005

- Workplaces in which employers, such as Pepsico, operate EHR programs;

- Organizations applying anonymization and de-identification techniques in EHR systems to conduct continuing medical and health-care research, such as public health authorities, epidemiological researchers, disease registries, regional research databases, clinical trials, and market researchers.

- Multi-region systems (such as the Connecting For Health Prototype Nationwide Health Information Exchange that will experiment with connecting health communities in Boston, MA, Indianapolis, IN, and Mendocino, CA); and

- Vendor –driven EHR and health data exchange projects (such as IBM's Interoperable Health Information Infrastructure).

A five-phase process, based on the structure of previous assessments, would be appropriate for use in each type of organization studied:

1. **Phase I: The Pre-EHR Application Setting** would describe the collection, storage, use and sharing practices under existing manual and computerized systems prior to the introduction of EHR applications. This process would also describe existing privacy rules and procedures, and identify any unresolved or disputed privacy issues present in the pre-EHR context.

2. **Phase II: The EHR Program** would describe the organization's EHR plan, objectives, and timetable; the extent of deployment thus far; and the privacy rules applied to the new program. This phase would examine the responses of all parties involved in the transition, from medical staff and administrators to technology staff and patients.

3. **Phase III: Impact Assessment** would identify the major changes in health data handling caused by the implementation of the EHR program and would discuss their effects of patient privacy. Specifically, this phase would assess the impact of EHR implementation on:

   - The nature and extent of data collection and storage;

   - Patient control over secondary uses of their medical data;

   - Confidentiality and security of health information;

   - Patients' ability to access, correct and amend their records; and
   - Existing internal health record-related dispute resolution procedures.

   This phase would also note the effects of applying new or existing privacy rules to the implementation and operation of EHR.

4. **Phase IV: Inter-Zone Assessment** would identify changes in the handling of patient data (whether identified or anonymized) *between* Zone 1 (primary care), Zone 2 (payment, quality assurance, fraud control) and Zone 3 (societal uses of health data).

5. **Phase V: Evaluations** would use the data derived from Phases I to IV to discuss the effects of EHR-derived changes in information practices on patient privacy expectations and interests. This phase would assess whether novel privacy risks have been identified that may need to be addressed through new legal or organizational policies.

(2) The right kind of privacy surveys

Properly designed, surveys of patients with experience of real-world EHR programs will show whether networked health data processing tends in practice to exacerbate or alleviate the strong concerns Americans currently have about the concept. These surveys will also pinpoint exemplary privacy protection practices within experimental systems that can and should be included in new standards for the operation of a nationally linked system.

Of course, the quality of a survey depends on many subjective factors: the fairness and balance of the wording of the questions and responses; the placement and order of questions; the timing of the survey in relation to major events; the quality of the sample; the survey methodology (telephone, online, in person); any weighting of responses done by the survey firm; the non-response rate and its effects; and the credibility of the survey summary and analysis.

New surveys in this field should aim to identify the privacy concerns (and perceived benefits) arising from these projects among a variety of health care recipients. Surveys would examine total-public attitudes, experiences, and policy preferences and standard demographic differences (e.g. by age, gender, income, education, race/ethnicity, etc.). But proper surveys will also test how the public divides based on literacy levels, computer and online usage or not, by health status (in good health, managing a continuing health condition, etc.), by nature of health care services and relationships, and other relevant segmentations.

If, (as experience suggests) the traditional telephone survey does not adequately permit the measurement of these nuances, online surveys –with their ability to collect open-ended narrative statements from respondents – would be a powerful tool. Such narrative-collecting surveys should be a part of the patient-experiences empirical study of current EHR programs.

However, while the closed-responses of online surveys can be statistically adjusted to account for the non-Internet using population, this is obviously not possible with narrative data. Therefore, narratives would need to be collected from non-Net users via an alternative mechanism. This suggests that a combination of survey methods should be applied, to produce the fine-grained snapshot of public and involved-patient responses to EHR and networking developments.

(3) Applying Key Standards of "privacy"

As a one-word evocation of a cluster of individual expectations and legal rights, "privacy" is a useful term to focus policy discussions in democratic societies. This is as true in the health care field as in other organizational settings. However, to be truly meaningful and effective, technology-privacy impact assessments in each organizational setting must apply specific privacy concepts and standards that have developed over four decades of information technology and privacy experience.

Two leading sets of personal data handling principles have emerged as the foundation of privacy protection in the context of evolving information technologies: the U.S. Fair information Practices model, and the OECD/EU Data Protection model. At the core of both of these models is a set of five key privacy rights:

- *Notice* - full information to a data subject of what personal information is or will be collected, for what purposes, and with what relevance and level of social acceptability;

- *Choice* - provision of options for the data subject for any secondary or additional uses of his/her personal information by the collecting organization. Typically, choices involve "opt in" or prior-content choices and "opt-out" choices, depending on the types of additional uses involved;

- *Confidentiality/Security* – necessity-limited access to personal data within the collecting organization and the application of data security measures to assure such confidentiality, consistent with the sensitivity of particular data sets;

- *Subject Access* - the right of data subjects to examine the personal information in their files, to seek corrections of any errors and omissions, and to enforce limits on unapproved secondary uses; and

- *Enforcement* - legal mechanisms exercisable through courts and government bodies, as well as intra-organizational procedures to receive and resolve individual privacy complaints.

In the U.S. setting, the Fair Information Practices model has been institutionalized in general laws for the public sector (such as the Federal Privacy Act of 1974 and its state counterparts), as well as in laws for specific private sectors (see discussion above). In the health context, it is important to note that each Zone of health data use implicates a different combination of these rights and practices.

For example, because of an existing strong culture of confidentiality, the most pressing issues in Zone 1 (the direct care context) are likely to be data security and the relevance of the health data sought (especially where providers seek sensitive lifestyle data). In Zone 3, secondary and social uses of health data are more likely to raise questions surrounding notice, choice and access. It will be important in assessing technology impacts to identify and consider the specific dimensions of privacy in any particular context under consideration.

(4) A Sample Privacy Impact Analysis

The complex policy choices involved in the privacy-sensitive operation of EHR systems can be illustrated via a sample privacy impact analysis of the implementation of one of the most fundamental privacy or Fair information Practices standard – that data subjects should have appropriate access to their own records. While the potential "patient empowerment" effects of increased access to personal health information has been hailed as one of the major benefits of an electronic record system, there is growing evidence that patients already feel overwhelmed by the amount of health information they receive.[105] As such, a record design that emphasizes greater direct data access may not, when analyzed deeply, be appropriate or desirable in particular cases, or even for the majority of Americans, or may require an unacceptable level of patient-support services to provide record comprehensibility

A privacy impact analysis of patient access rights in an EHR world begins by identifying the governing policy standard, enumerating its intended benefits, and then considering to what extent the benefits of the policy standard may or may not be realized in real-world contexts.

Privacy Policy Standard: Patients should have the right to see their own medical records, to learn how information in their record has been disclosed, and to challenge the correctness or completeness of information items contained there.

Intended Benefits: Direct access by patients to their computerized medical records may/can:

- increase patient participation in their own health management through active record-checking practices;

- allow patients to verify the accuracy of particular identifying information or transaction items and obtain correction of any errors;

- identify sensitive information that the patient does not want recorded, or wants kept in highly protected confidential status, and to negotiate this process;

- allow the patient to see disclosures from the record, especially to Zone 3 organizations;

[105] See, for example, "Awash in Information, Patients Face a Lonely, Uncertain Road," The New York Times, August 14, 2005

- inform patients about any monitoring of health-condition states, compliance with medication routines, lifestyle changes, or other patient statuses that could affect health or life insurance coverage, employment, licensing, or other consumer or employee relationship; and

- enhance patient confidence in the confidentiality and data security measures applied to his or her medical records.

New Patient Record Access Patterns?

A proper empirical analysis will examine the ways in which patients in current EHR programs are exercising rights to inspect their computerized medical record. Are rates of access the same as when the records were manual, partially automated, decentralized, (etc.) or are there new patterns of patient access in the EHR systems? If there are new patterns, what are the purposes, effects, and – especially – the patient reactions to new access opportunities? Do the new access rights result in more medical errors being identified – and corrected? Do patients who exercise access become more compliant in disease management, lifestyle alterations, etc.? Are there already problems in administering patient access rights (see below)?

Privacy Realities and Issues to Resolve

An empirical analysis poses a series of policy questions, and then looks to see whether current EHR programs offer evidence of how those issues are unfolding in practice.

- ***Record comprehensibility.*** Most consumer and citizen records are comprehensible on their face, or, like credit reports, are put into understandable formats in the process of providing consumer access. Medical records, however, beyond personal identifiers and narrative materials, are organized around technical notations, medical jargon, laboratory results, and diagnostic terms of art. How will enhanced access to computerized records be made understandable to patients? Will this require extensive and expensive personal counseling, by physicians, patient representatives, or other counselors? Is this being built into the EHR system under consideration?

- ***Non-Computer Using Populations.*** Roughly 165 million American adults go online today, but about 60 million adults do not go online or don’t use computers. How will this segment of the patient population be serviced in terms of record access? Again, will this require extensive and expensive support services, and is this being built into the EHR system under consideration?

- ***Access Limitations.*** Will there be types of information and reports in the computerized medical record that, by policy or law, patients will not be entitled to see or which can be screened off by health professional decision? Will patients be fully informed at the outset of the medical record automation about such limitations? Will there be types of patients or types of medical conditions for which there would be limited access to one's own records? And will there be procedures by which patients can seek exceptions to such limited access, or to have the exclusions lifted?

- ***Patient Access Costs and Security.*** Will patients be given unlimited direct access rights (and procedures) to examine their records? How will secure identification be arranged? How will encrypted materials be unencrypted? Will patient direct access be a free service or will there be charges to the patient for such usage? Will a certain amount of patient access be free but extensive accessing require payment?

This sample privacy impact examination underscores the complexities of managing privacy interests in a computerized and networked medical record environment. Properly balancing the benefits of the system to patients with its privacy risks will require a detailed and nuanced approach. Since some Fair Information Practices or privacy rights that function well in the consumer-business, employer-employee, and citizen-government contexts will not translate so obviously to the health care and health-system administration context, an empirical analysis seeks to identify those special health care dimensions, and to analyze how fundamental privacy goals can still be achieved.

(5) Addressing Data Security and ID Theft

Data security is the process by which an organization keeps its promises of confidentiality, against threats from internal and external assailants. However, no large-scale personal-data system with multiple users and continuing flows of data communications and processing can guarantee – and deliver – unfailing security.

What can be done to greatly minimize health information privacy breaches in a national system of electronic health records and networks is to construct a combination of protections – clear legal duties, stiff penalties for violators, application of biometric identifiers for both health-organization employees and individual patients, strong data system access and audit controls, wide use of encryption for sensitive data, an independent regulatory agency oversight of data-security practices, and provision of compensation for victims.

Of course, such confidentiality and security measures will create significant costs for health organizations, and will interfere with what many system developers might like to do in building fast and powerful EHR systems. But unless reasonable representatives of consumers and patients are convinced that EHR systems are trustworthy in practice, thereby alleviating the concerns of a currently highly skeptical public majority, fears about the confidentiality and security of patient information will be a major brake on EHR development.

(6) How to Approach Secondary and Social Uses

Over the past three to four decades, there have been significant debates over privacy issues in Zone 3 settings. Examples include: how employers require and use employee health information; how health and life insurers use health information in their underwriting and pricing processes; when law enforcement officials can obtain access to medical records for criminal investigations; when there must be compulsory reporting of medical conditions for public health, child-abuse detection, and other society-protecting efforts; when medical researchers may have access to medical records for clinical trials and epidemiological studies; and many other major activities.

As already described, American society has called for and obtained important limitations on how personally-identified medical data may be required or used by particular Zone 3 organizations. Examples include legal rules for exclusion of genetic test data for health or life insurance or employment, or patient advance-consent requirements for medical researchers to access medical records. As we have also noted, there are debates in process over whether federal HIPAA Privacy Rules have addressed Zone 3 privacy standards sufficiently, and many states have enacted and continue to propose further health privacy laws affecting various Zone 3 activities.

As a matter of pragmatism, we believe an empirical study of EHR and Data Network effects does not call automatically for a program of re-writing health privacy rules for all or most Zone 3 settings. This would stir a whirlwind of legislative and political battles, and would surely use up limited privacy reform capital resources. Rather, we believe the policy focus should be on:

- whether record computerization and networking *are creating* or *will definitely create* significant changes in the scope of data collection or types of uses of personal health information in Zone 3 decision-making;

- whether this has positive effects on the social processes of that Zone 3 activity; and

- whether there are privacy effects that are adverse and are not justified by the balancing process among privacy, disclosure, and surveillance that is the heart of all privacy policy-making.

In short, identification of needs for new privacy rules in Zone 3 settings should be based on actual identified changes in personal health information acquisition and uses and whether these in fact represent significant new privacy harms.

CONCLUDING PERSPECTIVES

In the opening of this paper, we expressed our judgment that this decade will see a major transformation of personal health data handling into heavily computerized patient records and implementation of national electronic networks. Our sense is that this is not a matter of whether but when and how. And, we have indicated that – unless a significant privacy program is developed and installed as part of the initial rollout – EHR and Network programs risk high public as well as potential legislative resistance.

So what suggestions can be added to what has already been proposed?

(1) Multiple Assessments by a Variety of Assessors

Fortunately, given the long history of American efforts to implement health IT, there already exist numerous past studies of IT's potential impact on privacy, and of suitable ways to mitigate adverse privacy impacts. These studies may serve as a valuable starting point for current work on ensuring that an electronic health data network does not increase the risk of misuse or mishandling of patient information.

Going forward, the magnitude and complexity of current EHR efforts suggests that there will be a need for impact assessments of various aspects of the new technologies conducted by a variety of different groups. Ideally, there will be alternative empirical studies, some by government bodies, some by health professional organizations, some by technology vendors (especially on data security issues and choices), some by consumer, patient, and privacy groups; some by health system research specialists; some by legal experts; and some by experienced privacy-beat reporters in the mass and specialized media.

From these types of empirical and policy-analysis studies across the next 4-6 years, we should be ale to assemble a solid estimate of the privacy impacts of EHR and Data Network programs – and to conduct the policy debates that these snapshots will frame.

2. Informing and Involving the Public

Surveys undertaken over the past several decades have given us a clear picture of the dimensions of health privacy concern among Americans, showing that these concerns are not uniform across patient groups, and that there is a much higher level of trust in direct providers of health care than in others who handle personal health information. They also show significant levels of concern over the increasing circulation and sharing of health data among all three "Zones" – something that may be greatly amplified within an electronic health data network.

If patient trust is to be gained, and the claimed benefits of the network to be realized, these insights must be incorporated at the start into new policies for health information use and sharing. Above all, patients must be made part of the development process, and continual efforts must be made to ensure that they are fully informed and able to participate.

The proposed developments have the potential to raise serious concerns among the American public, which in many cases will not dissipate unless the public is provided with specific details. Any system created and operated in the absence of appropriate public notice and patient input will be dogged by mistrust. And if participation is intended to be voluntary, a top-down, non-consultative process may be doomed to mass avoidance and failure.

3. And Privacy is not absolute

As the EHR and Network programs proceed, we must recognize that privacy is not and cannot be an absolute in a democratic society. Public disclosure of some personal information for social and political purposes and for protection of individuals and society are always valid, competing interests to be balanced. That the claims to privacy and choice in personal disclosures are especially high and important in the health care field does not mean that they can, or should, always prevail over all competing interests.

Now is the time for those involved in current health IT developments to develop a specific mechanism for balancing interests in a new electronic health data network. Achieving balances that a majority of the American public, as well as the health care community, can embrace as the best possible (though never perfect) system will be vital to the future development and operation of any future national electronic network.

****

APPENDICES

THE PROGRAM ON INFORMATION TECHNOLOGY, HEALTH RECORDS AND PRIVACY

Our Program will conduct seven ongoing activities, all centered on the privacy aspects of current developments in health information technology adoption:

- Conduct continuing public opinion surveys of the public and various leadership groups, with Harris Interactive as our survey partner.

- Conduct empirical case studies of the privacy experiences in emerging health information technology experiments and programs.

- Develop legal and policy analyses of the privacy, confidentiality, subject access, and due process aspects of a national or decentralized-model EHR system.

- Track the privacy rules and experiences in EHR projects of other democratic nations.

- Publish Reports and Reports, and develop an Electronic Newsletter.

- Organize seminars and conferences on program themes.

- Provide privacy advisory services to organizations planning or conducting EHR programs, technology firms providing EHR-oriented services, and government agencies reviewing and funding EHR programs.

Program Resources Available

The Program's home page can be accessed at www.privacyexchange.org. Resources available at the Program's home page include:

- The report of our February 2005 Harris Interactive survey of the public's attitudes toward HIPAA safeguards, EHR and privacy;

- Dr. Alan Westin's February 23, 2005 testimony on privacy issues in a EHR program at the NCVHS Subcommittee on Privacy Hearing on Privacy and Health Information Technology in Washington, D.C.;

- Our analysis of sixteen national surveys of health care and privacy, How The Public views Health Privacy: survey Findings From 1978 to 2003"; and

- This Report, August, 2005.

We invite those interested in following our work and accessing our resources to register at the Program site (with the protection of our strong privacy policy) and to share their thoughts and reactions with us.

Staff

Program on Information Technology, Health Records, and Privacy
An Activity of the non-profit Center for Social and Legal Research

Director
Dr. Alan F. Westin, LLB, PhD
Professor of Public Law & Government Emeritus, Columbia University

Associate Director
Vivian van Gelder, LLB

Counsel
Robert R. Belair, LLB

Legal Staff
John Haley, LLB
Lyle Himmel, LLB
Kevin Coy, LLB

Program Administrator
Lorrie Sherwood

Communication Director
Irene Oujo

Research and Editorial
Natalie Kochmar

Administrative Assistant
Julie Previzi

Webmaster
Hillary Sherwood

Survey Organization
Harris Interactive

Contacts: Mail: Suite 414, Two University Plaza, Hackensack, N.J. 07601
Tel. (201) 996-1154 Fax (201) 996-1883 email: ctrslr@aol.com
Dr. Westin's direct email – alanrp@aol.com

AUTHOR BIOGRAPHIES

Dr. Alan F. Westin
Director, Program on Information Technology, Health Records and Privacy

Dr. Alan F. Westin is Professor of Public Law and Government Emeritus at Columbia University, where he taught for 37 years. He is the founder of the Center for Social & Legal Research and President of its ***Privacy & American Business*** activity. Dr. Westin is the author or editor of 26 books on constitutional law, civil liberties, American politics, and privacy, and has been listed in Who's Who in America for three decades. In 2005, he received the Privacy Leadership Award of the International Association of Privacy Professionals, the nation's leading organization for privacy officers in business, government, and the non-profit sector.

Professor Westin's first major books on privacy – Privacy and Freedom, published in 1967, followed by Databanks in a Free Society 1972 (for the National Academy of Sciences)– are considered seminal works on privacy. Each correctly predicted how advances in data surveillance of the mid-1960s and new computer and telecommunication applications of the 70s would affect American organizations that keep records about consumers, employees, and citizens, from hospitals, health and life insurers, credit bureaus, banks to colleges, police, and welfare agencies. Both books called for creating new laws, new organizational policies, and continuous new-technology privacy assessments in the governmental, business, and non-profit areas, if basic privacy values and rights were to be preserved in an increasingly information-technology driven world.

Dr. Westin is a leading authority on consumer-privacy public opinion surveys, and in understanding and interpreting the privacy attitudes of the American consumer. He has worked with Louis Harris & Associates (now Harris Interactive) and Opinion Research Corporation on over 50 national surveys since 1978 exploring consumer privacy issues. He has created privacy indices, which are universally used and quoted. His reports on consumer privacy concerns and attitudes have been featured in the New York Times, Wall Street Journal, Consumer Reports, and dozens of other national publications, and he is a frequent commentator about consumer privacy on national television and radio.

Dr. Westin was the principal expert witness in the enactment of the first two national privacy laws in the United States – the Fair Credit Reporting Act of 1970, providing consumer rights in the credit-bureau industry, and the Federal Privacy Act of 1974. Over the past forty years, he has been a member of U.S. federal and state government privacy commissions; an expert witness before legislative committees and regulatory agencies; and a privacy consultant to many U.S. federal, state, and local government agencies, such as, at the federal level, the Census Bureau, Social Security Administration, General Services Agency, Department of Commerce, and Office of Technology Assessment.

Dr. Westin has also advised many consumer-product companies, including IBM, American Express, Citicorp, Bell Atlantic, Empire Blue Cross and Blue Shield, Equifax, Microsoft, Chrysler, and Prudential Insurance, on privacy governance and policies within their companies as they effect their consumer-business relationships.

Health Information Privacy Activities
Since the mid-1960s, Professor Westin has maintained a continuing special interest in medical confidentiality and health-information-systems privacy issues.

A comprehensive field study of computerization trends and health information was led by Dr. Westin for the U.S. National Bureau of Standards between 1974-76, and produced Westin's report on Computers, Health Records, and Citizen Rights (1976). The Privacy Code this report recommended was sent by NBS to every hospital in the U.S., and served as a model for hundreds of hospital and health institutions. The NBS Report was the leading empirical study of how computer use in the late 1960's and early 1970's was affecting the three main zones of health information use – direct care, payment and quality-assurance, and social uses of medical data.

Between 1978 and the early 1980s, he served as Research Director of the National Commission on Confidentiality of Health Records, a national association composed of the major health-care provider, payer, and quality-care associations in the United States. During this period, he spoke frequently on privacy and health information issues at national conventions or special meetings of the American Medical Association, Health Insurance Association, American Medical Records Association, American Orthopsychiatric Association, American Psychiatric Association, and many other health-professional groups.

Dr. Westin has been a featured speaker at the U.S. Department of Health and Human Services Privacy Task Force Conference on Medical Records and Privacy (February 1993); a reviewer of reports on privacy for the National Institute of Medicine (on emerging regional health data systems), the Journal of the American Medical Association, and for the U.S. Office of Technology Assessment (on privacy and the computerized medical record).

Dr. Westin was the privacy advisor to an award-winning 1994 Public Television Special Documentary on "Privacy and Health in the American Workplace." Dr. Westin drafted a national corporate-employee and human resources executives survey conducted by Louis Harris and Associates for use on this program, covering employee health and privacy issues in depth.

In 1993, he served as the academic advisor for a national public and leaders Harris survey on "Health Information Privacy." Results from this survey were released at a national conference in Washington, D.C. in November 1993, at which Dr. Westin spoke, co-sponsored by the U.S. Office of Consumer Affairs, the American Health Information Management Association, and Equifax Inc.

Also in 1993-95, Dr. Westin served as Principal Investigator on a 15-month project on privacy issues in the uses of genetic testing and genetic-test applications, funded by the

U.S. Department of Energy for the Human Genome Project and its ELSI Program (Ethical, Legal and Social Issues). In 1997-99, he led a study of future uses of genetic testing in the Life Insurance Industry, commissioned from the Center for Social and Legal Research by State Farm Insurance Company.

Over the past three years, Dr. Westin has led discussions of the HIPAA Privacy Rules at many national conferences. He has been a privacy consultant to several major pharmaceutical companies, from Eli Lilly, Glaxo Welcome and Smith Kline to Merck.

He was also privacy consultant to Empire Blue Cross, Blue Shield; State Farm Insurance; and Mutual of Omaha. Dr. Westin also led a Global HR Privacy Policy Development project of Privacy & American Business, covering trans-border personnel data flows of multi-national firms that involved the worldwide handling of medical and health data by those companies.

In January 2005, Dr. Westin created the Program on Information Technology, Health Records and Privacy. Its first activity is the release of a new survey in February 2005, “How the Public Sees Health Records and an Electronic Medical Record Program,” for which Dr. Westin served as Academic Advisor.

Dr. Westin views the re-shaping of the nation’s health care system through advanced technology applications as one of the most important technology-society developments of the next two decades. It will be a priority of the new Program to help insure that privacy interests and patient empowerment are embedded in any new Electronic Medical Record systems -- from the start.

VIVIAN VAN GELDER
Associate Director

Vivian van Gelder is an Australian-trained, New York Bar-certified attorney who has been, since 2002, a staff attorney and international writer and editor at Privacy & American business and the Center for Social and Legal Research.

Ms. van Gelder is responsible for tracking and reporting on privacy and data protection developments around the world, and works with Dr. Alan Westin to coordinate the activities of the Center’s Japan-U.S. Privacy and Data Protection Program.

Ms. van Gelder has also taken part in a privacy risk assessment for the HR division of a major American multinational, and monitors health data protection laws and regulations around the world.

Coming, as she does, from a family of health care professionals, Ms. van Gelder brings a unique perspective to policy issues in health information management. She is currently working with Dr. Westin as Associate Director of the Center’s Program on Information Technology, Health Records and Privacy, and is the co-author of this Report.