5125

TOWARD A NATIONAL HEALTH INFORMATION INFRASTRUCTURE

Report of the Work Group on Computerization of Patient Records

To the Secretary of the U.S. Department of Health and Human Services

April 1993,

TOWARD A NATIONAL HEALTH INFORMATION INFRASTRUCTURE

Report of the Work Group on Computerization of Patient Records

To the Secretary of the U.S. Department of Health and Human Services

April 1993

Work Group on Computerization of Patient Records

Work Group Staff

American Hospital Association
Thomas Granatir, Chairman3 12-280-6183
Joanna DePorter

Members

Aetna Health Plan
Steve Brooks
Cary Sennett, M.D.

American Association of Retired Persons
William Decker

American Group Practice Association
Cori Ofstead
Kristin Swyers

American Health Information Management Association
Margret Amatayakul

American Hospital Association
Donna Ganzer
Sandy Metzler

American Medical Association
Jerome Seidenfeld, Ph.D.

American Nurses Association
D. Kathy Milholland, Ph.D., RN

Blue Cross and Blue Shield Association
Shirley Kellie, M.D.

Blue Cross Blue Shield of Iowa
Scott McCracken

Bridgman Consulting
Shel Bridgman

Group Health Association of America
Robert Giffin, Ph.D.
Dennis Hodges

Healthcare Information and Management Systems Society
John Page

Health insurance Association of America
Kathleen Fyffe

Medical Group Management Association
Steven S. Lazarus, Ph.D.
Randy Teach

Kaiser Permanente
Alex Au-Yeung
Simon Cohn, M.D.

The Joint Commission on Accreditation of Healthcare Organizations
Paul Schyve, M.D.

The Travelers Insurance Company
Garry Hurlbut

Washington State Hospital Association
Tom Byron

Observers

Agency for Health Care Policy and Research
Michael Fitzmaurice, Ph.D.

Defense Advanced Research Projects Agency
John Silva, M.D.

General Accounting Office
Ira Sachs

Health Care Financing Administration
Dick Lyman
Nicole Simmons

EXECUTIVE SUMMARY

Background

In November **1991,** the Secretary of Health and Human Services convened a forum of health care leaders to identify ways to reduce health care administrative costs. After the forum, the following working groups were created: the Work Group for Electronic Data Interchange, the Work Group on Administrative Costs and Benefits, the Work Group on Performance Monitoring, and the Work Group on Computerization of Patient Records. The latter work group, including organizations representing patients, providers, purchasers, evaluators and health policy experts, was assembled by the American Hospital Association to identify practical steps towards the implementation of computer-based patient records.

Current Environment

Today, patients' health information is often fragmented, poorly documented and duplicative. Information about a single episode of care could reside in the records of several different providers -- history and symptoms in a physician record, lab results and surgical procedures in a hospital record, and rehabilitation in a home care agency record. Even within a single provider location, such as a hospital, information about a patient may be contained in different departmental systems, some of which are computerized, some of which are not, and few of which are integrated due to the lack of standards for defining, coding and transmitting data.

Generally, providers have been unwilling to invest large sums of money in information systems without assurances that the costs will be justified by the benefits. Several advanced computerized patient record systems have been successfully installed in hospitals and ambulatory care settings but few have been widely replicated and information about the costs and benefits is limited. In particular, there is little scientific evidence to prove that CPR systems will reduce administrative costs. There are, however, several studies that show the CPRs can lead to better quality and more efficient patient care management (e.g., fewer lab tests, shorter lengths of stay).

Vision

This work group believes that we must harness the capabilities of computers to improve the quality and efficiency of patient care. More complete and accurate patient information will become available across time and place (with appropriate safeguards for patient privacy). Caregivers will have access to practice guidelines, prompts, reminders, and other decision support tools to enhance diagnosis and treatment and to evaluate the likely outcomes of alternative treatment options. Patients and purchasers will be able to obtain information on the cost and quality of health plans and providers. Researchers, regulators, health plans, evaluators, and policymakers will have access to data to support decisions about health care delivery and financing and evaluating the effectiveness of emerging health care technologies. Costs will be reduced by eliminating redundant functions and streamlining inefficient processes.

In order to achieve our vision, we need a **health information infrastructure** -- an interconnected communication network linking all participants in the U.S. health care system. Each health care facility and practitioner would connect to the network via its own **computer-based patient record system** -- an information system that would have the ability to create, store, retrieve, transmit, and manipulate patients' health data in ways that best support decision making about their care. In addition, support for better patient care decision making and analysis of patient outcomes would be available through **reference data bases** -- aggregate data from many patients -- and computerized knowledge-based **systems** which use decision logic and practice guidelines to help caregivers make decisions about diagnoses and treatment options. As they do today, health care providers would control access to information stored in patient records in order to preserve patient privacy. When authorized, data from such a system could flow to health care managers, policy makers, researchers, and purchasers to monitor the performance of the health care system and make key decisions for the future.

Strategies

We believe that with a well-planned, adequately financed, and incremental approach, this vision is attainable in the next ten to fifteen years. The strategies we propose represent first steps in the development, adoption and use of CPR systems and the health information infrastructure.

- **Develop national standards for documenting and sharing patient information.** The American National Standards Institute Healthcare Information Standards Planning Panel (HISPP) should coordinate the development, adoption, and use of national information standards. Standards should be developed for patient data definitions, codes and terminology, for inter-system communication, and for uniform patient, provider, and payer identifiers.

- **Establish national standards for protecting the confidentiality of patient information.** Enact federal legislation applying to all health information which resolves inconsistencies and inadequacies in existing laws protecting patient privacy and creates a Federal Information Privacy Commission to establish uniform requirements for protecting health information.

- **Improve knowledge about the state-of-theart.** Better information should be collected and made available about what kind of information systems providers have, how much systems cost, how much they save, how they could be used more effectively, and how they could be improved.

- **Promote development of interconnected communication networks.** Federal funding should be provided to support the development of health information networks that operate to share health information between providers and others within a community. Members of the health care community should collaborate with other industries and government to develop health care information technology that is compatible with the

emerging national information infrastructure that would link, through a national "information superhighway," institutions and resources throughout the country.

- **Evaluate the usefulness and cost-effectiveness of all data requests.** Regulators, insurers, and others should take responsibility for demonstrating the reliability, validity, usefulness and cost-effectiveness of data sets before requiring that they be collected and reported.

The table below outlines our proposed strategies, identifies a lead organization for each, and estimates the associated time frame and cost.

Summary of Proposed Strategies

STRATEGIES	LEAD ORGANIZATION	TIME FRAME	ESTIMATED COST
I. IMPROVE KNOWLEDGE ABOUT STATE-OF-THE-ART			
LA. Conduct provider surveys	Computer-based Patient Record Institute (CPRI)	1993-1994	$800,000
LB. Develop reference model for evaluating costs and benefits of CPR systems	Department of Health and Human Services (HHS)	1993-1996	$3 million
I.C. Analyze information needs and uses in a variety of provider settings	CPRI	1993-1996	$15 million
I.D. Evaluate issues related to organizational, professional and personal change	CPRI	1993-1996	$3 million
II. DEVELOP NATIONAL STANDARDS			
II.A. Promote development, adoption and use of health information standards			
II. A. 1. Fund HISPP standards planning and coordination	HHS	Ongoing	$100,000/year
II.A.2. Develop, test and promote use of a patient data set for emergency purposes	Healthcare Informatics Standards Planning Panel (HISPP)	1993-1995	$500,000
II.A.3. Develop standards for the content of the patient record	HISPP	1993-1996	$100,000

STRATEGIES	LEAD ORGANIZATION	TIME FRAME	ESTIMATED COST
II.A.4. Compare and contrast coding schemes and develop needed coding schemes	HISPP	1993-1996	$500,000
II.A.5. Develop uniform provider, payer and patient identifiers	HISPP	1993-1994	$50,000
II.A.6. Foster development of standards certification process	CPRI	1993-1994	$50,000
II.B. Establish national legal standards for protecting the confidentiality of patient information	Congress/President	1993-1994	
II. C. 1. Evaluate existing data sets	HHS	1993-1996	$1.5 million/yr
II.C.2. Enact legislation requiring federal agencies to demonstrate the usefulness and cost effectiveness of any mandated data set	Congress/President	1993-1995	
III. DEVELOP LINKAGES BETWEEN EXISTING AND FUTURE COMPUTER-BASED INFORMATION SYSTEMS			
III.A. Encourage development of community health information networks	HHS/CPRI	1993-1996	$25 million
III.B. Collaborate with other industries and government to create the health care component of the National Information Infrastructure	CPRI	1993-ongoing	
TOTAL COSTS		1993-1996	$54.4 million

Implementation Timeline

Below, we have attempted to lay out an estimated timeline for widespread, national implementation of CPR systems and the health information infrastructure. Although a timeline suggests a sequential process of development and implementation, we expect many of the components to be developing simultaneously.

YEARS 1 - 4

Standards. The most important step toward the implementation of computer-based patient records (CPR) is the development and adoption of standards for defining, coding, and transmitting health care data so that information can be shared between systems.

- Adoption of existing standards
- Development of needed standards for defining, coding and sharing patient data
- Enactment of federal legislation protecting confidentiality of patient information
- Development of national standards for the creation, authentication, and storage of patient health records

Research and Development. Also needed is better information about currently implemented systems to help system developers design better systems and to help providers evaluate their system needs. We believe this can be supplied by an aggressive program of demonstrations and evaluation.

- Development of models for evaluating CPR systems
- Demonstrations of emerging CPR systems
- Early demonstrations of linkages between users of patient information within communities
- Continued development of decision support tools (e.g., practice guidelines, performance indicators)
- Development of strategies for training health care professionals in the use of CPRs

YEARS 3 - 10

Evaluation and Initial Implementation. Once standards have been adopted and information has been made widely available about the attributes of successful systems, we expect community health information networks to become more widespread, and systems to become more responsive to user needs. Demand will increase accordingly and systems will proliferate.

- Continued development and adoption of standards
- Replication and evaluation of demonstrations of CPR systems and community networks
- Dissemination of information about successful implementation of CPR systems and community networks
- Increased use of knowledge based systems and reference data bases (for direct patient care, outcomes analysis, etc.)
- Increased focus on CPRs in education and training of health care professionals
- Greater use of high speed communication highways for health care applications

YEARS 9 - 15 AND BEYOND

National health information infrastructure. Realization of the full potential of computer based record systems demands not only that information be captured and stored in computers but that it be accessible to authorized users across time and place. A national high speed

communication highway is needed to enable all participants in the U.S. health care system to communicate electronically.

- Widespread acquisition and implementation of CPR systems
- Widespread establishment of community information networks
- Ongoing refinement and integration of CPR systems, knowledge based systems, and reference data bases
- National availability of high speed communication highway

Toward a National Health Information Infrastructure

Work Group on Computerization of Patient Records

APPENDIX

Abbreviations

AHCPR	Agency for Health Care Policy and Research
ANSI	American National Standards Institute
CPR	computer-based patient record
CPRI	Computer-based Patient Record Institute
HCFA	Health Care Financing Administration
HHS	Department of Health and Human Services
HISPP	Healthcare Informatics Standards Planning Panel

INTRODUCTION

The cost and quality of health care are currently of major concern to the American public. Ways to improve the value of care -- what quality can be purchased for what cost -- are at the forefront of today's health reform agenda. The Work Group on Computerization of Patient Records represents a large segment of the providers, purchasers, evaluators and consumers of health care in this country. We are united in our belief that one major way to improve the value of care is to create a national **health information infrastructure.**

By such an infrastructure we mean an interconnected communication network linking all participants in the U.S. health care system. Each health care facility and practitioner would connect to the network via its own **computer-based patient record system --** an information system that would have the ability to create, store, retrieve, transmit, and manipulate patients' health data in ways that best support decision making about their care. As they do today, health care providers would control access to information stored in patient records in order to preserve patient privacy. When authorized, data from such a system could flow to health care managers, policy makers, researchers, and purchasers to monitor the performance of the health care system and make key decisions for the future.

By increasing the accuracy, completeness, and accessibility of patient information, this infrastructure can **improve quality, increase efficiency, and control costs** within our health care system. Such an infrastructure would move this country toward these goals even within the current fragmented structure of the health care system, and would be critical to the success of any of the health reform proposals currently being advanced that envision better coordinated health care delivery. For such coordination to occur, information about patients must move smoothly across times, sites, and providers of care. To become more efficient, providers must have accurate, detailed, and timely information about their performance. And, to help purchasers and consumers make decisions about health plans and providers, information must become available about the cost and quality of care. The infrastructure we propose would supply all of this information.

National enthusiasm about computer-based patient records and an expanded information infrastructure has grown considerably over the past year. However, there are currently many impediments to achieving computerized patient records, and to developing a health information infrastructure to support them. If important policy, technical, operational, and financial issues are not addressed up front, the costs of implementing this infrastructure might surpass the benefits we are able to derive from it.

This report represents our thoughts, and those of the experts we consulted, about how this country should undertake its pursuit of computerized patient record systems, After explaining the impetus behind the creation and mission of this work group, we will describe our vision of a health information infrastructure and will examine the challenges and opportunities posed by the current environment. Finally, we will propose specific strategies to meet these challenges and achieve our goals.-

BACKGROUND

In November 199 1, the Secretary of Health and Human Services brought together health care leaders to discuss ways to reduce administrative costs in our health care system. In addition to such issues as reducing inefficiencies associated with utilization review and billing, one of the key items on the agenda was the automation of patient information. At the forum, the following working groups were formed: the Work Group for Electronic Data Interchange, the Work Group on Administrative Costs and Benefits, and the Work Group on Performance Monitoring and the Work Group on Computerization of Patient Records (see Appendix A for a description of each working group).

The Work Group on Computerization of Patient Records, assembled by the American Hospital Association, included organizations representing patients, providers, payers and health policy experts (a complete listing of work group participants appears at the front of the report). Recognizing the far-reaching implications of CPRs for each of these organizations, the mission of this work group was to:

- Define the vision of computer-based patient records from the perspective of the many groups represented on the work group.

- Identify practical steps in a broadly constituted strategy to support the development and implementation of computer-based patient records in our current and future health care environment.

THE VISION

This work group believes that we must harness the capabilities of computers to improve the quality and efficiency of patient care. More complete and accurate patient information will become available across time and place (with appropriate safeguards for patient privacy). Caregivers and patients will have access to practice guidelines, prompts, reminders, and other decision support tools to enhance diagnosis and treatment and to evaluate the likely outcomes of alternative treatment options. Patients and purchasers will be able to obtain information on the cost and quality of health plans and providers. Researchers, regulators, and evaluators will have access to data to support decisions about health care delivery and financing. Costs will be reduced by eliminating redundant junctions and streamlining inefficient processes.

To achieve this vision, we need a health information in&structure consisting of several components. At the heart of the infrastructure are computer-basedpatient record (CPR) systems -- computerized information systems maintained by providers to capture, store, retrieve, transmit, and manipulate patient-specific health care-related data, including clinical, administrative, and payment data. Using standard definitions, codes, and formats that enable data to be universally recognized and processed, CPR systems would be linked (with appropriate mechanisms allowing patients and their providers to control access to information) through high-speed communication highways capable of transmitting multi-media data (including voice, image, and text) electronically.

Support for better patient care decision making and analysis of patient outcomes would be available through reference data bases -- aggregate data from many patients (without traceable patient identifiers) -- and computerized knowledge-based systems which use decision logic and practice guidelines to help caregivers make decisions about diagnoses and treatment options and evaluate outcomes of health interventions. For example, a knowledge-based system can identify radiologic and bacteriologic evidence of a disease, identify potentially dangerous drug interactions, and suggest therapeutic interventions. These knowledge-based systems may be developed and maintained by individual provider organizations or developed regionally or nationally (e.g., National Library of Medicine) and shared by many organizations.

We embrace the vision described by the Institute of Medicine in its report ***The Computer-Based Patient Record: An Essential Technology for Health Care'. The*** IOM defines the CPR as "an electronic patient record that resides in a system specifically designed to support users through availability of complete and accurate data, practitioner reminders and alerts, clinical decision support systems, links to bodies of medical knowledge and other aids." This definition has led to some confusion because for many the term "computer-based patient record" has a strong but narrower intuitive meaning: the storage of a patient's paper health record in a computer. For clarity's sake, we distinguish the **computer based-patient record** -- which would consist of all

THE CURRENT ENVIRONMENT

National enthusiasm for the concept of computer-based patient records has grown considerably over the past year. The evidence of widespread public and private support includes:

- Publication of the Institute of Medicine (IOM) report, ***The Computer-Based Patient Record: An Essential Technology for Health Care*** in July 1991.[2] This report, which received widespread attention and acclaim, expressed strong support for the development and adoption of computer-based patient records.

- The establishment of the Computer-Based Patient Record Institute (CPRI) in early 1992. CPRI's mission is to "initiate and coordinate urgently needed activities to facilitate and promote the routine use of computer-based patient records throughout health care."[3] The CPRI board includes provider groups, medical informatics experts, businesses, vendors, and insurers (a description of CPRI's mission, goals, structure and membership is included in appendix B). Since its inception, the CPRI has established several working groups to examine issues such as standards, confidentiality, and professional education. Because of its mission and broad representation, the Work Group on Computerization of Patient Records believes that the CPRI is well positioned to take the lead in carrying out many of the recommendations made in this report.

- Provisions to hasten the adoption of computerized patient information systems have been included in several Congressional health reform proposals. Senator Christopher "Kit" Bond, R-MO introduced the Medical and Health Information Reform Act of 1992 (S.2878) which would have defined a clinical data set that hospitals would be required to provide electronically to Medicare Peer Review Organizations to streamline their quality and utilization review activities. Representative Fortney "Pete" Stark, D-CA introduced the Health Administrative Simplification Act of 1992 (H.R. 4956) which would have required the development of standard formats for electronic billing, the use of electronic health insurance cards, and the establishment of regional claims clearinghouses to process all claims. Representative Stark reintroduced a similar bill, the Health Care Cost Containment and Reform Act of 1993 (H.R. 200), in January 1993.

- The Department of Health and Human Services (HHS) has demonstrated its enthusiasm through various patient information system initiatives, including (1) proposing legislation in 1992 under the Bush Administration calling for the development of a "nationwide electronic health care information network" and the implementation of computerized patient record systems in hospitals by 1996 and (2) creating the HHS Computerized Patient Record Council to coordinate departmental activities related to computerized patient records.[4]

- The Computer Systems Policy Project (CSPP), an affiliation of chief executive officers of computer hardware companies, is calling for a public-private partnership to develop and deploy a national information infrastructure that would link institutions and resources throughout the country and internationally. The CSPP has advocated a national infrastructure that includes:

Interconnected and interoperable public (e.g., telephone lines) and private (e.g., internal corporate networks) communication networks.

Technical standards for linking the pieces of the network.

Easy to use, powerful personal computers and workstations, including those that respond to handwritten or spoken commands.

Software applications and data bases (public and private) that are widely accessible over the network (which acts like a lending library).[5]

Although envisioning an infrastructure that would support a wide variety of applications, the CSPP has highlighted potential improvement in health care delivery as one of the key benefits that would result from such an infrastructure.

- Most recently, strong support for computerization of health information has come from the Clinton Administration. The Administration's plan for investing in technology specifically mentions the need to improve access to information in health care as one of the driving forces behind the development of a national information infrastructure and "information superhighway." The President's plan includes:

  Implementation of the High Performance Computing and Communications Program* to fund development of more powerful computers, a national high-speed computer network, and more sophisticated software.

  Creation of a Task Force on Information Infrastructure, a high-level inter-agency task force within the National Economic Council, to work with Congress and the private sector on identifying and implementing policy changes needed to accelerate the formation of a national information infrastructure.

  Creation of an Information Infrastructure Technology Program to assist industry in the development of advanced hardware and software in health care, manufacturing, education, and libraries.

  Provision of funding for networking pilot projects to demonstrate the benefits of linking schools, health care facilities, governments, and other public information producers. The Administration proposes to make $64 million available to the Department of Commerce's National Telecommunications and Information Administration to fund these networking pilot projects.

* The High Performance Computing Act of 1991, introduced by Vice President Gore when he served in the Senate, authorized $2.9 billion in financing over five years for research, development, and support of the National Research and Education Network through which industry and academia are developing technologies for a data superhighway.

We welcome the increasing support for computerizing patient information. We recognize, however, that many challenges must be overcome before we can hope to achieve our vision. Some of these challenges are discussed below.

There is no example of a fully automated CPR in use today. The Institute of Medicine describes a handful of systems "that might qualify as today's CPR systems." The features shared by these systems include maintaining a large data dictionary, tagging each transaction with the time and date, allowing flexible data retrieval and reporting, and offering a research tool for using the data.[6] All of the systems highlighted in the IOM report, as well as several others not mentioned in the report, have an impressive list of functions and features, but all have limitations and none can currently support all aspects of our vision. Furthermore, most were developed by and for academic medical centers and few are widely installed beyond the development site.

It has been two years since the IOM report was written, and a plan to develop an operational model of a fully automated CPR has not been proposed. Some experts believe that one of the reasons for this is that system developers often design systems without an adequate understanding of the process of information flow that is being computerized.' Without such a framework, system designs are often complicated and sometimes impractical. For example, a system may require a practitioner to move through many screens of administrative information before getting to the clinical data that is of interest. Also, technology and its applications have not yet been refined to the point where practitioners will choose to enter information into a computerized information system over a paper record. For example, voice-activated data input has not yet been perfected; free text -- which captures the nuances of clinical observations in ways that l-ill-in-the-blank screens and other forms of structured text cannot -- is not readily translatable into data that can be analyzed by a computer; and, when working with very large data sets, speed can still be a problem. Moreover, the amount of clinical data that can be stored in a computer is so vast that without tools for easily analyzing the data, practitioners may be concerned about their ability to assimilate all of the relevant information about a patient.

So, despite the rapid and impressive evolution in technology, much development is still necessary.

Although we anticipate that over time the benefits of CPRs are likely to substantially exceed the costs, the initial investment will be large, while the benefits will be long-term and will be distributed among many different users (e.g., providers, payers, researchers, etc.). Providers may be unwilling or unable to invest large sums of money in CPR systems without assurances that it will pay off. According to a recent survey by Coopers & Lybrand and Zinn Enterprises, hospitals' biggest deterrent to buying clinical information systems is the difficulty in justifying their costs.[8] Cost-effectiveness is obviously hard to prove without an operational example of a fully automated CPR, but we do not even have reliable figures to evaluate the overall cost-effectiveness of those contemporary systems that come closest to our vision of a CPR.

There are many barriers to collecting cost-benefit information. The best source for system evaluations is the user; however, there are disincentives for providers to conduct formal cost-benefit analyses of the systems they install. Many providers do not employ people with the analytic skills to design and conduct controlled cost-benefit studies. Some are reluctant to spend time and money evaluating a system they have already purchased. Moreover, no one wants to fmd that they have made a multimillion dollar mistake.[9]

We do have some evidence that partially automated systems can be cost-effective. Not surprisingly, the little existing scientific evidence about the cost-effectiveness of clinical information systems has come almost exclusively from academic medical centers that have such systems. Recently published results of a randomized controlled clinical trial conducted by Tierney and others at the Regenstreif Institute of Indiana University show significant cost savings associated with physician use of microcomputer workstations for writing all inpatient orders. For the physician teams that used the workstations, average total charges were $887 per patient, or 12.7 percent, lower and average length of stay was 0.9 day shorter." Another study by the same authors found that using microcomputer workstations to present physicians with previous test results reduced the number of tests ordered by 8.5 percent and reduced the dollar cost of testing by 13 percent per visit." Another study by these authors found that when physicians at an academic primary care medical practice were informed of the charges for outpatient diagnostic tests (by ordering tests through a microcomputer workstation), the number of tests decreased by 14 percent and charges decreased by 13 percent or $6.68 per visit.[12] Gardner and others of the University of Utah conducted a quantitative and qualitative assessment to determine the value of the pharmacy module of the HELP automated medical record system at LDS Hospital. They found that the system has yielded a $3.94:1 benefit/cost ratio from avoiding complications due to drug interactions.[13]

All of these examples show that clinical information systems can improve the quality and efficiency of patient care. They do not, however, provide information about the net impact of these systems -- how much it costs in hardware, software, and personnel time (including training and maintenance) to achieve these savings.

In addition to evaluations of specific systems, there have been a few attempts to estimate more broadly the costs and benefits of computerizing patient information.

- To support its 1992 proposal for a "nationwide electronic health care information network," HHS developed estimates of the costs and benefits of the electronic network to the overall health care system. HHS estimates that if fully implemented by the year 2000, savings over the next eight years would exceed $100 billion and that more than half of the expected savings would come from "clinical savings" (e.g., reducing the number of diagnostic tests, increasing personnel efficiency, decreasing length of stay).[14]

- A 1992 study commissioned by several telecommunications firms estimates that telecommunications applications (such as computer-based patient records, systems that allow health care providers to communicate with patients at home, video conferencing to facilitate consultation between remote providers and medical experts) would save $36 billion annually. The study estimates that savings would come from more efficient

management of patient information, faster and more efficient claims processing, and improved management of hospital inventories. However, the report does not provide an estimate of what it would cost to achieve these savings."

Although these types of studies cannot tell us how much a CPR will cost or how much it will save, they do represent some of the best evidence we have that CPRs can be cost-effective. The Agency for Health Care Policy and Research (AHCPR) recognizes the need for more information, and is currently funding a project at El Camino Hospital in Mountain View, California, to develop and apply a cost/benefit methodology that providers can use to evaluate patient information systems. The project is designed to describe the present state of development and use of computerized hospital information systems, identify needs for further development, and evaluate the operational features and costs of commercially available systems.[16]

The benefits of CPR systems will accrue to payers, patients, regulators, researchers, employers, as well as providers. The costs associated with these systems cannot and should not be assumed by providers alone. Lacking, however, is any attempt to systematically evaluate how the costs and benefits of CPRs and the health information infrastructure could be shared equitably among all who will benefit (e.g., providers, payers, patients, regulators, evaluators, researchers, employers).

Implementation of computerized patient record systems introduces organizational, professional, and personal change that must be managed. When a system is introduced that changes the flow of information and makes work more efficient, work patterns within the institution change -- and so do various professional departmental roles. Failure to consider resistance to change is likely to result in a system that is rejected by the users for whom it was developed.[17] A study by the Congressional Office of Technology Assessment found that computer-based information systems, once implemented, often result in "unforseen costs, unfulfilled promises, and disillusionment."[18] Other studies have found that nearly half of all clinical information systems fail, due to user resistance and other factors." Still another survey, of 620 hospitals, indicated that hospitals use less than one-fourth of the capabilities built into their computer systems.[20] And after spending $200 million on a computer system for its clinical center four years ago, the National Institutes of Health (the government's top medical research center) is trying to sell the system because it is not being used.[21]

AHCPR is currently funding a project designed to assess the feasibility of identifying and evaluating barriers, including sociological and organizational factors, to systems implementation in hospital and ambulatory care settings. If such a study is determined to be feasible, AHCPR intends to contract for a multi-year evaluation of barriers to integration and implementation of clinical information management systems in representative provider sites."

Standard data formats, definitions, structures, and codes are needed in order to connect the "islands of data" that currently exist, and to allow for fully integrated systems in the future. In many hospitals, clinics, and other provider settings a significant amount of important

patient information is already stored in computers. However, because there is no one vendor that offers superior systems for all applications, most organizations have a variety of departmental systems with little or no integration. This has created a whole new set of challenges -- how to get systems designed by different vendors to "talk to each other." Patient demographic information is generally entered into a computer during the admitting process. Many laboratories and pharmacies are computerized. Surgical reports, hospital discharge reports, and consultant notes may be dictated and then transcribed using word processors. Yet, because different systems store and identify information in different ways, integrating information from different sources, even within the same institution, is expensive (custom interfaces between systems can range from $50,000 to $150,000 each in today's nonstandard world), if not impossible. [23,24] The implications are far broader when one considers the vision of a health information infrastructure that links health data across sites of care.

Even advanced systems designed without regard for national health care information standards may work against the kind of information networking we envision for the future. Without standards for defining, coding, and formatting data, the "islands of data" can never be bridged and many of the benefits of computerization can never be realized.

Generally, we distinguish between three types of health care information standards:

- Message ***standards*** define the fields, format and structure of a message sent from one computer to another, from a hospital to an insurer, or an instrument such as an EKG to a terminal displaying the reading. Message standards specify such things as whether dates are represented as MM/DD/YY or YYYYMMDD and whether fields are fixed or variable in length. [25] Message standards development is generally undertaken and underwritten by vendors and software developers, and many standard-setting groups currently are hard at work developing health care message standards that would obviate the need for specialized interfaces.

- ***Coding standards*** represent terms and concepts in a uniform way. For example, the ICD9-CM code for appendectomy is 47.0. In many domains coding standards are well developed (e.g., drugs, procedures, diagnoses), but they are frequently overlapping. For example, there are two detailed coding systems for drugs -- the World Health Organization drug codes and the National Drug Code. In other domains, such as procedures, there are multiple coding schemes (e.g., ICD9-CM and CPT-4), but neither are sufficient in terms of detail or coverage. And in other domains (e.g., clinical findings) codes may be either absent or insufficient.[26]

- ***Content standards*** identify, and in some cases define, the broad ***categories*** of information (e.g., diagnostic test reports, current health problems) to be contained in the patient record. The American Society for Testing and Materials (ASTM) has begun the development of a standard for the ***content and structure of an automated patienr record*** that specifies the categories of information to be contained in the record. ASTM is also in the process of developing a standard for the ***content and structure of an automated longitudinal health record*** that would summarize information from the primary record

and would serve as a unified, coordinated synopsis of clinically significant health information aggregated over a person's lifetime.[27]

Content standards are often confused with *data dictionaries.* A data dictionary defines the *fields* of information in the patient record. For example, within the category diagnostic tests, the fields could include, name of lab test, results of lab test, date, provider identifier, and patient identifier. Fields such as name of lab test would link to tables of *codes* that list all of the valid values for that field (e.g., glucose, potassium, complete blood count). Although we strongly believe in the need for standardizing codes, the internal structure of systems, including their data dictionaries, need not be standardized.

Until very recently, standards development has been uncoordinated, which has led to costly duplication of effort in some areas and gaps in others. Standards development is generally a voluntary, consensus-driven process. Many of the standards developed in this country are done so by groups designated by the American National Standards Institute (ANSI) as "accredited standards committees." In order to be accredited by ANSI, these committees must follow a formal balloting and voting process for reaching consensus among their members; Although the process for reaching consensus *within* a group is well established, until very recently, there has been a lack of coordination *between* groups involved in setting health information standards. As a result, there are multiple "standards" for some functions and none for others. For example, ICD-9-CM (International Classification of Diseases, 9th Revision, Clinical Modification) and CPT-4 (Current Procedural Terminology) classify many of the same surgical procedures, but the codes, applications, purposes and often the terminology, used by the two classification schemes are different. The activities of healthcare standard setting organizations are constantly evolving, so we have not attempted to describe their individual efforts. However, the Agency for Health Care Policy and Research, Office of Science and Data Development maintains an updated report summarizing the activities of selected healthcare informatics standards organizations.

In March 1992, ANSI organized and chartered the Healthcare Informatics Standards Planning Panel (HISPP) to coordinate the work of various standards groups towards achieving a unified set of nonredundant, nonconflicting standards. MSPP will also coordinate standard-setting activities in the United States with those of the European community. HISPP itself will not develop standards. Rather it will establish work groups to examine areas of overlap and gaps and obtain voluntary consensus about which groups will work on standards for which areas. The panel receives limited funding from AHCPR to support mailing, meeting space, and other operational costs, but participation is entirely voluntary and participating organizations are responsible for their own expenses.

The major standards groups appear to have accepted HISPP in the role of coordination and oversight. However, the panel is still relatively new, its resources are limited, and it is too early to tell how successful it will be in taking a voluntary approach to coordinating what has until

now been a completely fragmented activity. A more detailed description of HISPP is included in appendix C.

Linkages between systems will significantly enhance access to patient information, thereby offering tremendous potential for improving the quality and efficiency of health care delivery. But, with enhanced access come concerns about confidentiality and the protection of patient privacy. Patient information is already shared among those who deliver and pay for care, but the health information infrastructure we envision, which will make patient information more accessible to caregivers, payers, and others, will create many new opportunities for abuse, unless protection for patient privacy is built into its design and use.

Potential for large-scale breaches of confidentiality is magnified by the ease of sharing electronic documents. According to Adele Waller, an attorney and nationally recognized expert on this subject, "currently feasible computer security measures are particularly inadequate for networked systems and probably cannot protect providers that install computer-based patient record system from substantial exposure to liability. "[28] Furthermore, as capability for storage and analysis of personal records increase and the cost of collection decreases, the demand for such information by providers, payers, policymakers, and researchers will likely multiply. There may be pressure to collect more data than is strictly necessary for a given purpose -- collected data may then be maintained in a large data base, where it may be vulnerable to misuse.

Current laws written to protect, privacy vary significantly from state to state, are often conflicting, and frequently do not consider the implications of electronic records.[29] The inconsistencies among states already create problems with compliance in some circumstances (e.g., the centralization of record-keeping operations by health care organizations operating in more than one state). Increasing use of electronic patient records is expected to aggravate these difficulties. Records will be routinely transmitted across state lines, and may even be *created* simultaneously in two states, as when a physician working across the Wisconsin border dials into the computer system of a hospital located in Illinois.

In addition, many state laws do not address certain key issues, such as:

- A patient's right to see, copy, and correct his or her own records.
- The need for special protections for information about certain conditions for which there is heightened risk of discrimination (e.g., HIV infection, genetic abnormalities, mental illness, and substance abuse).
- The obligations of providers other than hospitals and physicians to protect confidentiality.

As a result of the patchwork laws governing confidentiality of patient records, providers may hesitate to share information outside their organization in an electronic (or paper) environment due to risk of liability for unintentional breaches of confidentiality. And, even more troubling, patients may hesitate to fully inform clinicians due to potential discrimination resulting from

inappropriate access to their health information by employers, creditors, or others. See appendix D for a more complete treatment of this topic.

In many states, laws and regulations governing licensure of providers impede the use of CPRs. More and more state hospital licensing laws are being changed to specifically permit the use of computerized patient health records as the legal record of care. However, there are still some states that effectively prohibit the use of CPRs by requiring that orders and/or practitioner signatures be written in ink or by restricting the permissible health record storage media to the original or microfilm.[30]

Licensure laws for other providers (e.g., nursing homes, health maintenance organizations) also present barriers to CPRs. For example, Illinois long-term care facilities are required to write or type resident records. Also, all orders, treatment plans, and other documents must have the original written signature of the practitioner.[31]

Not only do these types of laws pose barriers to the implementation of CPRs in certain states, but the variation between state laws presents obstacles to the development of CPRs by making it difficult, if not impossible, to develop patient record systems that comply with requirements in all states.

There is **an immediate need for patient-level clinical data to support the evaluation of health care cost and quality.** Purchasers, insurers, regulators and researchers collect patient-level data to support evaluations of the quality and efficiency of providers and the effectiveness of treatments, technologies, and the delivery system as a whole.

- ***Accrediting/certifying/licensing agencies*** collect data to evaluate whether providers meet their standards of performance. For example, the Joint Commission on Accreditation of Healthcare Organizations has developed an Indicator Monitoring System to collect detailed clinical information to support comparisons of outcomes among health care organizations.

- ***Federal/state/regional/local regulatory agencies*** collect data to evaluate issues of quality, cost, and access. For example, over 20 states have data commissions that collect varying types of patient-level information from hospitals and other health care providers.

- ***Private and public purchasers/payers*** collect data for purposes of claims processing, utilization review, predicting future costs, etc.

- ***Researchers*** collect data to support evaluation and analysis of a whole range of issues -- from effectiveness of a certain drug to delivery system reform.[32]

Currently, the only extensive data base of patient-level information about health care services exists through claims captured to administer health insurance. These administrative data sets

contain basic demographic as well as some clinical and diagnostic information and are widely used for purposes other than the adjudication of claims. However, meaningful analysis of health care costs and quality frequently requires more clinical detail than is currently captured in these administrative data bases. Furthermore, the validity of using data collected for reimbursement to evaluate quality, efficiency or effectiveness is questionable. Problems and errors with the clinical data contained in these administrative data bases are well documented.

Generally, once all clinical information is computer-based, the transmission of detailed clinical information for use by regulators, evaluators, purchasers, and researchers will be relatively simple. Indeed, many are interested in the development of the computer-based patient record primarily to support these sorts of evaluation activities. However, we believe it is crucial that those who provide care determine what information should be contained in the patient record. Information needed to provide care should satisfy most evaluation needs of external organizations, but there is some information, such as patient satisfaction and functional status, that is not currently contained in the medical record but is important for evaluating the process and outcomes of care.

As we have already said, it will probably be 15 or more years before all providers have fully operational CPRs, and those with a legitimate need for the information cannot be expected to wait that long. Until we have widespread implementation and use of CPRs, the only way to build data bases of detailed clinical information is to collect information from existing paper records and enter it into a usable electronic format. However, this is very labor intensive and requires skilled personnel trained in medical records, nursing or other clinical professions. Perhaps the most significant example of such a system is the Uniform Clinical Data Set (UCDS), which was developed by the Health Care Financing Administration to collect information needed by the Medicare Peer Review Organizations (PRO) to evaluate the quality and appropriateness of care provided to Medicare beneficiaries. On average, data abstraction to support UCDS includes 250 data elements and takes 60 minutes per record. Taking into account labor costs alone, the annual cost of collecting such a data set for all inpatient admissions in the U.S. would be in excess of $500 million dollars. To put this in perspective, Medicare currently spends $250 million to fund the PRO program in all fifty states.

Although providers recognize the importance of evaluating the cost and quality of care, the nature and extent of data demands present many problems.

- Collecting the data can be very time-consuming and costly and may divert resources from patient care activities. External organizations frequently do not evaluate their data demands to determine whether all of the information they are requesting is necessary, reliable or valid for their intended purpose.

- There is often significant overlap in data requests from different organizations, but there has been virtually no effort on the part of these organizations to coordinate requests or identify core sets of data elements that could serve multiple purposes.

- External organizations develop their own data definition, data collection and data coding conventions. These conventions may be completely different from those used by the

providers from whom they are collecting the information. This leads to misinterpretation of the data and potentially to erroneous decision making. It also presents significant barriers to merging existing data bases to support large scale projects.

- In order to cope with the data demands, providers may install computer systems designed to facilitate data collection for reporting purposes. This may divert resources from systems designed to support better patient care management within the institution.

Experimentation with community health information networks is just beginning. Our vision for CPRs depends upon the establishment of communication linkages between various users of patient information. Communication networks are critical to the long-term vision of CPRs, and they may also offer opportunities for improving the quality and efficiency of clinical information transfer in the near term. Although as yet there are no operational examples of community health information networks, a few communities are planning networks that will link health care providers so that patient health information can be shared across time and place. Examples include:

- A group of providers (2 hospitals, 2 hospital-based clinics, and 16 remote clinics) are using a computerized patient record system, the Regenstreif Medical Record System, to link perinatal records generated at all sites. The system is designed to capture important clinical information about the patient into a single record that is linked to the patient's prior record and is available by computer for any future caregiver. This project has received broad community funding support. Some of the funding for this project came from the Indianapolis Campaign for Healthy Babies, a private/public consortium formed in response to the high infant mortality rate in Indianapolis/Marion County. Additional funding was provided by a Maternal and Child Health Grant from the Indiana State Board of Health.[33]

- Ameritech Corporation, in partnership with Aurora Healthcare, a two-hospital system in Milwaukee, is currently developing the Wisconsin Health Information Network (WHIN), a for-profit service designed to give providers, payers, employers and other health information users a single public network for clinical and financial transactions. WHIN proposes to handle a variety of insurance transactions, but of greater interest to this work group are the provider linkages it is designed to provide, including allowing practitioners to review clinical reports such as lab results, pharmacy profiles, and radiology reports in their offices.[34]

- The Ambulatory Care Council (ACC), a group of ambulatory care providers that serve low-income communities in the Chicago area, is developing a plan to link their patient information systems. The ACC has secured a three-year grant from the Chicago Community Trust to begin development of an integrated information system that would permit patient information to be shared among the participants, including hospitals, community health centers, Chicago Department of Health, Illinois Department of Public Health, Illinois Department of Public Aid, and others.[35]

- The Hartford Foundation is funding Community Health Management Information System (CHMIS) planning projects in Washington State, Iowa, and most recently, Vermont. These projects differ considerably in scope and intent, and none are engaged in developing CPR systems. However, all are statewide efforts involving providers, purchasers, consumers, and government with the goal of developing integrated information systems to facilitate claims processing and to provide health care purchasers and consumers in a defmed geographic area with "buy right" information. As yet, none of the projects is operational or funded for **implementation.**[36]

STRATEGIES

We believe that with a well-planned, adequately financed, and incremental approach, the challenges presented by the current environment can be overcome. The most formidable obstacles to the development of the health information infrastructure are:

- the development and adoption of uniform standards for defining, coding and transmitting health data;
- the adoption of standards for protecting patient privacy;
- the significant investment (initial and ongoing) in hardware, software and training; and
- the organizational/behavioral barriers to using CPR systems.

We have built our strategies in response to these obstacles. The strategies that we propose require a cooperative effort on the part of the public and private sector. Since the activities of the Work Group on Computerization of Patient Records end with the publication of this report, we must look to other groups to carry out the strategies we propose. The Computer-based Patient Record Institute (CPRI), with its broad representation, is poised to coordinate many of the research and education strategies. Similarly, the Healthcare Informatics Standards Planning Panel (HISPP) is best suited to coordinate and provide national direction to voluntary standards development because it is broadly representative of national standard setting organizations and is recognized by the American National Standards Institute. However, both the CPRI and HISPP are new organizations and they will need financial support to coordinate an effort of this magnitude.

The strategies we propose are focused on the next three to four years. For each recommendation we have also suggested "next steps" that should be taken.

I. IMPROVE KNOWLEDGE ABOUT THE STATE-OF-THE-ART

Better information is needed about what kind of systems providers have, how much systems cost, how much they save, how they could be used more effectively, and how they could be improved. We recommend that the following series of projects be conducted to answer these questions.

I.A. Conduct provider surveys to improve knowledge about the current level of provider computerization so that providers, payers, policymakers, and vendors will better understand where we are today, where we want to be in the future, and what we need to do to get there.

We recommend that the CPRI be funded to conduct provider surveys to develop a better understanding of the general level of computerization in different health care settings (e.g, hospitals, health maintenance organizations (HMOs), practitioner offices, nursing homes, etc.), and to identify outstanding systems that can serve as models for others implementing or

evaluating systems. These surveys will help plan for the time frame and resources required to achieve our vision by documenting the state-of-the-art of health care computerization. It will also help determine how satisfied providers are with the systems that they already have, and identify barriers to implementing and using information systems.

The work group has developed a draft survey to be used as a starting point in carrying out this recommendation (see appendix E). We propose surveying hospitals, practitioner offices, group practices, HMOs, home health providers, nursing homes, and ambulatory care facilities.

Time frame: Begin 1993, completion within 12 months.

Estimated Cost: $500,000

Next Steps

- Develop and disseminate case studies of outstanding systems.
- Evaluate how current systems could be linked through community health information networks (e.g., linking hospital lab systems to practitioner offices).
- Use results as a baseline against which to measure periodic reassessments of progress toward computer-based patient record systems.

I.B. Develop a reference model for evaluating the costs and benefits of clinical information systems within organizations.

We recommend that the Department of Health and Human Services (HHS) be funded to develop a cost-benefit evaluation methodology, such as the methodology currently being developed by AHCPR at El Camino Hospital, which can be applied to clinical information systems in a variety of settings (e.g., HMOs, ambulatory care, practitioner offices) that are close in function and feature to CPR systems (e.g., decision support, direct entry by caregivers, linkages with other health care organizations or providers). Systems to be included in the study could be identified using results from the provider surveys described above.

The projects should be designed to accomplish the following:

- Identify and evaluate impacts of different information systems. For example:

  Does the system increase staff productivity?
  Does faster information retrieval improve the quality of care or the efficiency of patient management?
  What are the strengths and weaknesses of alternative forms of data entry technology (e.g., keyboard entry, pen-based entry)?
  How does the system impact organizational dynamics (e.g., roles and responsibilities, job satisfaction)?

What are the initial and ongoing system costs (hardware, software, personnel)?

- Test whether, and to what extent, expected benefits are actually realized.
- Estimate quantifiable benefits accruing to each user group (e.g., provider, payer, employer). For example, shorter hospitalizations resulting from more streamlined order processing will benefit patients, hospitals, payers, and employers. Availability of information to support performance monitoring will benefit patients, payers and employers.

These projects should be coordinated with studies of the costs and benefits of community health information networks (described below). Also, the projects should be coordinated with similar efforts being conducted by CPRI, Department of Defense, Department of Veterans Affairs and other organizations.

Time frame: Begin 1993, completion within three years.

Estimated Cost: $3 million

Next Steps:

- Develop standard methods that providers could use to evaluate the systems that they plan to implement, are currently implementing, or have already implemented so that they can make better use of the systems they have and make better decisions about systems they are contemplating.
- Encourage providers to use these methods to continuously evaluate their information systems.
- Construct data bases of comparative information that providers could use to support information system purchasing decisions and negotiate risk-sharing contracts with vendors (e.g., build savings guarantees into leasing arrangements).
- Develop a mechanism to share the costs of developing, implementing, and maintaining CPRs among those who will benefit.

I.C. Analyze information needs and uses within various health care settings to support the design, implementation, and use of CPR systems.

We recommend that CPRI coordinate projects to analyze work processes in a variety of provider settings (e.g., hospitals, nursing home, HMOs). These projects should be designed to answer questions such as:

- What information do practitioners and others (e.g., payers, researchers, government agencies) need?
- Where is the information found?
- How is the information used?

The work group believes that documentation of the commonalities and differences in information needs and uses among institutions and providers would serve as a resource for future system development by helping system designers to identify those aspects of information systems that can be standardized and those that must remain flexible.

Time frame: Begin 1993, completion within three years.

Estimated Cost: $15 million ($5 million per year)

Next Steps:

We expect results of these analyses to be used by:

- System developers to design systems that are better able to meet users' needs.
- Providers with existing information systems to better realize the capabilities of their systems.
- Providers contemplating purchasing systems to determine their needs and evaluate how well available systems could meet these needs.
- CPRI and others to:

  Identify information that is routinely shared among providers (e.g., discharge abstract, lab report) for which standards should be developed.

  Identify the interrelationships between information needs and uses in different types of provider settings. This will support construction of the overall architecture of the health information infrastructure.

I.D. Evaluate issues related to organizational, professional, and personal change that may pose barriers to the implementation of CPR systems.

We recommend that CPRI be funded to evaluate barriers to systems implementation, such as the study currently being conducted by AHCPR. This evaluation should be conducted in a variety of health care settings. In addition to identifying barriers to implementation, the projects should be designed to:

- Determine how best to train health care providers in the use of CPRs -- including development of health professional school (e.g., medical schools, nursing schools) classes that use CPR technology.

- Identify how best to involve practitioners in decisions regarding the purchase and implementation of CPRs.

- Develop model programs that providers can use to help them manage the implementation of CPRs.

Time frame: Begin 1993, completion within three years.

Estimated Cost: $3 million

Next Steps:

- Providers should apply the implementation strategies developed as a result of these evaluations.

- Health professional schools should instruct students in the use of computers as a data management and analysis tool.

II. DEVELOP NATIONAL STANDARDS

National standards for defining, coding and transmitting data are needed to support the sharing of information among those who collect and use it. Also needed are national standards for protecting the confidentiality of information stored in CPRs.

II.A. Promote the development, adoption, and use of national health information standards.

- We recommend that HISPP:

  Continue the overall standards planning and coordinating process. Additional funding will be needed to support their administrative costs (e.g., mailing, meeting space).

  Continue to publish and widely distribute a directory of groups involved in developing health care information standards so that those interested in participating will know whom to contact.

  Coordinate the development of a patient data set that **could be** ***lifesaving if it were available in an emergency situation (e.g.,*** current problems, allergies, major surgeries, primary caregiver, source of more information about the patient's

health history). The ASTM longitudinal record, as well as findings from the analysis of information needs and uses described above, should be used to help identify the types of information that would be included in such a record. Also needed are evaluations of mechanisms for storing and controlling access to this information (see section III.A).

Coordinate activities to develop standards for the content of the patient record. Standards should build on existing work of the ASTM standards for the content and structure of the primary record of care (see page 10). Comparison of data dictionaries in current systems (e.g., Department of Defense Composite Healthcare System, Department of Veterans Affairs Decentralized Hospital Computer System) to identify data fields that are common to existing data dictionaries should also be used as a basis for content standards.

Work with the CPRI Codes and Structures Work Group to coordinate activities to compare and contrast currently existing coding standards, identify where additional coding schemes are needed, coordinate the development of needed coding schemes, and promote the adoption and use of existing coding schemes by system vendors and users. We strongly believe that coding schemes adopted for national use should be in the public domain.

Work with WED1 and the CPRI Codes and Structures Work Group to coordinate the development of uniform provider and patient identifiers.

- We recommend that CPRI foster development of a mechanism for certifying whether systems use national standards.

Recommendations	Time Frame	Estimated Costs
Fund HISPP standards planning and coordination	Ongoing	$100,000/year
Develop, test and promote use of a patient data set for emergency purposes	Begin 1992, completion within two years	$500,000
Develop standards for patient record content	Begin 1993, completion within three years	$100,000
Compare and contrast coding schemes and develop needed coding schemes	Begin 1993, completion within three years	$500,000
Develop uniform provider, payer and patient identifiers	Begin 1993, completion within 12 months	$50,000
Foster development of standards certification process	Begin 1993, completion within 12 months	$50,000

Next Steps:

- HISPP should:

  Coordinate the maintenance and updating of the emergency patient information summary.

  Coordinate the maintenance and updating of the patient record content standard.

  Coordinate the development of coding schemes in areas where current schemes are insufficient.

- CPRI and other professional organizations should actively promote the adoption of national standards by:

  Providing public education about the existence and importance of standards.

  Encouraging providers that are planning to purchase systems to demand contractual guarantees that systems use national standards.

  Endorsing and participating in HISPP.

Encouraging practitioners to play a more central role in developing standards for patient record content and coding.

II.B. Establish national legal standards for protecting the confidentiality of patient information.

The Work Group believes strongly that both legislative and operational mechanisms to protect the confidentiality of patient information must be in place before the health information infrastructure can be implemented. We recommend that:

- Congress and the President enact federal preemptive legislation to resolve inconsistencies and inadequacies in existing laws that protect patient privacy. This legislation should apply to **all** health information and should include provisions that would:

  Establish a Federal Information Privacy Commission as part of the national information infrastructure that would establish uniform requirements for protecting the confidentiality of health information, and potentially other types of information (e.g., credit, personal finances). Members of the Privacy Commission would be appointed by the President, and would represent patients, providers, payers, researchers, other federal agencies, and other interested parties. The Privacy Commission would have regulatory power and would be responsible for implementing and enforcing provisions of the federal legislation.

  Set minimum security standards for CPR systems (e.g., audit trails, passwords). These standards should be reviewed and updated on an ongoing basis.

  Define patients' rights to control access to their own individually-identifiable health information.

  Establish standards for agreements in which patients authorize the redisclosure of their health information. Such authorization agreements should (1) specify the purpose for which the information is being disclosed, (2) prohibit redisclosure for any other purpose, and (3) limit the period of time for which authorization for disclosure is granted.

  Defme patients' rights to examine, copy and correct any patient identifiable information.

  Specify fair information practices that create a balance between what information an individual is expected to divulge to a record-keeping organization and what he or she seeks in return; minimize the extent to which the information is a source of unfairness in any decision made on the basis of such information; and create and define obligations respecting the uses and disclosures of such information.

  Require publication of the existence of health care data banks.

Establish strict penalties for inappropriate use of confidential information (e.g., discrimination, employment decisions). Penalties for inappropriate **access** to confidential' information (e.g., reading a patient's record) should also be established, but should be somewhat less severe than those for inappropriate **use.**

Establish appropriate protections for highly sensitive data (e.g., mental health, substance abuse, communicable and genetic diseases).

Not mandate changes in state public health reporting laws.

Establish that compliance with requirements of the legislation would be a defense against actions for improper disclosure.

CPRI and WED1 are in the process of developing model legislation and should be consulted.

- All individuals and organizations that collect and/or have access to individually identifiable health data (e.g., providers, payers, researchers) should restrict access of their employees or agents according to their "need to know ."
- Societies of health professionals should educate their membership about their responsibilities in adhering to ethical codes that require them to protect the confidentiality of patient information.
- Providers should include provisions on confidentiality and redisclosure in contracts with all third parties, including payers and other providers.
- Further study of several issues should be coordinated by the CPRI:

  Development of better security mechanisms to prevent unauthorized access.

  Ways of limiting data matches between health data and other types of individually-identifiable information (e.g., bank records).

  Ownership of electronic health information.

  Possible limitation of court subpoena power over patient health records.

  Feasibility of a nationwide, uniform system for encrypting (scrambling) individual identifiers such as social security numbers. Such a system would allow patients' encounters to be linked over time while protecting the patient's identity.

  Issues related to developing national standards for the creation, authentication, retention, and storage of patient health records.

Time Frame: Begin 1993, completion within 12 to 18 months.

Next Steps:

- Establish national legal standards specifying ownership of electronic health information.
- Adopt a national system of individual identifiers for patients, providers, and patients.
- Establish national legal standards for documenting and storing health information that are consistent with computerization.

A more detailed discussion of issues and recommendations related to patient confidentiality is included in appendix D.

II.C. Evaluate the usefulness and cost-effectiveness of all data requests -- the value of data must be measured against the cost of collecting data

We recommend that:

- Regulators, insurers, and others take responsibility for demonstrating the reliability, validity, usefulness and cost-effectiveness of data sets before requiring that they be collected and reported. Evaluations should be designed to determine whether:

  Measures are reliable and valid for the intended purpose.

  Benefits of having the data set outweigh the costs of collection.

  Each data element is needed, or if the data set could be reduced.

  It is necessary to collect data for 100 percent of cases, or if a representative sample would be sufficient.

  National standards for nomenclature, definitions, and codes are used.

- Congress should direct funding to the Department of Health and Human Services (HHS) for evaluations of existing data sets to identify any overlaps; and recommend how data collection could be coordinated to reduce the administrative burden on providers.

- Congress and the President should enact legislation (similar to the Paperwork Reduction Act**) requiring federal agencies to demonstrate the usefulness and cost-effectiveness of data sets before they can be mandated.

Time Frame: HI-IS evaluation - ongoing.

Legislation - begin drafting 1993, enactment within 18 months.

Estimated Costs: HHS evaluation - $1.5 million/year

Next Steps:

- Data requirements should be continuously evaluated to determine if:

  They are serving the purpose for which they were developed.

  The data are available from existing electronic data bases.

  The data are reliable.

  Data definitions and codes are consistent with national standards.

III. DEVELOP LINKAGES BETWEEN EXISTING AND FUTURE COMPUTER-BASED INFORMATION SYSTEMS

Interconnected communication networks that operate locally, regionally, and nationally are needed to support the health information infrastructure we envision.

III.A. Encourage the development of community information networks to test a variety of models for establishing communication links between users of patient information in a community.

We recommend that:

- Federal funding be provided for demonstrations of community information networks. We urge the Department of Health and Human Services (HHS) to make available the $10 million earmarked in the 1993 Labor/HHS Appropriations Bill to fund planning grants for electronic, community health information networks through which clinical and insurance information could be transmitted. We also encourage the Administration to specify that $15 million of the $64 million proposed for information highway demonstrations be used to fund community health information network demonstrations.

** The Paperwork Reduction Act of 1980 requires federal agencies to estimate the annual record keeping and reporting burden of certain proposed regulations and to report this information to the Office of Management and Budget for review.

The Secretary of Health and Human Services, in consultation with CPRI and other health care representatives, should establish criteria for awarding grants and evaluating project results. In order to qualify for federal funding, community health information network projects should be required to:

Subject themselves to a standardized external evaluation so that costs and benefits (both quantitative and qualitative) can be compared between networks. Results of these evaluations would be made publicly available.

Demonstrate that they are taking adequate measures to establish system security and protect individual patient confidentiality.

Incorporate existing national health information standards.

These projects should be coordinated with evaluations of clinical information system costs and benefits and should be designed to answer questions such as:

What are the costs and benefits of community health information networks?

How can network costs be shared equitably among all participants (e.g., subscription fees, user fees)?

What are the strengths and weaknesses of various models for storing, sharing, and controlling access to patient health records, including a patient information data set that could be lifesaving if it were available in an emergency situation (see section II.A.). Models that should be evaluated include (but are not limited to):

- Regional or local data bases containing the entire patient record
- Regional or local data bases containing summary information about the patient
- Decentralized storage within provider systems with an indexing system that would indicate where patient information is located
- Smart-cards

How do community health information networks fit into the national information infrastructure?

- Networks should adopt and use national transmission, coding and content standards, where available. Networks should be designed with the **flexibility to adapt to new** standards as they are developed.

Time Frame: Begin 1993, completion within three years.

Estimated Costs: $25 million

Next Steps:

- CPRI, other professional organizations, and the government should monitor the progress of pilot projects and educate the public about community health information networks.
- Broader demonstrations of successful network models should be conducted.

III.B. Members of the health care community should collaborate with other industries and government to create the health care component of the national information infrastructure.

- An interindustry consortium should be established, with health care representation (coordinated by CPRI), to promote:
  - Development of computer applications in health care and other industries that are compatible with the national information infrastructure.
  - Development of software systems that utilize and incorporate state-of-the-art technology from health care and other applications (e.g., banking, manufacturing).
  - Development of security mechanisms to guard against inappropriate access to and use of information.
- Health care applications should be emphasized as an important component of the High Performance Computing and Communications Program.
- The health care sector (HHS and other health related agencies) should be represented on the National Economic Council's Task Force on Information Infrastructure.
- A portion of the $64 million proposed for information highway demonstrations should be earmarked for community health information networks (described above).

We would also like to express our strong support for the inclusion of health care applications within the Information Infrastructure Technology Program.

Time Frame: Begin 1993 - ongoing.

Estimated Costs: See previous recommendation.

Funding for all of the recommendations presented above should be sought from a combination of public and private sources. Due to the nature of the studies and demonstration projects we have recommended, likely sources of public funding would include the Agency for Health Care Policy and Research. Private funding should be sought from foundations and information system vendors.

CONCLUSION

It is our belief, and certainly our hope, that many share our long-term goal of a national health information infrastructure. that will link all participants in the U.S. health care system. Less agreement exists, however, about what we need to do now and in the near future to achieve this goal as efficiently and quickly as possible.

The strategies we have proposed represent first steps in an evolving process. We hope that the organizations we have called upon to coordinate and carry out our recommendations will accept the challenge. We also hope that our recommendations will help guide the decisions of ***policymakers*** as they set priorities for our present and future health care delivery system; ***providers*** as they make choices about implementing and using information systems; ***purchasers, evaluators and regulators*** as they develop the systems they need for evaluating health care services; and ***vendors*** as they design the CPR systems of the future.

Although we must depend on other groups to carry out the strategies we have proposed, we, the organizations that together make up the Work Group on Computerization of Patient Records, are each committed to working with our own constituents and with each other to lay the groundwork needed to advance our vision.

The conclusions and recommendations presented in this report do not necessarily represent official policy of the participating organizations.

REFERENCES

1. Dick, R. S., and Steen, E. B., editors. The *Comvuter-Based Patient Record: An Essential Technoloav for Health Care.* Washington, DC: National Academy Press, 1991, p. 11.

2. Dick, R. S., and Steen, E. B., editors. The *Comvuter-Based Patient Record: An Essential Technology for Health Care,* Washington, DC: National Academy Press, 1991.

3. Computer-Based Patient Record Institute. 1992 Mar. *23.*

4. U.S. Department of Health and Human Services. Initiatives Toward the Electronic Health Care System of the Future. White paper, Washington, DC, 1992.

5. Computer Systems Policy Project. *Perspectives on the National Information Infrastructure: CSPP's vision and Recommendations-for Action.* Washington, DC, 1993 Jan. 12.

6. Dick, R. S., and Steen, E. B., editors. The *Comvuter-Based Patient Record: An Essential Technoloav for Health Care.* Washington, DC: National Academy Press, 1991, pp. 69-70.

7. Dorenfest, S. I. The Hospital Information Systems Industry. Presentation to the Work Group on Computerization of Patient Records. Washington, DC, 1992 Aug. 26.

8. Gardner, E. Reality hinders efforts to fill info system wish lists. *Modem Healthcare, 1992, Nov. 23.* pp. 35-48.

9. Glandon, G. L., Presentation to the Symposium on Computer Applications in Medical Care (SCAMC), panel on Evaluating Health Care Information Systems: A Multi-Method Approach, November 10, 1992.

10. Tierney, W. M., Miller, M. E., Overhage, J. M., and McDonald, C. J. Physician inpatient order writing on microcomputer workstations: Effects on resource utilization. *JAMA. 1993* Jan. 20. 269(3):379-383.

11. Tierney, W. M., McDonald, C. J., Martin, D. K., Hui, S. L., and Rogers, M. P. Computerized display of past test results. *Annals of Internal Medicine*, 1987 Oct. 107(4):569-574.

12. Tierney, W. M., Miller, M. E., and McDonald, C. J. The effect on test ordering of informing physicians of the charges for outpatient diagnostic tests. New *England Journal of Medicine. 1990* May *24.* 322:1499-1504.

13. Gardner, R. M., et al. Assessing the Effectiveness of a Computerized Pharmacy System. *Proceedings of the Fourteenth Annual Symposium on Computer Applications in Medical Care.* Los Alamitos, CA: IEEE Computer Society Press, 1990.

14. Department of Health and Human Services. ***Savings from the Medical and Health Insurance Information Reform Act of 1992.*** Washington, DC, ***1992*** Oct.

15. Little, A. D. ***Telecommunications: Can It Help Solve America's Health Care Problems?*** Cambridge, MA. 1992 July.

16. Agency for Health Care Policy and Research. ***Evaluation of a Comurehensive Hospital Information System . 1992.***

17. Sobolewski, J. S. Towards Implementation of Successful Medical Computer Applications. In: Blum, B. I., editor. ***Information Systems for Patient Care. New*** York City: Springer-Verlag, 1984, pp. 165-176.

18. As cited by James G. Anderson, in a presentation to SCAMC panel on Evaluating Health Care Systems: A Multi-Method Approach,: November 10, 1992.

19. Dowling, A. F. Do hospital staff interfere with computer system implementation, ***Health Care Management Review,*** 1980. 5:23-31; Lyytinen, K.,andHirschheim, R. Information systems failure--a survey and classification of empirical literature. ***Oxford Surveys in Information Technology. 1987.*** 4:257-309; Lyytinen, K. Expectation failure concept and systems analysts view of information system failure: results of an exploratory study. ***Information & Manaaement, 1988.*** 14:45-56; all as cited in Anderson presentation, ibid.

20. Gardner, E. Information systems: computers' full capabilities often go untapped. ***Modem Healthcare. 1990,*** May ***28.*** pp. 38-40.

21. Grave, F. Federal government, computers don't mix. ***Chicago Tribune. 1993*** March 7. Section 1, p. 25.

22. Abt Associates Inc. ***Overcoming Barriers to Integration and Imvlementation of Clinical Information Manaaement Systems: Feasibilitv Study.*** Project Description. 1992.

23. Dunbar, C. In pursuit of a single healthcare computing standard. ***Computers in Healthcare. 1991*** November. pp. 28-31.

24. McDonald, C. J., Martin, D. K., and Overhage J. M. Standards for the electronic transfer of clinical data: Progress and promises. ***Topics in Health Record Management, 199*** 1. 1 ***l(4)*** :1- ***16.***

25. McDonald, C. J., and Hripcsak, G. H. Data Exchange Standards for Computer-based Patient Records. In: Ball, M. J., and Collen, M. F., editors. ***Aspects of the Computer-based Patient Record. New*** York City: Springer-Verlag, 1992, pp. 157-164.

26. McDonald, C.J. ***Approach to Analysis of Computerized Patient Records,*** Presentation to the Work Group on the Computerization of Patient Records. Washington, DC, 1992 Aug. 25.

27. Murphy, G. Patient information standards development: a progress report from ASTM. *Journal of AHIMA*. 1992 Aug. 63(8):49-54.

28. Waller, A. A. Legal Aspects of Computer-based Patient Records and Record Systems. In: Dick, R. S., and Steen, E. B., editors. *The Computer-Based Patient Record: An Essential Technology for Health Care*. Washington, DC: National Academy Press, 1991, pp. 156-179.

29. Waller, A. A., Chernoff, S. N., and Fulton, D. K. Automated medical records: Legal questions and risks. *Computers in Healthcare*. 1989, *Nov.* pp. 27-32.

30. Waller, A. A. Legal aspects of computer-based patient records and record systems.

31. Ibid.

32. The Hospital Research and Educational Trust. *Inventory of External Data Demands Placed on Hospitals*. *Chicago:* HRET, 1990.

33. Golichowski, A. M., McDonald, C. J., Tiemey, W. M., Overhage, J. M., Brown, H., Lemmon, L., Blevins, L., Meeks-Johnson, J., and Glazener, T. Managing perinatal data with the Regenstreif medical record system. Journal *of Ambulatory Care Management*. 1992. 15(4):40-53.

34. Wakerly, R. The Wisconsin Health Information Network. Presentation, HIMSS Communications Conference, Chicago, 1992 Oct. 10.

35. Ambulatory Care Council. An Ambulatory Information Integration Plan for Chicago and Cook County. Report of the Information Integration Workgroup, Chicago, 1992.

36. Benton International and John A. Hartford Foundation. Community Health Management Information System. 1991 Nov. 15.

APPENDIX A

Work Groups formed at November 1991 Forum -on Health Care Administrative Cost

- **Work Group for Electronic Data Interchange (WEDI),** co-chaired by the Blue Cross and Blue Shield Association and the Traveler's Insurance Company, was challenged to recommend a plan for increasing the use of electronic claims by 10 percent each year and to examine the potential for uniform electronic billing. WEDI published a report of its findings and recommendations in July 1992. In February 1993, WED1 resumed its effort to promote the use of electronic data interchange and is currently preparing a follow-up to the 1992 report.

- **Work Group on Administrative Costs and Benefits,** chaired by the Health Insurance Association of America, formalized an ongoing activity to evaluate health care administrative costs. The group has contracted for a study to advance the public's understanding of administrative costs in the health care system.

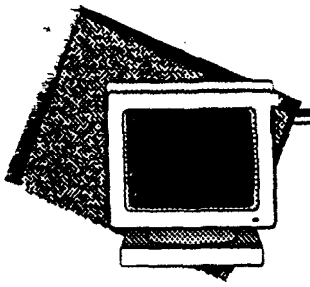
- **Work Group on Performance Monitoring,** chaired by the American Hospital Association, was created to identify ways to reduce the administrative costs associated with external utilization management. The work group brings together organizations representing providers, payers, employers, consumers, utilization review organizations, and accrediting bodies to consider ways to assure that utilization management mechanisms are efficient, contribute to quality improvement, make information available to consumers about provider and health plan performance, and are scientifically valid.

- **Work Group on Computerization of Patient Records,** chaired by the American Hospital Association, engaged in strategic planning for the computerization of patient records. The mission of the work group is to define the vision of computerized patient records from the perspective of the many organizations represented on the work group and to identify practical steps in a broadly constituted strategy to support the development and implementation of computerized patient records in our current and future health care environment.

APPENDIX B

Computer-based Patient Record Institute

Vision, Mission and Goals



COMPUTER-BASED PATIENT RECORD INSTITUTE, INC.

COMPUTER-BASED PATIENT RECORD INSTITUTE (CPRI)

VISION

The health care **delivery** system must use a comprehensive, longitudinal patient record to provide all clinical, financial, and research data.

The **computer-based** patient record contributes to more effective and **efficient** care through:

- universal, timely, and intuitiie access to lifetime health data **collected** and maintained across the continuum of care:
- support for continuous **quality** improvement in health care delivery;
- ready access to knowledge bases to support clinical practice, administration, education, and research: and
- patient participation in health status documentation, **wellness,** and disease prevention

while maintaining the confidentiality of sensitive patient and provider data.

Claims Processing

1

Administrative Reform

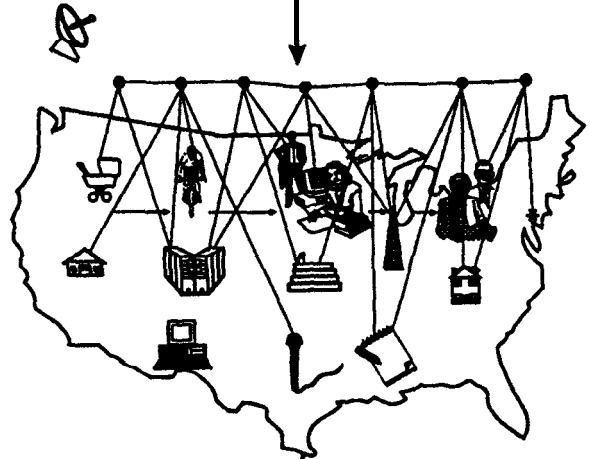
Direct **Cost** Savings

Improved Economy

Computer-Based Patient Record

Patient Care Information

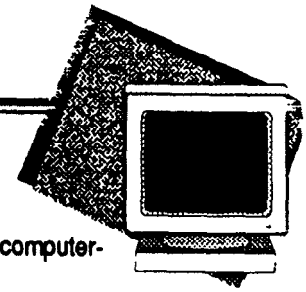
Healthcare Reform



Improved Health Status

Improved Productivity

Improved Economy



MISSION

The CPRI will initiate and coordinate urgently needed activities to facilitate and promote the routine use of computer-based patient records through health care.

GOALS

The goals of CPRI are to:

- Promote the development and use of standards for computer-based patient record messages, communications, codes, and identifiers.
- Demonstrate how computer-based patient record systems can lead to improvements in effective and efficient patient care.
- Encourage creation of policies and mechanisms to protect patient and providerconfidenttallty and ensure data security.
- Educate health professionals and the public about computer-based patient records.
- Coordinate the building of technical and legal infrastructures that enable the use of computer-based patient records.
- Promote computer-based patient record research activities.

FIRST YEAR ACCOMPLISHMENTS

Member organizations and volunteer participants helped CPRI have a very successful first year. Some accomplishments of CPRI in 1992 include:

Infrastructure

Incorporated and adopted bylaws.
Developed a comprehensive work plan.
Initiated a search for a president.
Drafted a generic funding proposal and target list of funders.

Participation

Recruited 22 organizational members.
Attracted of over 700 organizations and 1,400 individuals in a database.
Drew 150 participants to the 5 work groups.
Accepted 150 subscribers to the newsletter, CPRI Mail.
Elected 13 Board members.

Recognition

Delivered over 100 presentations.
Provided over 50 interviews for national press.
Disseminated the vision of CPR in press commentary.
Exhibited at several conferences.
Referenced in several pieces of draft legislation.
Achieved industry recognition of the term "CPR."

Communication

Held 4 general meetings, with over 400 total participants.
Wrote and mailed 6 newsletters and 5 press releases.
Created 2 promotional videotapes.
Provided educational assistance to Congressional and Agency staff.
Represented CPRI at important meetings and conferences.
Initiated development of advocacy programs aimed at health professionals.

Information Resource

Initiated a CPR lexicon.
Served as a product research clearinghouse.
Answered questions on confiintiality and security Issues.
Mated development of model poliis and procedures for access, data security and system security.
Provided input into standards setting organizations.
Coordinated with ANSI/HISPP.
Funded an electronic compendium of important literature on cost/benefits of CPR.
Initiated recommendations for universal identification.
Initiated analysis of coding schemes.
Initiated functional specification definition.

COMPUTER-BASED PATIENT RECORD INSTITUTE, INC.

APPENDIXC

American National Standards Institute

Healthcare Informatics Standards Planning Panel

Scope, Purpose, Mission and Functions

ANSI
American National
Standards Institute 11 WEST 42ND STREET. NEW YORK, NEW YORK 10036
TEL 212.642.4900
FAX. 212.398.0023
Cable: Standards, New York
International Telex: 42 42 96 ANSI UI
D-U-N-S 07-329-4837

HISPP 4
(Revised September 1992)

AMERICAN NATIONAL STANDARDS INSTITUTE
HEALTHCARE **INFORMATICS** STANDARDS PLANNING PANEL (HISPP)

CHARTER STATEMENT

Scope:

Healthcare informatics Standards. This shall include standards for:

1. Healthcare models and electronic healthcare records.
2. The interchange of healthcare data, images, sounds and signals within and between organizations/practices.
3. Healthcare codes and terminology.
4. The communication with diagnostic instruments and healthcare devices.
5. The representation and communication of healthcare protocols, knowledge, and statistical databases.
6. Privacy, confidentiality and security of medical information.
7. Additional areas of concern or interest with regard to healthcare information.

Purpose and Mission:

To perform the functions of a Standards Planning Panel per Section C2.3 of the ANSI *Procedures for the Development and Coordination of American National Standards* in the field of healthcare informatics standards. Specifically, the planning panel would coordinate the work of the standards groups for healthcare data interchange and healthcare informatics (e.g., **ACR/NEMA**, ASTM, HL7, IEEE) and other relevant standards groups (e.g., X3, X12) toward acheiving the evolution of a unified set of non-redundant, non-conflicting standards that are compatible with **ISO** and **non-ISO** communications environments. In addition, a balanced subcommittee of the planning panel shall interact with and provide input to **CEN/TC** 251 (Medical Informatics) in a coordinated fashion and explore avenues of international standards development (e.g., **ISO** and IEC).

This effort is both timely and urgent. The standards being developed will yield many improvements and efficiencies to the delivery and management of healthcare. They will also greatly facilitate health services and medical effectiveness research. Moreover, CEN/TC 251 (Medical Informatics) has requested input to their standardization efforts. If the USA is to have influence in these developments, we must be able to provide early input to their process and a unified response to their proposals.

The ANSI **HISPP** will not write standards or make technical determinations, which is the purview of existing standards developing organizations and committees. It will serve a coordination role deemed appropriate by ANSI's constituency for such panels, in cooperation with these groups and in accordance with Appendix C of the ANSI *Procedures for the The Development and Coordination of American National Standards.* All materially and directly affected interests are strongly encouraged to participate in this open forum to foster cooperation and coordination, so that its efforts may benefit from all possible perspectives and expertise. Cooperation and coordination can only be achieved and effective through active participation, information exchange and agreement by all concerned interests.

AMERICAN **NATIONAL STANDARDS INSTITUTE**
HEALTHCARE INFORMATICS STANDARDS PLANNING PANEL (HISPP)

FUNCTIONS AND OPERATIONS
(Adapted from Section C2
of the ANSI *Procedures for the Development and Coordination of American National Standards)*

Functions:

In accordance with Appendix C of the ANSI *Procedures for the The Development and Coordination of American National Standards.* the ANSI HISPP will:

(1) Define problems;
(2) Determine whether standards can solve identified problems;
(3) Identify the scope and subject of needed standards;
(4) Determine priorities for the development of needed standards;
(5) Determine whether standards projects are already underway which cover the scope of needed standards;
(6) Encourage developers to initiate projects for identified needs;
(7) Coordinate the actions of standards developing organizations and committees undertaking such projects;
(8) Develop a schedule for the timely development and promulgation of needed standards.
(9) Take action on behalf of, or make recommendations to other ANSI boards, councils, committees or panels, as appropriate, on issues related to national, regional and international healthcare informatics standardization.

Membership:

Voting membership of the ANSI HISPP shall consist of various entities (organizations, companies, government agencies, individual experts and the like), and the greater majority of these Panel members should support the efforts of the Institute to conduct this Panel through membership in ANSI. The membership will be categorized by interest groups such as Users, Producers. Professional/Trade Associations, Government Agencies, Standards Developers, and Others. The ANSI Executive Standards Council (ExSC) shall approve the initial membership of the Panel and any requests for new memberships, based on the ability of those seeking membership to make major contributions to the functions of the Panel.

Officers:

The ExSC shall appoint the initial Chairman of the ANSI HISPP. Thereafter, the Chairman shall be elected for a one-year term of office by a simple majority of the voting members of the Panel.

Staff:

A member of the ANSI staff shall serve as Secretary of the Panel without vote. The Secretary will provide all required administrative support for the Panel.

Structure:

Subcommittees of the Panel may be formed for specific sectors of healthcare informatics standardization, if needed, and temporary ad hoc groups may be convened to accomplish specific tasks.

Meetings:

The ANSI HISPP shall meet as necessary.

Actions of the ANSI HISPP:

Actions of the ANSI HISPP shall be by majority vote of the full voting membership, either at a meeting with a quorum present, or by letter ballot. Any actions or inactions may be appealed to the ExSC.

Reports:

The ANSI HISPP shall report to the ExSC at least annually, or upon request of the ExSC. The ANSI HISPP Chairman will serve as an non-voting ex officio member of the ExSC.

APPENDIX D

Computer-based Patient Records:

Confidentiality, Privacy and Security Concerns

COMPUTER-BASED PATIENT RECORDS: CONFIDENTIALITY, PRIVACY AND SECURITY CONCERNS

INTRODUCTION

Much of American society views the computerization of personal information with suspicion, if not overt hostility. Episodic reports of individual and institutional abuse of computerized personal information fuel this public distrust.

Nowhere is this more likely to be true than with health information. Information about the functions of a person's own body, in illness or health, is some of the most intimate information possessed by an individual. It is quite likely that convincing the public that the confidentiality of their health information can be guaranteed will be a difficult task when the data are held in electronic repositories, and potentially accessible to perhaps millions of people. Patients may fear that governments, companies or individuals who can affect their lives may gain unauthorized access to their health information, and use it to make adverse decisions about them, or to take actions that result in their harm.

The Work Group on Computerization of Patient Records that society's concerns about the privacy and confidentiality of health information must be resolved in order for the vision of a national system of computerized health records, connected by electronic health care networks, to be realized.

The public must be assured that the benefits of computerization contributing to their personal good, and to the public good, substantially outweigh its potential risks. Otherwise, citizens are likely to (1) oppose any legislation and government spending that may be required to implement computerized systems, (2) lose their trust in the overall health care system, and (3) withhold information from health care providers that could be key to provision of appropriate care. Most importantly, lack of such assurance may lead to the weakening of the relationship between individual patients and providers.

THE GOAL OF THIS REPORT

This appendix to the Work Group report analyzes the risks and benefits to patient privacy of computerizing health care information, documents the controls currently imposed on access to that information and identifies areas of weakness in those controls. It lays out, where possible, the types of controls the Work Group believes should be in place to protect patients' important rights of privacy and confidentiality, and to build public trust in the electronic health care system of the future.

For the purposes of this report, privacy is defined as the right of individuals to control disclosure of their personal information. Confidentiality is the expectation that information, when provided to an authorized user, will not be redisclosed. Data security refers to the methods by which access to confidential information is limited.*

*As used here, data security does not include the concept of data integrity, which would include methods to ensure that data is entered and changed only in an authorized and prescribed manner, and that random errors do not creep into the data. The latter issue is beyond the scope

The scope of this section's recommendations includes all electronic health information, which is defined here as individually identifiable health records and other clinical information maintained in electronic form -- whether held by an insurer (e.g., diagnoses, procedures), a provider, or an employer (requests for sick leave).

As the Privacy Protection Study Commission said so well 15 years ago, there is a need to balance the legitimate needs of users of information with the right to privacy. Here, the Work Group attempts to locate the proper balance point between that right and uses that contribute to the private and public good. Where enough knowledge is not available to make judgments, the report recommends areas for further research, concept definition and legal and legislative action.

The section attempts to build on, rather than supplant, the valuable recommendation and analysis of issues related to confidentiality contained in the report of the Workgroup for Electronic Data Interchange (WEDI).[1] It also attempts to complement, rather than duplicate, the work of several other groups considering similar issues.

Unlike other reports addressing the privacy issue, this one does not attempt to recommend criteria for all the possible uses for which various entities -- from life insurance companies to employers to banks -- may ask an individual for authorization to access his or her health records. While the Work Group believes that many of these issues need to be resolved, we recommend that the existing bodies responsible for legally or voluntarily regulating each industry set the ethical standards as to the appropriate and inappropriate uses of health information.

This section owes a particular debt to the Secretary of Health Education and Welfare's Advisory Committee on Automated Personal Data Systems, which in 1973 defined the following principles, to which the Work Group subscribes:

- 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 or. her is in a record and how it is used.
- There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his/her consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him or her.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must take precautions to prevent misuse of the data.

THE SECURITY OF PAPER RECORDS

Today's patient record is, essentially and most often, a paper record. Some patient care data, such as medical laboratory reports, is already widely produced in electronic form. But to date

of this section.

there have been no widespread conversions from paper to computer-based format of all the elements which typically comprise a patient record.

If a paper record is in active use (or at a minimum, not in locked storage), anyone who comes in physical contact with the record can, conceivably, read it. The detective hero in the movie "Fletch" dresses in medical garb, walks into a hospital's medical records storage room, finds the record he seeks, and reads it. This is a (stylish, but) fictitious example; however, unauthorized access to paper-based patient records can be easy, and is probably more common than the public realizes and the provider community would like to admit.

Existing controls over access to health information often rely on physical control over paper records, physical access to computer terminals, written signatures, visual identification of authorized users, and other mechanisms that will not necessarily be easily adapted to an electronic world.'

The security of copies of paper records provided to entities monitoring provider performance (e.g., insurers, Medicare Peer Review Organizations) relies on the integrity of the U.S. mail, and on laws preventing tampering with the mail. Another assumption implicit in mailing records is that the volume of items sent through the U.S. mail is huge, and that it is difficult to locate an individual package. Neither of these assumptions will apply to electronic records.

Access to a health record itself may be difficult to achieve -- it requires physical presence at the site where records are stored -- but when authorized access to a health record is provided, it frequently provides access to all information contained in that physical record. Special security may be provided to specific data elements simply by storing them in different forms and different locations.

However, in the current, paper world, it is difficult to properly secure information that must be available immediately or is frequently used. It is difficult to control access to particular pieces of information based on a person's role (in providing care, billing, etc.) or need to know.

COMPUTERIZATION AND THE RISK OF DISCLOSURE

Electronic maintenance of health records poses similar risks. Anyone who can gain access to the electronic files where such records are stored will be able to "see" the records. If the information comprising the records is not protected or encrypted in some way (or not adequately protected), anyone who can "see" the records will be able to read them.

Even with the rapid expansion of computers into health care, Deborah L. Hamilton of Hewlett-Packard Laboratories has stated that no data security system currently available truly meets the needs of health care (as outlined above). Most security systems, she says, either "emphasize confidentiality above all else" --as appropriate for the military -- or provide rapid, widespread information access. Health care needs a combination of both.'

Computerization also heightens some risks to data security. First, large amounts of computerized information are often maintained in one place. Therefore, if someone gains unauthorized access to a computerized system that contains health information, he or she could potentially access much larger quantities of information much more quickly than if he or she had gained unauthorized access to a warehouse full of paper records.

Second, as the industry develops and implements patient information systems that share data across multiple sites, the security risks are magnified. Networked information may be

transmitted over public communication channels such as telephone lines or by radio, which greatly increases the security risk. Nationwide electronic networks would potentially give a much larger number of entities access to records.

Third, as large-scale storage and analysis of personal records becomes feasible, the potential uses of such information will multiply. Providers, payers, policy makers, researchers will all find the availability of vast amounts of computerized health care information seductive, and it is likely that many more individuals and organizations will claim they "need to know", to have access to the information, than make such claim today.

Fourth, computerization lowers the cost of collection and maintenance of information. This can encourage the collection of more data from health records than is strictly necessary for a given purpose (such as research), and the unnecessarily-collected data may then be maintained in a central database, where it may be vulnerable to misuse.[4]

Finally, linkage of an individual's computerized health records across providers would require a nationwide health care identification coding system. If an existing coding system, such as the Social Security Number (SSN), were used for health records, information about an individual's health status could potentially be linked, without the individual's consent, to financial records, military records, or other records that include the SSN. The information created could then be used to the individual's harm.

Many of these enhanced risks may be exemplified by a recent case in which a banker who was a member of a state health data commission linked the names on a listing of cancer patients to a list of his borrowers, and called in the mortgages of those who were on both lists.'

Additional risks to data security will arise during the period in which the transition from paper to computerized health record systems is being made. During this period (which has already begun) those individuals and organizations which use and maintain patient care records will be supporting two parallel record systems: a paper system and a computerized system. Assuring the type of privacy and confidentiality protections recommended in this report will be exponentially more difficult in the management of two parallel, physically distinct, patient record systems.

As can be seen, computerizing health information poses some risks to confidentiality. However, the Work Group believes that the power of computers also gives society the ability to improve on paper-oriented controls by imposing more detailed, uniform and enforceable controls over who has access to which elements of information.

Under the proper data and system security measures, the health information in fully computerized patient records would be far less accessible to unauthorized users than the information in paper patient records is today.

Recommendation: The Work Group endorses the WED1 recommendation that overall data security for health information be established through federal legislation (detailed below).[6] The Work Group also recommends that specific data security mechanisms and standards be developed by voluntary standards organizations (such as those cooperating in the American National Standards Institute's Healthcare Informatics Standards Planning Panel), and to be applied uniformly across the health care system.

The Work Group believes strongly that both the legislative standards and the specific standards set by voluntary groups must be in place before a computerized health care records system can

operate nationwide. We believe mechanisms to control access to those authorized must be stringent, and the effectiveness of these mechanisms must be understood and accepted by the general public.

These mechanisms should be able to restrict access to select individuals to read, store, retrieve, transmit, and share information. Individuals should be able to gain access according to their authority under the statutory disclosure provisions recommended below, or by authorization by the patient.

Recommendation: To provide for the enforcement of laws and regulations regarding confidentiality, and to allow imposition of penalties for misuse, the'information system must maintain an audit trail. In particular, the system must be able to trace all data access activities and to know where the data came from, who generated and who accesses the data, and when. Patients must be provided access to the audit information.'

What would have happened if our movie detective had been looking for a fully computerized patient record, protected by such data security measures? Unless the information he sought was already on screen, Fletch's search for the right record would likely have yielded him no more than an "Access Denied" message.

THE HUMAN PROBLEM

The problem of unauthorized disclosure of health record information after authorized access to the record will remain when the health care industry switches from paper to electronic records. This is a human problem, not one of system or data security.

The concerns generated by this uncondoned activity, when considering computerized health records, arise from the potential for far more individuals having authorized access to computerized record than do so now to paper records. Unfortunately, the sad fact is that the more individuals there are with authorized access to the data, the greater the likelihood there is of unauthorized disclosure of some of it.

This problem is compounded by the lack of restrictions as to which employees or agents of an entity that has been authorized access to a record, may individually access the record. A number of cases have been litigated in which, for example, a hospital administrator looks at the records of relatives or acquaintances, for reasons other than improving the patients' care.[8]

Recommendation: The Work Group recommends that a provider, payer or other entity restrict access to specific elements of patient health information according to an individual's role in providing care or other services to the patient, and according to the individual's "need to know. "

Recommendation: The Work Group recommends that the penalties for ***inappropriate use*** of confidential information (e.g., discrimination, employment decisions), as established in the Federal preemptive legislation recommended below, be severe, and that enforcement of these penalties be strict. Fines should be large enough so that they will not be considered just another cost of doing business; prison sentences should be long enough to be effective deterrents. Penalties for ***inappropriate access (e.g.,*** reading confidential information) should also be established, but should be somewhat less severe than those for inappropriate use.

Recommendation: Even with the protections offered by the preceding two recommendations, the Work Group believes that most problems society may encounter in this area will have to

be dealt with through non-technical means -- through training, education, and professional codes of ethics.

Societies of health professionals should strive to educate their membership about their responsibilities in adhering to ethical codes that require them to protect the confidentiality of patient information, and to high personal standards of behavior.

Providers should teach all their employees, contractors and medical staffs, who have access to health record information about proper security methods, and educate them as to the prohibitions against the data's unauthorized disclosure or use. This education should stress that individuals and organizations who disclose health care data without authorization, or use the health care information to which they have access in prohibited ways, will face severe penalties for such unauthorized disclosure or prohibited use.

POTENTIAL LIABILITY PROM DISCLOSURE

The legal duty to protect confidentiality of patient information is independent of the medium -- electronic or paper -- by which the information is collected and stored. However, as noted above, the potential for large-scale breaches of data security are substantially greater with computerized patient information, and the associated liability risks are therefore greater.

Compounding the problem is a lack of generally accepted data security standards to protect this computerized information. According to Adele Waller, "currently feasible computer security measures are particularly inadequate for networked systems and probably cannot protect providers that install computer-based patient record systems from substantial exposure to liability. "[9]

The American Medical Association's (AMA) Council on Scientific Affairs has found that when an improper disclosure occurs the patient will almost always sue the provider maintaining the record -- regardless of the precautions the provider took to protect that record.[10] Because of the liability risk, providers may be hesitant to share sensitive information via electronic networks.

Recommendation: The Work Group recommends that an operational, nationwide standard .of computer security be established. These minimum operational standards for security and confidentiality should be reviewed and updated on an ongoing basis. Providers will be more likely to share sensitive information via electronic networks if they can use accepted security standards as a defense in a lawsuit.

We believe the standard should hold that those who collect, maintain and disclose patient identifiable information should be expected to take stringent but reasonable measures to protect the confidentiality and security of the information. The standard should not require that these measures be absolutely fail-safe, in order for an entity to be protected against liability.

Recommendation: The Work Group also recommends that providers take special legal precautions to protect themselves, because they bear the greatest risk of liability from unauthorized disclosure. The AMA Council on Scientific Affairs has evaluated this issue; we agree with the Council's recommendation that a provider should include provisions on confidentiality in contracts with all third parties, including payers and other providers, that the provider has given access to patient records.
We recommend that these contracts require the third party to:

- Keep individually-identifiable patient information from the records in strict confidence;
- Use the information only for the purpose for which it was obtained, as specified in the contract;
- Control disclosure of the information to only those employees who have a need to see it, based on their role in carrying out the purpose for which the information was obtained, as specified in the contract;
- Return or destroy any information no longer needed to carry out the purpose for which the information was obtained;
- Xndemnify the provider or practitioner for liability from breach of confidentiality or security by the third party.

LEGAL PROTECTIONS

Current laws governing providers' responsibility to protect confidentiality are inconsistent and inadequate. State licensure laws and the common law both impose obligations on providers to preserve the confidentiality and security of health records. Although they are generally similar in their intent, these laws differ from state to state both in scope and application.

The inconsistencies among states already create difficulties for some providers attempting to comply, for example when a health care organization operating in more than one state attempts to centralize its record-keeping operations. Increasing use of electronic health records is expected to aggravate these difficulties. Records will be routinely transmitted electronically across state lines, and may even be created simultaneously in two different states; as when a physician working across the Wisconsin border dials into the computer system of a hospital located in Illinois.

In addition, many state laws do not address certain key issues, such as (1) a patient's right to see, copy and correct his or her own records; (2) the need for special protections for information about certain conditions about which there is heightened risk of discrimination (e.g., HIV infection, genetic abnormalities, mental illness, and substance abuse), and (3) the obligations of providers other than hospitals and physicians to protect confidentiality.

In 1985, the Commissioners on Uniform State Laws developed a Uniform Health Care Information Act (UHCIA) in an attempt to address some of these issues and to standardiie the laws governing how providers can use and disclose health information." This model act has been praised by legal experts, but only two states -- Montana and Washington -- have enacted it.

The legal obligation of parties other than providers to protect patient information is similarly inconsistent among states, and it is even less well defined. The Federal Privacy Act protects the confidentiality of personal information collected by the federal government, but the protection is far from absolute. Although some states have adopted the provisions of the Privacy Act, there are still many states in which there are no laws establishing the framework for the use and disclosure of patient information for research purposes.[12]

A variety of state and federal laws restrict private payers from releasing patient-identifiable health information. However, according to the WEDI report, the only "universal" deterrent to

improper disclosure is a civil suit for invasion of privacy and even this deterrent is limited. For example, it can only be applied if a patient knows his or her privacy has been invaded; there is some evidence that most privacy violations go undetected.[13] Also, as with state laws governing providers, patients are not always granted the right to access or correct the information about them contained in payer files.

The National Association of Insurance Commissioners (NAIC) has developed model legislation which addresses disclosure of personally identifiable health information by insurers and insurance support organizations (e.g. utilization review firms, the Medical Information Bureau). The legislation also includes provisions which allow the patient to access and correct their records. So far, the model legislation has been adopted by only thirteen states.

Also of interest is a proposed Privacy Directive under consideration by the European Economic Community (EEC), which addresses collection, management and use of personal data. The directive requires the entity controlling a file to take appropriate technical and organizational measures to protect personal data against accidental or unauthorized access, modifications, or processing. It also outlines the rights of individuals identified by the data, which include the right to know the name and address of the controller of the file, to know everyone who has accessed it, to examine the information, and to correct it.[14]

Recommendation: The Work Group believes that Federal preemptive legislation is necessary to resolve the inconsistencies and inadequacies in existing law. We concur with the WED1 recommendations that such legislation require a Federal agency, with input from consumers, providers, payers and other interested parties, to set standards for the confidentiality of health care information. [15]

The Work Group disagrees, however, with WEDI's recommendation that these standards be established by the Secretary of Health and Human Services. We believe that allowing the Secretary to set these standards could pose a conflict of interests, as HI-IS is itself an interested party in the use and disclosure of personally-identifiable health information.

The Work Group therefore recommends that the legislation establish an independent Federal Privacy Board, with members appointed by the President to represent consumers, providers, payers, researchers, other federal and state agencies, and other interested parties. The Privacy Board would be responsible for setting standards, implementing and enforcing the provisions of the preemptive legislation recommended here.

The Work Group agrees with WED1 that the provisions of the federal preemptive legislation should:

- Establish uniform requirements for preserving confidentiality and privacy rights.
- Apply to the collection, storage, handling, and transmission of individually identifiable health care data, including initial and subsequent disclosures, in electronictransactions, by all public and private third party payers, providers and other involved in the transactions.
- Not mandate changes in state public health reporting laws.
- Establish security protocols for electronic storage, processing and transmission of health care data.

- Specify fair information practices that create a balance between what information an individual is expected to divulge to a record-keeping organization and what he or she seeks in return; minimize the extent to which the information is a source of unfairness in any decision made on the basis of such information; and create and define obligations respecting the use and disclosures of such information.

- Require publication of the existence of health care data banks. The Work Group also recommends that the distribution of such publications should be specifically targeted at consumers. (For example, publication in an insurance company trade journal would not be sufficient).

- Establish appropriate protections for highly sensitive data (e.g. mental health, substance abuse, communicable and genetic diseases).

- Establish that compliance with the Act's requirements would be a defense against actions for improper disclosure.

- Establish penalties for violations of the act, including civil damages, equitable remedies, and attorneys fees where appropriate. The Work Group believes this provision is particularly important to building public trust in the confidentiality protections.

- Provide for enforcement by government officials and private, aggrieved parties.[16]

The Work Group also recommends that the above legislation and standards should apply not only to electronic information for health insurance purposes (as WEDI recommended), but also to all other health information, regardless of the medium in which it is stored, the entity or individual involved in collecting, maintaining and processing it, or the purpose for which it is collected.

The Work Group recommends that the EEC directive and the UHCIA model also be considered in developing Federal legislation and standards. (Additional areas for which we recommend development of legislation and standards are discussed below).

PATIENTS' ACCESS TO RECORDS

Patients frequently perceive difficulty in gaining access to their own health care records. This is despite the fact that the laws of most states grant the patient or the patient's authorized representative at least a limited right of access to his or her medical records. This right has also been granted by the courts in states without such laws.

However, some states restrict access to records pertaining to a patient's mental health. In addition, several states do not permit a patient to inspect his or her hospital record until after the patient has been discharged.[17]

The American Hospital Association publication, "A Patient's Bill of Rights," states as principle that: "The patient has the right to obtain from his physician complete current information concerning his diagnosis, treatment and prognosis in terms the patient can be reasonably expected to understand. When it is not medically advisable to give such information to the patient the information should be made available to an appropriate person in his behalf."[18]

The American Hospital Association's policy on disclosure of patient record information states

that patients should also have the right to:

- Verify that a hospital has created and is maintaining a record of his or her care;
- Determine to whom disclosure of the record has been made;
- Request a copy of the record upon payment of reasonable charges for the service;
- Request correction or amendment of information included in the record; and
- Designate a representative to have reasonable access to information within the record.[19]

The American Medical Association (AMA) has an official policy on Patients' Access to Information Contained in Medical Records stating that "allowing patients access to information in their medical records will have, on the whole, a favorable impact on patient care and physician-patient relationships, provided that appropriate safeguards are incorporated in the enabling legislation enacted by the state."[20]

The AMA's Council on Ethical and Judicial Affairs has also issued an "opinion" relative to the issue of patients' access to records. This opinion states that, "...on request of the patient a physician should provide a copy or a summary of the record to the patient or to another physician, an attorney, or other person designated by the patient." The Council has also stated that, "medical reports should not be withheld because of an unpaid bill for medical services."[21]

The Joint Commission on Accreditation of Healthcare Organizations has a standard stating that "the patient and/or the patient's legally designated representative has access to the information contained in the patient's medical record, within the limits of the law."[22]

Recommendation: The Work Group recommends that, in addition to the provisions outlined by WEDI, the Federal legislation or standards outlined above establish standards and procedures for patient examination, copying and correction of any patient identifiable information.

The Work Group suggests that the policies of the American Hospital Association, the American Medical Association, and the Joint Commission serve as a starting point for developing these standards.

PATIENT AUTHORIZATION FOR DISCLOSURE

Even if federal law gives patients the right to access their records, in practice access would still be limited. Most patients are unaware of who is maintaining information about them because the authorization forms allowing providers to redisclose their information (to payers, utilization reviewers, life insurers, etc.) are so broad.

A typical payer's authorization form requires a patient to authorize a provider to furnish whatever information is necessary to process a claim, in return for receiving reimbursement for the service.[23] Generally, the period of time during which the authorization is valid is not limited and the form does not specify how the information will be used or who will have access to it (this will be discussed later in the section). In essence, many authorization forms require patients to provide unlimited access to their personal information in order to receive benefits.

Currently, many individuals may not fully understand that their signature on a particular document authorizes release of their health record data to other parties. Those that do

understand this may not fully appreciate all the implications of the uses to which their released health record information may be applied. And in authorizing release of health record data, individuals may not make a distinction between data containing individually identifiable information, and data in which such information is shielded.

_ For example, if a patient believes information she has given her doctor will be used only to help treat her, help pay her doctor's bills, and help disinterested researchers -- because that is all she believes she has given her authorization for -- she should not subsequently be solicited by individuals or organizations offering products to her based on their knowledge of her most recent health history, if that knowledge has come because others had access to the data in her health record.

In the hypothetical example given above, we use the expression "if ... others had access ...". By "others", we mean those with authorized and direct primary access to the record, as well as those with authorized but indirect, secondary access to the record or to particular elements of it.

Recommendation: The Work Group recommends that the legislation and standards outlined above also establish standards for agreements in which patients authorize the redisclosure of their health information. Such authorization agreements should (1) specify, in sufficient detail, the purpose for which information is being disclosed, (2) prohibit **redisclosure** for any other purpose, and (3) limit the period of time for which authorization for disclosure is granted.

The Work Group also recommends that providers make a special effort to educate their patients that information held in their health records will, in the normal course of business and science, be seen by others. The patient should be told who else is to have access to the health information, what part of the complete set of information each entity is to be allowed to see, and what the purpose is of each disclosure. Only then should patients be asked for their informed consent for such disclosure.

If the organization (such as an insurer) collecting and using an individual patient's health care data cannot or will not adequately and completely inform the individual of the uses to which the data will be put, the individual should have the right to deny that entity access to his or her health care data, without being denied the benefits that would otherwise be available.

The Work Group also believes that if an individual furnishes proof that his or her personal health care information has been accessed or was or is being used inappropriately or illegally, the individual should be allowed to withdraw any previously given authorization for access to his or her health information (within the limits of other provisions of law, and only, with respect to payers, after payment for services already provided has been processed).

OWNERSHIP OF PATIENT HEALTH CARE INFORMATION

Ownership of patients' health care information is a complex topic, because ownership of patient health records has long been held to be divisible.

On the one hand, it is generally accepted, and enshrined in some state laws and hospital licensing regulations, that the physical patient record is the property of the health care institution that has provided the care.

On the other hand, it is also generally accepted and supported by common law and many state laws that the patient owns the information about care provided to him or her contained in the

record. Generally, this latter ownership right gives the patient control over the disclosure of the information in the record contents, with certain limitations (e.g., disclosure under public health reporting statutes, limiting patient access to their own records when such access is deemed to be potentially harmful to the patient.)

It is frequently unclear, however, exactly what rights and responsibilities are associated with these ownership rights. And those rights and responsibilities that are clearly defined may vary from state to state, as it has been held that the patient does not have a federal constitutional right of ownership.[24 25]

As a result the following issues arise: Does the right of ownership of the physical record imply responsibility to control access to the information contained in the record? What are the limits of this right of ownership? Do the rights and responsibilities that apply to health care institutions also apply to other types of providers maintaining records, such as pharmacies maintaining prescription records?

Introducing the concept of electronic storage of health records raises even more complex questions, such as: What constitutes the physical record? Who owns the physical record in a networked environment where providers from multiple organizations record information in a shared database?

Little legal research or analysis of the issues has been conducted on ownership of information stored electronically. In an attempt to fill this gap, the Institute of Medicine (IOM) Committee on Regional Health Data Networks is conducting a ten-state review of ownership provisions, as part of its review of issues related to the John A. Hartford Foundation's Community Health Management Information Systems projects.

Recommendation: The Work Group believes that federal legislation will eventually be needed to uniformly defme the concept of ownership of electronic health information. However, before development of such legislation can begin, the Work Group believes further study, analysis and definition of the rights and responsibilities and associated with ownership is needed.

While the IOM's ten state review will be an important first step in evaluating current law, it is unlikely to be sufficiently comprehensive to serve as the basis for the development of federal preemptive legislation, We recommend that a thorough analysis of current state laws and applicable case law related to other industries, as well as to the health industry, be conducted. This analysis should call on people experienced with developing and enforcing contracts between providers and shared computing services, who may be able to help identify some of the problems and potential solutions to defming ownership of information in an electronic environment.

THE BALANCE POINT

A variety of individuals and institutions have a self-defined "need" to see clinical information about individual patients. These include the primary users of the information -- patients and health care providers providing services for the patient -- and a number of secondary users of information generated by those providers and patients.

The secondary users include: health care providers not treating the patient (for education or quality assurance); health insurers (for payment and performance monitoring and underwriting); life insurers (for underwriting); employers (for pre-employment fitness and drug testing, health insurance and workmen's compensation claims, and monitoring of worker exposure to hazards);

researchers; and government agencies (for monitoring public health and determining eligibility for benefits.)[26]

The number of potential secondary users is expanding, and, as noted previously, requests to access such data can be expected to increase even more rapidly, as large quantities of information become accessible in one place and in electronic form.

Patients' desires to keep their records confidential may conflict with these users' needs. The proper balance between these clashing needs and desires have often been decided in court,*' as most state laws now say that only the patient may authorize his physician to disclose health care information that is protected by the provider-patient privilege, except for information required to be reported to the state under state law.[28]

Recommendation: The Work Group believes that such privacy issues should not, in general, be adjudicated on a case-by-case basis, resulting in decisions that may be contradictory, or have limited application and limited jurisdiction. Instead, the Work Group believes that patients should control what specific disclosures of their information are made, within a broad Federal regulatory framework.

This framework should be established by the Privacy Board. It would govern what types of disclosures are permissible without the patient's authorization. It would attempt to balance the patients' rights to privacy with the benefit of specific unauthorized disclosures to the good of individuals other than the patient, and to the good of the general public.

The Work Group outlines the issues surrounding several specific cases of information disclosures below, although it does not make any recommendations as to their resolution, In discussing these cases, the Work Group assumes that a nationwide electronic health care information system can provide patients the opportunity to authorize access to their records in situations where obtaining authorization would not previously have been practical.

Individual Providers

The greatest benefit of computerizing patient records is that providers will have easy access to complete patient health histories, without relying on memory, that could dramatically affect their treatment of a patient.

Currently, a new provider typically only knows about a patient what that patient chooses to reveal. The patient allows that provider to access his or her clinical information in the expectation of a benefit: that the information will assist the provider in maintaining his or her health or curing an illness. Conversely, if a patient chooses to withhold elements of his or her medical history from the provider, he or she may reduce the expected benefit or place him- or herself in danger.

If patient records are available through an electronic network, the potential exists for a provider to access a patient's medical history without the patient's authorization. The patient's control over his or her own clinical information could thus dramatically decrease. While this may increase the clinical benefit to the patient, some patients might choose -- if they were given the choice -- to protect their privacy and forego the benefit.

Another benefit of computerizing patient clinical information is that it facilitates communication among providers and the coordination of care. When diagnostic images, for example, can be sent over electronic networks, practitioners will be more likely to consult with experts about

interpretation and diagnosis -- leading to the likely improvement of appropriate diagnosis and treatment.

Sometimes, a practitioner may feel that it is not feasible to obtain the patient's consent for such consultation. While it may not be current practice not to provide a consultant with information identifying the individual patient, it would be theoretically possible for the original provider to discuss the case without identifying the patient, without reducing the quality of the consultation.

Emergencies

Currently, a provider treating a patient in an emergency situation generally has little access to previous health information about that patient. Because this information may not be availabie, the Centers for Disease Control currently recommends that emergency workers treat all unknown patients as if they are potentially infectious.

Computerization of health records promises a great improvement in the availability of such information, which may provide great benefit to the patient. An electronic system could also be designed to allow those patients who wish to forego some or all of such benefits complete discretion on what data would be released and what withheld. For example, a patient may wish to keep information about AIDS or other infectious diseases private even in emergencies.

However, providers may argue that they need this information in order to protect themselves from the hazard, and may refuse to provide services unless the information is provided. In fact, the Ryan White Comprehensive AIDS Act of 1990 states that an emergency response employee must, upon his or her request, be informed if a patient he or she has been exposed to has a life-threatening disease, and if the employee has been placed at risk.[29]

Public Health Officials

Many states have statutes requiring the compulsory reporting of various diseases. Some, but not all, of such reporting includes individually-identifiable information. The intent of such reporting is to protect the public from harm. The computerization of patient records could lead to vast improvements in the availability and accuracy of such reportable information. If records were accessible through a network, such reporting could even be made automatic, and built into the system.

Sometimes, reportable information is used to take or recommend public health precautions affecting the general population. However, sometimes it can result in decisions that restrict an individual's rights, such as quarantine or compulsory treatment of a disease. The spread of AIDS has highlighted this conflict.

Many public health agencies deal with this conflict by, for example, not informing sexual partners of AIDS patients as to which of their partners has tested positive for HIV, but simply that they may be at risk. If the person being informed has had a limited number of sexual partners, however, it may be possible for him or her to deduce which partner is infected.

Courts

Courts have held that unauthorized disclosure of health record information may be made by providers without incurring legal liability in certain circumstances, including disclosures made as part of the judicial process. The Federal Privacy Act does not protect against disclosure of health information when required under a court subpoena. Consumers may fear that if

individually-identifiable health information is stored in large databases, litigants may routinely subpoena and screen large numbers of records for use in legal cases.

Researchers

Improving data for research about health services, national health status and the effectiveness of care will be one of the major benefits of widespread computerization of patient clinical information. In order to achieve this benefit, researchers need to have access to large amounts of compiled individual data without contacting each time such access is granted.

While for some research purposes data without identifiers or with scrambled identifiers will suffice, linking individuals' records derived from different sources, or conducting follow-up studies based on the records, inevitably requires identification.

Researchers argue that allowing patients to determine whether their records can be used for research or statistical purposes could be extremely cumbersome, and could bias the results of such projects.

The Privacy Protection Study Commission said that individuals are less likely to be concerned about violation of privacy if information about them collected without their consent is used solely for research and statistical purposes, as long as they are guaranteed that (i) such information cannot be used to make decisions about them and (ii) they cannot be identified in any published research or statistics.

Both the Public Health Service (PHS) and HCFA attempt to make these guarantees by signing agreements with researchers providing them individually-identified information on the condition that no information be published or redisclosed. The PHS Act protects such information from disclosure even in court.[30]

However, Dr. George Way, president of the Medical Society of New York, believes that such agreements will fail to eliminate widespread public concern. He has voiced the fears of some that, at least with respect to government research, "the collection of medical data for the entire population will serve to undermine the traditional dynamics within the physician/patient relationship. Patients...will be reluctant to share such information with the physician".

PERSONAL IDENTIFIERS AND DATABASE LINKAGE

An issue which will have to be resolved early in the process of moving to a nationwide electronic health information system is that of settling on a useful, and agreeable, patient identification code number (or other symbol) to be used in electronic health records systems.

The already available and near-universal Social Security Number (SSN) is most often mentioned when the subject of the personal identifier is raised. Its ubiquitous nature gives it obvious advantages. Unfortunately, it is this same ubiquitous nature that also gives rise to the disadvantages of using the SSN as the personal identifier.

Of most concern is that the SSN already identifies individuals in other, non-health-related, computerized data sources; by using an individual's SSN, health-related and non-health-related information specific to the particular individual could be linked. More broadly, whatever personal identifier coding system is chosen for use in a computerized health record system, there exists the potential of using personal identifiers to link health care data with other individual-specific computerized data; such as military records, IRS records, banking records

and court records. Using SSNs will make such potential linkages easier.

In some situations, such as use of a credit card to pay a health care bill, linkage on a case-by-case basis may be unavoidable. In others, such as a provider using its patient records to target marketing mailings, linkage could arguably be beneficial to the patient. In potential epidemics, public health officials' use of such linkages could be vital.

However, closely restricting and monitoring such linkages could serve to relieve public fears about potential adverse uses of their health and financial information, such as being denied a mortgage, being denied child custody, or being discharged from the military.

Recommendation: The Privacy Board should consider ways of limiting data matches between health data and other types of individually-identifiable health care information. It should also consider restricting connections to communications networks carrying patient clinical information from electronic networks designed for other purposes (e.g., Internet, Prodigy, banking networks).

Recommendation: Studies of ways to protect confidentiality of individual identifiers should be conducted. This should include study of the possible establishment of a nationwide, uniform encryption system for individual identifiers.

ACCESS CONTROLS IN NETWORKS

The Work Group believes that before regional or nationwide electronic health care networks are established, the following question must be resolved: How will the architecture of the electronic health care system be designed to appropriately restrict access to information.

There are essentially three ways that patients could exercise control over who may access their health information. Various architectures of the electronic health care network (as discussed under the "Networks" section of this report) may make each of these options more or less feasible.

(a) The patient could authorize access to information only upon request, on a case-by-case basis.

(b) The patient could set up a generalized protocol, or list of instructions, for who may access what type of information from his or her records (within legal constraints). These instructions could bar or enable certain individuals' access to the records, or could constrain access based on an individual's or entities' role. For instance, the patient may permit all emergency department physicians to have access to all his or her health information in the case of an emergency. Or the patient may restrict all persons and providers except for his psychiatrist from having access to his mental health records.

(c) The patient could fill out a form each time he or she sees a new provider, or begins a new course of care, defining who may have access to his or her information from that encounter or series of encounters. This method is being tested by Dr. W.E. Hammond at Duke University's occupational medicine clinic."

Recommendation: The Work Group recommends that these and other options be tested as part of future demonstrations of electronic health care networks.

References

1. Workgroup for Electronic Data Interchange, Report to Secretary of U.S. Department of Health and Human Services, July 1992, Appendix 4, "Confidentiality and Antitrust Issues."

2. Deborah L. Hamilton, "Identification and Evaluation of the Security Requirements in Medical Applications," Proceedings of the Fifth Annual IEEE Symposium on Computer-Based Medical Systems, pp. 129-177, 1992.

3. Hamilton, ibid.

4. George T.C. Way, "Remarks on the Issue of Privacy and Confidentiality as it Would Pertain to the Contemplated Computerization of all Hospital Discharges in the State of New York," [get remainder of citation from J.K.]

5. Peter Waegemann, Medical Records Institute, presentation to the HHS Task Force on the Privacy of Private-Sector Health Records, October 29, 1992.

6. WEDI, ibid.

7. T.L. Lincoln and D. Essin, "The Computer-Based Patient Record: Issues of Organization, Security and Confidentiality," International Federation of Information Processing Working Group 11.3 on DataBase Security, West Virginia, Nov. 3-7, 1991.

8. Waegemann, ibid.

9. Richard S. Dick and Elaine B. Steen, eds., The Computer-Based Patient Record: An Essential Technology for Health Care, Institute of Medicine Committee on Improving the Patient Record, National Academy Press, 1991, pp. 156-179.

10. Council on Scientific Affairs, Feasibility of Assuring Confidentiality and Security of Computer-Based Patient Records. 1991.

11. National Conference of Commissioners on Uniform State Laws, Uniform Health-Care Information Act, with prefatory note and comments, 1985.

12. Agency for Health Care Policy and Research. Feasibility of Linking Research-Related Data Bases to Federal and Non-federal Medical Administrative Data Bases. Rockville, M.D. April 1991: Appendix 4-5.

13. WEDI, ibid.

14. D.W. Miller, "What We can Learn from the European Privacy Standard," Healthcare Informatics, July 1992, pp. 92-94.

15. WEDI, ibid.

16. WEDI, ibid.

17. W.H. Roach, "Access to Medical Records, Part 1: Who May Review a Patient's Medical Record, " Topics in Health Record Management, June 1981, pp. 33-52.

18. American Hospital Association, Management Advisory: Disclosure of Medical Record Information. Chicago, IL. 1990.

19. American Hospital Association, ibid.

20. American Medical Association. Policy Compendium.

21. American Medical Association. Edition of Current Opinions of the Council on Ethical and Judicial Affairs. 1992.

22. Joint Commission on Accreditation of Healthcare Organizations. Accreditation Manual for Hospitals. Joint Commission on Accreditation of Healthcare Organizations, 1993, Standard RI.1.1.8.1.

23. E.K. Huffman, Medical Record Management, Berwyn, IL, Physicians Record Company, 1990.

24. Dick and Steen, pg. 167.

25. Roach, ibid.

26. Gail R. Wilensky and James 0. Mason, "Memorandum to the Secretary of Health and Human Services re: Action Plan on Computerized Patient Records," 1992.

27. Lori B, Andrews and Ami S. Jaeger, "Confidentiality of Genetic Information in the Workplace, " American Journal of Law and Medicine, 17: l-2, pp 75- 108.

28. National Conference of Commissioners on Uniform State Laws, ibid, page 2.

29. According to the Centers for Disease Control, regulations to implement the Ryan White Act have not yet been published and its provisions not yet enforced.

30. David H. Flaherty, "Privacy, confidentiality and the use of Canadian health information for research and statistics," Canadian Public Administration, 35:1, pp.75-93

3 1. Personal communication, July 1992.

APPENDIXE

Provider Survey

Provider Survey
Purpose and Methodology

Overview

The purpose of this survey is to determine the current status and potential capability for implementation of computer-based patient record systems. The survey methodology is outlined below was developed by a subgroup of the Work Group on Computerization of Patient Records and should be critiqued by an expert in survey design. The survey instrument should undergo content validation through expert review and evaluation of internal consistence, format and ease-of-use through a pilot test. Once finalized, the instrument is intended for mailing to a representative sample of hospitals and other health care providers. From the responses, providers which are apparently closest to the goal of ,a computer-based patient record system will be identified. This group will be interviewed using the survey instrument to validate and further clarify the responses. The results will be tabulated and used to extrapolate the current status of computer-based patient record system implementation.

Survev Team

A survey team must be compiled. This team will be responsible for all aspects of the survey. At a minimum, the team would include a project director, analyst, and interviewer. It is expected that the team will also use consultants on survey design and methodology. The project director will report to a CPRI Board Liaison. The project director will be responsible for developing the proposal for funding of the survey, all operations relating to conducting the survey, and compiling the final report.

Content Validation

The survey instrument has undergone scrutiny by members of the subgroup, but has had little review by other experts in the field of conducting similar surveys or from potential respondents. The instrument should be critically evaluated by one or more individuals or organizations with special expertise in conducting surveys in the area of health care computing. The purpose of this review would be to evaluate content.

The content of the survey has been derived from the ASTM 1384 standard and is intended to capture information about the current status and potential capability for implementation of computer-based patient record systems (ref: IOM definition, CPRI vision). The content must convey a paradigm shift from traditional hospital information systems and the current paper-based medical record to a comprehensive, longitudinal system affording universal, timely, and intuitive access by caregivers and other authorized users to lifetime health data and other supporting knowledge.

The survey instrument has been designed to be universally applicable. Any care site should be able to respond without modification. As the primary input into development of the instrument has been from the hospital perspective, however, it must be reviewed by experts from any other provider who will be surveyed. The providers to be included and the size of the sample will be determined, in part, by the nature and level of funding. It is recommended that at a minimum a solo practitioner, group practice administrator, nursing home official, home health agency representative, and one or more specialty service professionals such as caseworker for mental health care, independent physical therapist, and others review the survey instrument for applicability to their practice site.

Format

The format must allow for easy, complete, and accurate recording of the desired information. It is currently designed as a check-off matrix with space for a small amount of explanatory information to be added at the end. Row headings describe health data rather than forms typically found in paper medical records or components of hospital information systems. Column headings either provide for a "yes/no" response in the cells or provide codes for recording structured responses in the cells.

Survey Procedure

The survey instrument assumes an integration of data which is unlikely to exist completely in any site. It is thus critical that a single focus not be applied to the response: Potentially, the individual to receive the survey may be a "coordinator" who can ensure that various key staff are exposed to the instrument and have input. The information systems planning or other such committee might be the most appropriate respondent.

A follow-up with the initial contact would be made following the interviews to assess the burden to the provider in completing the survey by both means.

Pilot Testing

To assess the feasibility and useability of the instrument and survey procedure, a pilot test should be conducted. This might take the form of both a mail survey and interview. A small (20 hospitals and 20 other care providers) sample of providers should be contacted for cooperation. The survey would be sent to those providers with instructions for completion and deadline. After that deadline, interviews would be conducted with key representatives without reference to the mailed response.

Interviews should be conducted with several different key members of the provider's staff, both to ensure complete and unbiased data capture as well as to determine the most appropriate type of individual to whom the survey instrument should be sent.

Responses to the pilot test should be compared for internal consistency. Evaluative comments should be noted. Problems identified as a result of the pilot test should be used to revise the format of the instrument, eliminate problematic items, and refme the methodology.

Mail Survey

Once the instrument is finalized it should be mailed to a representative sample of care providers in each category of care providers. This sample will be determined both statistically and in view of the level of funding. A post card will be enclosed with the survey that would be filled out by the recipient indicating who has been targeted as the person to contact for follow-up. There will be one follow-up letter sent followed by one follow-up phone call to enhance return rate.

Evaluation of Mail Survey

The mail survey will be analyzed to **provide overview results** and to screen **providers for interview** follow-up. The Survey Team may utilize consultants to evaluate the responses and identify candidates for interviews.

Results of the mail survey will be published as **preliminary** information.

Interviews

Candidates for interview will be contacted for more in depth probing of their **current** level of computerization. Using the results of the pilot test, it may be necessary to restructure the instrument for interviewing purposes. This would provide greater depth to the data collected.

Evaluation of Interviews

The data collected from the interviews will be published in aggregate form, and with permission from the providers, potentially serve as case studies for other publications.

Subseuuent Research

Successful **results may yield additional opportunities for research. These might include cost/benefit analyses, focus groups for defining functional specifications, and potentially even identification of demonstration sites.**

PROVIDER SURVEY
Global Questions

1. Do you use the patient's social security number as the medical record number? (Y/N)
   If no, what do you use?

2. Do you use the patient's social security number as the patient accounting number? (Y/N)
   If no, what do you use?

3. What do you use for the physician identification number?
   A. U-PIN
   B. Social Security Number
   C. Tax ID Number
   D. DEA
   E. State License
   F. AMA Education
   G. Other _____

4. How do you identify other caregivers (e.g., RN, therapist)

5. Do you have access levels to protect sensitive information? (Y/N)
   If yes, how many?

6. What are your information system plans for the next two years?
   A. Acquiring new applications
   B. Integrating existing applications
   C. Tailoring existing applications to better meet needs
   D. Upgrading current hardware
   E. Establishing remote links to physicians
   F. Establishing remote links to other provider organizations (e.g., clinics, community health centers)
   G. Other

7. What significant obstacles need to be overcome for you to meet your information system goals?
   A. Resource constraints
   B. Functionality of applications
   C. Use and acceptance of applications by caregivers
   D. Development of system-to-system linkages
   E. Other

8. What improvements in technology would you most like to see?
   A. Improvements in system-to-system linkages
   B. Improvements in functionality of applications
   C. Integrated voice/data technology
   D. Improvements in image (e.g., x-ray) storage and transmission
   E. Other

9. Are practitioners able to access hospital information systems from their offices?

10. Comments

	Automated Y = Yes N = No P = Partial (1)	Data entry N = Nurse P = Physician O = Other allied health prof. C = Clerical	Retrieval P = Paper v = Video	Decision support A = Alerts P = protocols/ diagnosis K = Knowledge systems C = Critical paths	Data Format N = Narrative c = Code V = Value I = Image	How is data archived? H = Hard Copy O = Optical Disk Image D = Digital	Can data be provided in ASCII? N = No If yes, how long (months)	Data available for recall at point of care? (Y/N)	Integrated w/ ADT system? N=No I=immediately upon entry F=following entry
NON-ENCOUNTER SPECIFIC									
Demographic									
Financial information									
Legal agreements									
Provider									
Immunizations									
Exposure to hazardous substances									
Cumulative patient history									
Problem list									
Physical exam and assessment									
Orders/treatment plan									
Diagnostic test results									
Medication profile									
ENCOUNTER SPECIFIC									
Registration/administrative									
Practitioner									
Chief complaint/characteristics of present illness									
Clinical course									
Therapies/procedures									
Disposition									

1. If application is partially automated, please explain degree of automation (e.g. scope of services covered, implementation in pilot stage, etc.)

2. Additional comments - please explain any special features, limitations, etc.

SURVEY DEFINITIONS

ROWS

Non-encounter specific - information which is accumulated as the result of serial encounters.

1. Demographic - personal data elements sufficient to identify the patient.

2. Financial information- information on all parties responsible for payment of patient health care services.

3. Legal agreements - legally binding directions or restraints on patient health care, release of information, and disposal of body or body parts.

4. Provider - identifying data on the primary organization or individual responsible for documentation of care.

5. Immunizations- record of immunizations.

6. Exposure to hazardous substances - data on exposure to all agents that might be associated with adverse health effects.

7. Cumulative patient history - synopsis of relevant medical (including allergies), dental, family, social, environmental, and other history which would aid practitioners in treating the patient.

8. Problem list - current status listing of clinically significant health status events and factors, resolved and unresolved.

9. Physical exam and assessment - record of any comprehensive patient exam (e.g., physical, mental, psycho social).

10. Orders/treatment plans - data entries that direct a patient's treatment including data on any practice protocols followed, delivery of orders, and compliance with any diagnostic or therapeutic orders or treatment plans.

11. Medication profile - significant details of all medications prescribed and/or administered in the course of an episode of care.

Encounter specific - information which is accumulated as the result of a single encounter.

12. Registration/administrative - data elements clarifying time/date, location, type, and source of encounter.

13. Practitioner - identifying data on the practitioner providing care during the encounter.

14. Chief complaint/characteristics of present illness - patient expression of need for services and practitioner assessment of patient status.

15. Clinical course - chronological picture and analysis of the clinical course of the patient during an episode of care. Clinical course may be described in narrative or data flow format. Clinical course includes that which is typically found in physician progress notes, nursing notes, consultation reports, nursing care plans, intensive care flow sheets, and other such documents.

16. Therapies/procedures - significant details on **the nature and outcome** of all preventive and/or therapeutic services and/or procedures for diagnostic or exploratory or treatment purposes performed during the encounter. Information may include that which is typically found in operative reports, treatment records, cardexes, etc.

18. Disposition - describes circumstances at the termination of the patient encounter, including length of encounter, condition of patient, recommended treatment or follow-up of care, patient education/instructions, and discharge planning.

COLUMNS

1. Automated data - data are automated if they are stored in retrievable electronic format. Automated storage includes on-line and archived data, as well as data which may be retrievable from other departments or organizations through electronic means without resorting to paper or other hard copy media.

2. Data entry - the data entry function includes not only keyboard entry, but also scanning bar codes and hard copy, etc.

3. Retrieval - Viewing information that is stored in the system

4. Decision support

a. Alerts notify care providers when patient data exceeds preset limits, when data interactions indicate potential or actual problems, when provider orders are not in compliance with preset guidelines, etc.

b. Protocols/diagnosis assist providers in analyzing assessment data, differentiating among possible diagnoses, and selecting appropriate plans and protocols for managing particular conditions.

c. Knowledge systems provide practitioners with information they need from scientific and clinical literature.

d. Critical paths specify the sequence and timing of various interventions for different clinical problems.

5. Data format

a. Narrative is a text string of words or words and numbers which do **not have** a defined structure.

b. A code is a predefined alpha, numeric, or alpha-numeric sequence which uniformly represents one or more narrative descriptors or numeric **value** ranges.

C. A value is a numeric description.

An image is a pictorial representation which may or may not include narrative, code and value information.

6. Archived data

a. Hard copy includes paper, microfiche, x-ray film, and other non-electronic formats.

b. Digital'data is represented by numbers and can include special characters and the space character.

7. ASCII (American National Standard Code for Information Exchange) is the standard code used for information interchange among data processing systems.

8. Data available for recall at point of care - refers to electronically retrievable information that can be obtained in less than 5 minutes.

9. Integrated with ADT (Admission-Discharge-Transfer) system - an interface exists between the system capturing the information and the ADT system.

GLOSSARY OF TERMS

GLOSSARY OF TERMS

Classification System. An arrangements of the elements of a subject into groups according to preestablished criteria. For example, in ICD-9-CM the diseases are arranged in chapters, sections, categories and subcategories for tabulating events or episodes of morbidity and mortality.

Clinical information system. An information system that collects, stores and/or transmits information that is used to support clinical applications (e.g., pharmacy, laboratory, radiology, nursing). Billing systems and other financial systems would not be considered clinical information systems.

Coding System. A structured set of characters used to represent data items (e.g., the codes 01, 02,...,12 may be used to represent the months January, February,..., December of the data element months of the year.

Computer-based Patient Record System. A computerized system that captures, stores, retrieves and transmits patient specific health care related data, including clinical, administrative and payment data.

Computer-based Patient Record. All of the data and images collected over the course of a patient's health history.

Data dictionary. A description of all of the data fields within an information system (e.g., name of patient, name of test, test result).

Data set. Defmed sets of information collected for a specific purpose. For example, the Uniform Bill is a data set of information collected for the purpose of claims processing.

Data Element. Discrete pieces of information (e.g., a patient's name, date of birth, or principle diagnosis).

Database. A collection of one or more data sets.

Health care informatics. A discipline that combines health care sciences and computer science.

Health information infrastructure. An interconnected communications network consisting of computer-based patient record systems, computerized knowledge based systems, and reference data bases all of which are connected through high speed communications links using common definitions, codes and forms.

Knowledge based system. A computer system that combines access to data and systematic use of logic rules and probabilistic statements that can help caregivers make better clinical decisions -- for example, recognize out-of-range lab values or dangerous trends, associate symptoms with the correct diagnosis, select the optimal treatment approach.

National information infrastructure. An interconected communications network consisting of computers and workstations, software applications and databases, and technical standards for linking users.

Nomenclature. A system or set of names (in this case, names for terms used in patient care).

Practitioner. Any individual that provides health care to patients, including physicians, nurses, and therapists.

Provider. All types of individual and organizations that provide patient care, including physicians, nurses, therapists, hospitals, health maintenance organizations, clinics, etc.

Reference database. Public and private databases containing aggregate data about many patients or cases that can be used for effectiveness research, financial analyses, and other purposes.

Structured text. Concepts and ideas that arc described in text but are assigned codes so that the they can be recognized and analyzed by a computer.

Valid Value. All of the possible data elements that could be assigned to particular category of information. For example, if the category is "month" the valid values would be January, February, **....,** December).