Computerized Patient Records:
Role-Based Information Security in a Federated Environment

by

Thomas Y. Lee

B.S., Symbolic Systems, A.B., Political Science
Stanford University, 1992

Submitted to the Department of
Electrical Engineering and Computer Science
and the Technology and Policy Program
in Partial Fulfillment of the Requirements for the Degree of

Master of Science
in Technology and Policy

at the
Massachusetts Institute of Technology

May 1994

Signature of Author .....
Department of Electrical Engineering and Computer Science
May 6, 1994

Certified by .....
Dr. Lee W. McKnight
Thesis Supervisor

Accepted by .....
Professor Richard de Neufville
Chairman, Technology and Policy Program

Accepted by .....
Professor Frederic R. Morgenthaler
Chairman, Committee on Graduate Students

Computerized Patient Records:
Role-Based Information Security in a Federated Environment

by

Thomas Y. Lee

Submitted to the Department of Electrical Engineering and Computer Science
and the Technology and Policy Program
on May 6, 1994
in Partial Fulfillment of the Requirements for the Degree of
Master of Science
in Technology and Policy

Abstract

This thesis reviews policies and technologies for computerized patient record security. The concept of a federation is presented as a model for automating medical records. Based upon this model, redisclosure, over-disclosure, inference and aggregation are identified as specific threats to the confidentiality of the computerized patient record (CPR) that arise from sharing data across a federation. From the threats, a set of security objectives emerges. Existing, proposed and pending legislation and guidelines that address the objectives are surveyed; traditional access control policies are reviewed.

This thesis concludes that the protection afforded by existing, proposed and pending efforts is incomplete. Each policy merely adds another layer to the inconsistent patchwork of regulations and tenets that already exists to support confidentiality. Traditional access control measures are also not well suited to the characteristics of patient records in a federated environment. Traditional measures assume the existence of a central authority for administering security and are either too permissive or too inflexible.

Role-based access control is introduced as a better alternative for supporting disclosure and inference related threats to the confidentiality of the computerized patient record. The recommendations are intentionally phrased to facilitate role-based access controls as a logical mechanism to support policy implementation.

Elements of a security policy that rely upon role-based access control to address patient record confidentiality are presented as a series of recommendations. Separate recommendations are drafted for the Federal government, the states and individual institutions such as hospitals, payers and social services agencies which wish to share the data in the computerized patient record.

Thesis Supervisor: Dr. Lee W. McKnight
Title: Lecturer,
Technology and Policy Program

Acknowledgments

I would first like to thank my thesis supervisor, Dr. Lee McKnight, for all of his guidance, insight, and support. Dr. McKnight served not only as a thesis advisor but also as an academic advisor and career counselor. I am particularly grateful to him for permitting me to pursue a topic of my own choosing.

I would also like to thank the numerous members of academia, industry and government who generously offered their valuable time to provide comments, insight and pointers to useful sources: Dennis Branstad, David Clark, Randy Davis, Stephen Downs, John Fanning, Kathleen Frawley, Elmer Gabrieli, Rich Graubart, Gary Gray, Amar Gupta, Linda Harris, Cathy McCollum, Maria Meredith, Silvio Micali, Robert Moore, Mark Musen, Rick Peters, Karen Randall, Jerry Saltzer, Peter Szolovits, Beth Watson, and Katie Weeks. They deserve much of the credit for this thesis. However, any errors or inanities are, of course, the author's alone.

The Center for Technology, Policy and Industrial Development (CTPID) and the administrative and research staff of the Research Program on Communications Policy (RPCP) also deserve credit. CTPID provided research facilities. David Carver, Suzanne Neil and Richard Solomon supported my research from the beginning. Julia Malik and Gill Cable-Murphy tolerated my frequent, random forays through their office searching for reference materials while talking to myself.

My graduate student colleagues of RPCP: Joe Bailey, Paul Bosco, Sharon Gillett and Russell Rothstein are also deserving of thanks. They read drafts and counseled me in times of crisis. After I covered my own desk with books and rendered it completely useless as a workspace, they tolerated my encroachment onto their desktops and shelves as I searched for room to work. Joe Bailey, in particular, spent many hours just listening to me work through ideas in my own mind.

Fellow TPPers also played a large part in the completion of this thesis. Kara Callahan, Alex Hou, Chrissy Houlahan, Renata Pomponi and Todd Stout were a constant source of encouragement. Russ Cohn accompanied me on many a late night as he worked to complete his own thesis.

Special thanks go to my parents and my siblings Nancy and Terry for their support and encouragement. I would especially like to thank Nancy for going above and beyond the call by making the trek from New Jersey to help edit . My roommate, Papa Rao, also has my gratitude for tolerating my mess and the many sleepless hours which I cost him with my early morning risings and my late night returns from working on this thesis.

Special thank also go to the Hung family of the Chinese Bible Church of Greater Boston (CBCGB). Mr. and Mrs. Hung were largely responsible for making my MIT experience a bit more like home. Fellowship through CBCGB was a constant source of strength and a reminder that it is ultimately through God's grace and love that, among other things, I completed this thesis.

Finally, I would like to thank Dr. David Gaba of the Palo Alto Veteran's Administration medical Center and the Stanford University School of Medicine. Dr. Gaba introduced me to academic research, to medical computing and gave me my first opportunity to publish and present research at a major academic conference. His initial trust in a random, freshman undergraduate student has helped bring me to where I am today.

Table of Contents

List of Figures

List of Tables

Introduction

In the movie *The Fugitive* (© 1993. Warner Bros.), Dr. Richard Kimball, falsely convicted of murdering his wife, begins his search for the elusive one-armed man by posing as a custodian in Chicago's Cook County Hospital. While cleaning after-hours in the Department of Prosthetics, Dr. Kimball logs into the patient database and uses the physical characteristics of the prosthetic to trace the one-armed man's identity and whereabouts. Were the current Administration's vision of a National Information Infrastructure in place today, Dr. Kimball might have been able to access the same patient information without ever having entered the hospital.

For the health care system, a computerized patient record (CPR) that enables the electronic storage and retrieval of patient information, whether at home or in a medical center, offers tremendous promise for both decreasing the cost and increasing the quality of care. A recent study by Arthur D. Little estimates health care cost savings from electronic record keeping and electronic claims submissions may reach nearly $40 billion per year. [ADL92] Simultaneously, quality of care should improve due, at least in part, to increased availability of records and outcomes-based research using cross-matching of longitudinal patient records. [IOM91]

Even as information technologies promise to streamline the delivery of health care, however, they introduce new threats to the security of sensitive, confidential information about individuals contained in the medical record. While the audience may sympathize with Dr. Kimball and applaud his cleverness in using the hospital information system to trace the one-armed man, the movie also illustrates one of the vulnerabilities of electronic record-keeping. An unidentified individual, with no legitimate affiliation to the Cook County Hospital medical staff, accessed patient files and executed complex search and cross-matching queries to reveal potentially confidential, sensitive information. Sound like fiction? In 1987, on the trail of an international, computer espionage ring, Clifford Stoll tracked West German computer hackers into the Positron-Emission Tomography (PET) control computer at Lawrence Berkeley Laboratories. The computer is used to calculate radiation doses infused into patients as part of the PET imaging process. [STO89] It is frightening to think of what a malicious intruder might have been able to accomplish.

Whether or not computerized patient records (CPRs) are an effective means for addressing the nation's health care ills is beyond the scope of this thesis. This thesis explores technologies and policies to minimize threats introduced by the use of computer and communications technologies to the security of sensitive information contained in the medical record.[1] The thesis assumes that the CPR is implemented as a federation. One possible solution is proposed to the vulnerabilities posed by utilizing a federated electronic infrastructure to share sensitive information between one or more of the institutional players in the health care community. For this thesis, sensitive information is defined as any data which directly or, within reason, could indirectly identify a specific individual. The health care community is defined here to include patients, providers, payers, employers and supporting organizations.

---

[1] The issue of whether or not computerized patient records are an effective means for addressing the nation's health care ills is beyond the scope of this thesis. For information on recent legislation to mandate the use of computerized patient records, see BRO93 and IOM92.

Chapter 1 introduces a framework for discussing information security. Some of these security concerns are a reality of the electronic environment and exist regardless of what type of data is stored. Other vulnerabilities are inherent to medical recordkeeping. Vulnerabilities inherent to medical recordkeeping may be unaffected, mitigated, or exacerbated by the shift from paper to electronic media.

Chapter 2 presents the problem being addressed by asking, "What are the vulnerabilities?" The chapter begins by describing a federation; this thesis assumes that the CPR is implemented as a federation. Threats to and vulnerabilities of computer patient records that arise when institutions share potentially sensitive, confidential information in a federated environment are identified as security objectives to be satisfied.[2]

Chapter 3 considers the elements a policy should contain in order to address the concerns raised in Chapter 2. Proposed, pending and existing legislation at the institutional, state and federal levels are compared and contrasted.

Chapter 4 introduces role-based access control as a potential technology for supporting a security policy to meet the objectives from Chapter 2. The chapter begins by examining traditional discretionary and mandatory access control. Role-based access control is then presented as an alternative better suited to the patient record environment.

Chapter 5 combines the policies from Chapter 3 and the technologies from Chapter 4 into a series of recommendations for action by the Federal government, the states and individual institutions.

---

[2]The threats posed by sharing information in electronic rather than paper-based formats are distinct from the task of transferring electronic bits between institutions. Analysis of technical approaches for reliable, secure communication, while also a highly relevant subject for investigation, is beyond the scope of this thesis. As a starting point for finding more information on this subject, see OTA87, NRC91 and FOR94.

Chapter One

Information Security

This chapter introduces a framework for assessing information security for computerized patient records. After reviewing the issues encompassed by information security studies, the chapter constructs the framework and identifies how this thesis fits within the framework.

The notion of keeping secret information hidden away from prying eyes is not new.[3] [KAH67] Whether for reasons of national security or for personal privacy, information security stems from the desire to safeguard information. However, information security encompasses more than just keeping secrets. The evolution of both the types of information that society seeks to secure and the technologies by which that information is shared and stored has expanded the scope of information security studies. Today, the field of information security studies focuses on three fundamental issues: what are the objectives of information security, how is information security achieved, and how is the security of information verified?

Before addressing objectives, mechanisms and verification, however, it may be useful to begin by clarifying what information security is not. Although it has adapted to changes over time, the concept of information security should not be thought of as

[3] In *The Codebreakers*, David Kahn dates the first use of cryptograhically encoded information to the Third Century B.C.

relevant to only a single type of information or a single technology. In the past, the Department of Defense (DOD) has been the primary sponsor of and motivator for information security research. Subsequently, a common misconception equated information security with the Department of Defense's activities to uphold national security. As a result, the financial community thought that their needs, such as securing a financial transaction, had little to gain from DOD sponsored research. [CLA93] In fact, whether the motivation is investment banking or defense maneuvers, many of the underlying information security policies and procedures are the same.

Likewise, society is becoming increasingly dependent on "electronic ways to gather, store, manipulate, retrieve, transmit and use information." [OTA87:13] Consequently, the tendency is to associate information security with the security of a computer system. However, as discussed below, many of the concerns regarding the security of information are not at all unique to the electronic environment. Even within an information system, "security is only partly a technical problem: it has significant procedural, administrative, physical facility and personnel components as well." [NRC91:17] There is a danger that those new to the field of information security will lose sight of the forest, focusing only on a particular technology applied to a particular domain.

1.1 W hat are the objectives

Information security can be defined in terms of an institution's need for some combination of confidentiality, integrity and availability. [NRC91] Confidentiality involves controls on the disclosure of information. It is a security property that prevents either the existence or the content of information from being known by some population. [ECM88] One of the better known confidentiality policies is the DOD's hierarchical information classification scheme. An individual has a security clearance and information has a security classification that ranges from top-secret to unclassified.

Security clearance represents a formal authorization to access information that falls within a specified set of classifications. [DOD85]

Integrity refers to the quality of information and ensures that "[information] is changed only in a specified and authorized manner." [NRC91:293] As an example, integrity ensures that information received accurately reflects that which was sent. The accounting practice that does not permit erasure of an entry to correct an error supports integrity constraints. Instead, accountants must make a corrective entry on a new line. [CLA87].

Availability, the third information security parameter, ensures that information is usable within a given time frame. [NRC91] Availability has two elements. First, information must be accessible to an authorized user. Second, the information, once retrieved, must be in an interpretable format. Within the patient-physician relationship, availability means first, that the record is readily available to all health care personnel with a need to know in order to administer care. Second, that record should be in a standard format and use terminology familiar to the medical profession. A simple availability policy is to keep multiple copies of a valuable record and to store one copy in a physically secure place. [BRS94]

Although confidentiality, integrity and availability do not trade off against one another, neither are they completely unrelated. The differences in information security needs between a given pair of institutions are reflected in the balance of the three information security parameters. For example, both the financial industry and the defense community are concerned about integrity and the unauthorized disclosure of information. However, the financial industry places a higher premium on the need for information integrity relative to confidentiality than does the defense community. [CLA87] Ensuring that debits and credits are tallied in proper sequence is crucial in the business environment. Conversely, in the military, ensuring that information is not revealed to unauthorized personnel is critical.

1.2 How is information security achieved

The means for fulfilling information security objectives may be divided into physical, procedural and automated measures. [ECM88; NCS92] As noted earlier, concern for the confidentiality, integrity and availability of information existed long before the development of computer technologies. [OTA87] Likewise, although automated information security controls are a new development, many of the physical and procedural measures for achieving information security are unchanged by the migration to electronic media.

Physical measures refer to the environment in which the information is stored. Posting guards to check the identification of people entering and exiting a security area restricts access. Storing sensitive information in a fireproof cabinet ensures against loss to some natural disasters. Newer physical measures that derive directly from the use of automated information systems include biometric devices that check identities based upon fingerprints, speech patterns or blood vessel patterns in the retina. Back-up generators secure against power system failure.

Procedural mechanisms, which include both personnel and operating procedures, are crucial because "[m]ore security breaches are caused by human error, often by well intended people, than by other causes." [CEC93:22] One procedural mechanism that is common to many industries is the practice of separation of duty. Separation of duty ensures that no single individual has sole authority to execute a critical task. For example, separation of duty decreases the opportunity for fraud by prohibiting the person who places an order from also authorizing payment and receiving delivery. Other procedural mechanisms include the accounting practice prohibiting erasures or the DOD's hierarchical security classification system.

Automated controls, also referred to as logical controls, are a new class of considerations for satisfying security objectives that stem directly from the use of

information technologies; but logical controls involve more than simply automating procedural mechanisms. Support for distributed processing and electronic communications via wireless and wireline networks are also a part of automated controls. Common automated control measures include encryption and access controls.

Just as security objectives are a combination of confidentiality, integrity and availability, implementations are therefore a combination of physical, procedural and automated mechanisms. Especially with information technologies, the tendency is to focus on automated controls. However, an organization's information security needs prescribe a system which "is an interdependent collection of components ... that involves physical elements and people as well as computers and software." [NRC91:65]

1.3 How is information security verified

Unfortunately, establishing security objectives and enacting procedures and mechanisms to implement those objectives is not enough. "Inadequacies in a system can result either from a failure to understand requirements or from flaws in their implementation." [NCS92:9] Verification is the process of evaluating what degree of security is actually achieved by the security measures implemented within an organization. Verification takes place at three different stages: security policy, security model and implementation.

A security policy is an "informal specification of the rules by which people are given access to a system to read and change information and to use resources." [NRC91:77] It identifies the combination of confidentiality, integrity and availability that is appropriate for a particular organization's goals. Ultimately, the security mechanisms are implemented to satisfy these specifications. Consequently, it is important to verify that the policy accurately reflects the information security needs and desires of the organization.

To relate system behavior to security objectives, the policy is re-stated as a model using formal mathematical constructs. A good model supports verification in three ways. First, it is possible to mathematically evaluate whether there are any logical fallacies in the policy. Second, the model guides the selection and implementation of mechanisms to minimize the potential for inconsistencies between security requirements and system design. Third, as the need for security changes over time, the model identifies how the system should adjust. "A good model accurately represents the security policy that is actually enforced by the system. Thus, it clarifies both the strengths and the potential limitations of the policy." [NCS92:10]

Regardless of how rigorous the theoretical analysis of security policy is, however, satisfying information security objectives is ultimately dependent upon implementation. The final stage of verification asks whether the mechanisms accurately implement the policy. The implementation should restrict access and behavior as specified by confidentiality and integrity constraints. Equally important is availability. The system should not be more constraining than the policy requires.

Therefore, for an organization to be assured of achieving any degree of information security requires proof that the security policy matches the organization's needs and desires. Also, the security model used to guide the implementation must correspond with the security policy, and the implementation itself must verifiably enforce the model.

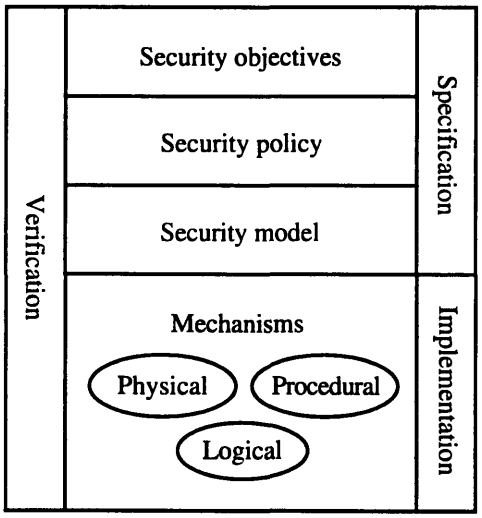
Underlying the entire verification process is the understanding that information security is inherently an uncertain activity. Thus, at every stage, a critical component of verification is risk analysis. The degree to which a security policy matches the organization's needs and desires or that an implementation verifiably enforces the model is not absolute. Information is only as secure as the weakest link in the system that is processing it, and no matter how reliable the security measures, ultimately, the system must rely upon people. History demonstrates that even the most reliable, well-

intentioned users can err. [KAH67] Verification is the process of determining with what degree of assurance – how reliably – an organization protects information.

1.4 A framework for information security studies

A complete study of information security therefore addresses both specification and implementation issues. Specifications vary in degree of detail on a continuum from a general list of objectives to a formal security model. In its formative stages, a security specification should define the balance of confidentiality, integrity and availability appropriate to an organization's needs. As a specification evolves towards greater detail, each successive specification document should be rigorously analyzed to ensure that the intent of the security objectives is accurately captured.

Figure 1.1
A framework for information security studies



Implementations relate a security specification to specific security mechanisms. Because of its precision, the security model provides guidance in selecting appropriate physical, procedural and logical mechanisms as well as providing a means for verifying

that the mechanisms correctly implement the security model. Correctness entails both restricting undesirable behavior as well as enabling actions that are permitted without unintentionally permitting unintended actions.

1.5 Focus of this thesis

This thesis will explore selected information security specification and implementation considerations as they pertain to institutions sharing information contained in a computer-based patient record. In particular, this thesis will explore security policy and the procedural and logical mechanisms to support confidentiality requirements of computer-based patient records.

To address confidentiality, the different players who seek access to sensitive, patient-identifiable medical information are first identified. More than a decade ago, researchers were already documenting the growing demand for personal medical data, not only to enhance the delivery of care, but also to support quality assurance and accreditation practices as well as to fulfill public policy and social objectives. [WES76; BRC84] However, access should be tempered by the purposes for which the information is necessary. Neither will all individuals and institutions need access to the entire record nor will they all need the ability to write in the record or to copy and re-distribute portions of the record.

The technology and policy of resolving security concerns encompasses logical, procedural and physical mechanisms. This thesis focuses on the implementation of logical mechanisms to support the security of computerized patient records. At the same time, it recognizes that physical and procedural measures play an equally important role in ensuring the security of computerized, sensitive patient information.

Because of the breadth of information security studies, many issues, while no less relevant or critical, are not addressed in this thesis. In addition to physical and procedural mechanisms, availability and communications are two such issues. Availability requires

that timely, accurate information be readily available to all individuals with a legitimate need to know. This concern raises issues such as replication, concurrency control, reliability and fault tolerant computing. Communications security, protecting information while in transit between institutions or players is another subject beyond the scope of this thesis. Encryption technologies for electronic communications or the use of smart cards to enable patients to transport personal medical information are currently a subject of great study.[4]

[4] As referenced in footnote 2, for further information on technologies for secure communications, see OTA87, NRC91 and FRD94. For further information on smart card technology, see OTA93 and ALP93.

Chapter Two

The Computerized Patient Record

This chapter uses the framework introduced in Chapter 1 to identify security risks posed by sharing sensitive, electronic medical records within and between institutions.

There is an increasing demand for access to individually-identifiable information in the patient health record. The burgeoning list includes health professionals who provide care, administrators and accrediting organizations that monitor the quality of care, managers who make financial decisions and third party payers that determine reimbursement. [BRC84; WES76; OTA93]

The need and ability to electronically share information among the myriad parties who desire or require access raises many security issues.[5] Many of these problems are inherent risks of electronic record-keeping and have little to do with content. Other vulnerabilities may be unique to medical records and are unaffected, mitigated, or exacerbated by the shift from paper to electronic media.

As background, the chapter begins by introducing the concept of a federated environment. Next, the chapter defines the paper-based *patient record* and relates that record to the concept of a federation. Security risks that arise from both inter- and intra-institutional use of the paper record are identified. This chapter then considers the

[5]Unless otherwise specified, future references to 'information security' imply confidentiality concerns that arise from sharing information among multiple parties.

implementation of the computerized patient record (CPR) as a federation to explore security issues that arise from the migration to information systems. "However, merely automating the form, content and procedures of current patient records will perpetuate their deficiencies and will be insufficient to meet emerging user needs." [IOM91:2] Therefore, the chapter concludes by reviewing proposals for an expanded patient record. New and changing risks are noted. Security objectives are identified.

2.1 What is a federated environment

A database system consists of automated information management software called a database management system, and a structured collection of information called a database. [HEM85:256; SHE90:183] A *federated database system* (also referred to as a *federated system*) is "a collection of cooperating but autonomous component database systems." [SHE90:183] A *federated environment* (also referred to as a *federation)* includes both a federated database system and the community of users that access the information within the constituent databases that comprise the federated system.

The centerpiece of a federation is the federated database system. Although the research literature varies quite widely in its interpretation of a federated system, at least three key concepts are generally shared by most researchers in the field: distribution, heterogeneity, and autonomy.

In a federated environment, information is drawn from many different user populations, each of which may have its own database system. As a consequence, data resources may be distributed physically or logically. Data that is distributed physically is divided among multiple computer systems that are either "co-located or geographically distributed but interconnected by a communication system." [SHE90:185] Data this is logically divided is stored and managed on a single computer system. For example, this thesis is bound as a single volume but is logically divided into chapters.

A second characteristic of federations is the heterogeneity between the constituent database systems. Both syntactic and semantic differences might exist. Syntactic heterogeneities include differences in data representation and in query language. [SHE90] With respect to data representation, some database systems might employ an object-oriented model while others use a relational model. Furthermore, the query language used to access information within the database may differ.

Even if two database systems are syntactically identical, they may still differ semantically. "Semantic heterogeneity occurs when there is a disagreement about the meaning, interpretation, or intended use of the same or related data." [SHE90:187] Does the data item "cost" include tax? Does the data item "name" list last name first and first name last or vice versa? What about the middle initial?

Heterogeneity within a federation may also stem from differences in the software and hardware infrastructure that supports the constituent database systems. At the operating system level, file systems, naming conventions, transaction support, and interprocess communication may be implemented in different ways. Inconsistent hardware may also complicate data sharing. [SHE90]

Autonomy is perhaps the defining characteristic of a federated system. That members of a federated system may elect to use incompatible syntactic structures or inconsistent semantic conventions is only one facet of autonomy within a federation. Autonomy also includes control of data sharing and control of data viewing. [HEM85]

Autonomy over data sharing ensures that each system participating in the federation determines how much information it chooses to share with other members of the federation. Negotiation is the process whereby two or more constituents within the federation determine what data is shared and agree on the terms and conditions under which that data is shared.[6]

---

[6]The 'terms and conditions' refer to such issues as how long the recipient may continue to share the information, access controls on the information, and the sender's obligations regarding updating information to ensure that the recipient has current data.

Data viewing includes the right of each constituent to receive the shared data in a consistent format. Because of the different semantic and syntactic heterogeneities, information shared with and received from a foreign database system should be translated into the recipient system's native format to provide transparency to users.

In the current information landscape, "databases have proliferated across a variety of networks, each under the control of a different organization, and with very little standardization among them." [ALO91:305] *Federations* are a response to the increasing economic and political pressure for institutions to share information and interoperate between "the plethora of legacy systems which were designed independently" and the "newer object-oriented and relational systems." [MOR92:131]

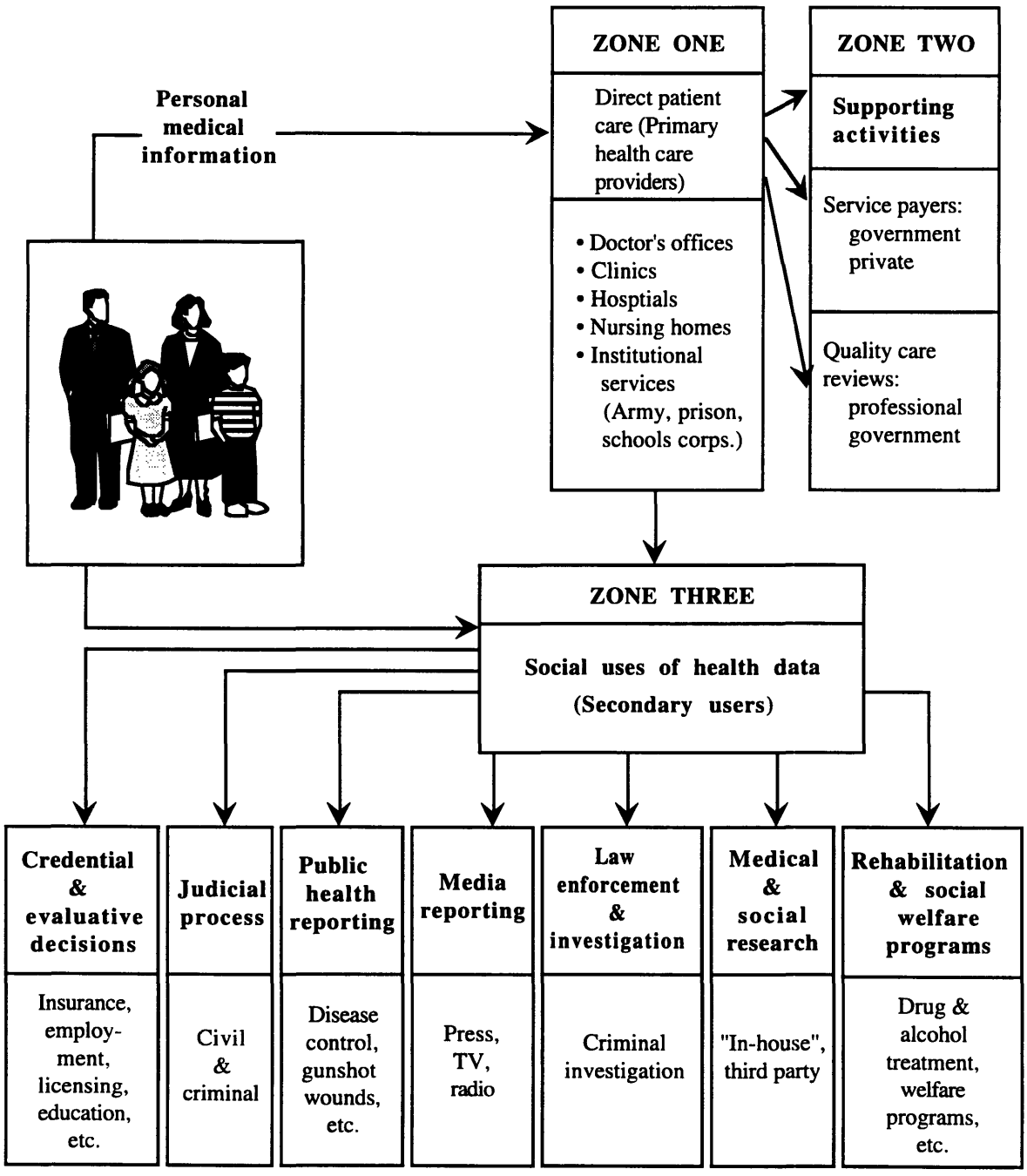
2.2 What is the patient health record

Traditionally, the individually-identifiable portions of the health record comprise the document which is "used by health professionals while providing patient care services to review patient data or document their own observations, actions, or instructions." [IOM91:11] Even before the introduction of information technologies, however, the health record had begun to evolve into much more. "How much more" can be operationally defined in terms of the confidentiality and integrity requirements of the health record: who wants access to the health record and why?

Users, defined as individual or institutional players who wish to access patient-identifiable portions of the record, are often divided into two or more different categories depending upon their intended use of the information. The Department of Health and Human Services suggests four classes of users. [GOS93] Westin, in his report to the National Bureau of Standards (now the National Institute of Standards and Technology) defines three. [WES76] The Institute of Medicine [IOM91; IOM94] and the Office of Technology Assessment [OTA93] each describe their own taxonomy. Regardless, all

agree on there being a distinction between use of the patient record while in the course of providing patient care and use for any other reason.

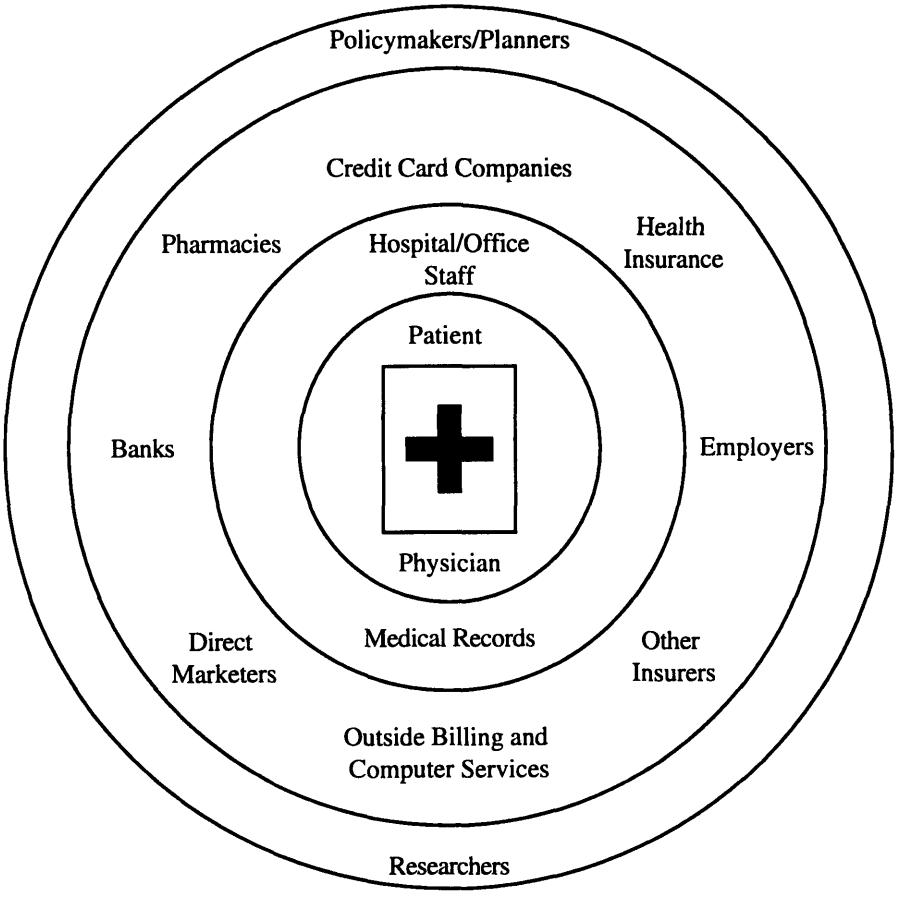
Figure 2.1
Classification of health record users into zones



Source: WES76:10

Primary users of the health record are those who access the patient record while in the course of providing patient care. To the primary care physician, then, the record registers "important medical benchmarks ... history and physical examination, a list of the patient's problems, diagnostic tests and procedures performed, the results of these tests, [and] monitoring done." [LIN92:4] For hospitalized patients, it is also a working document that records unverified concerns about possible conditions and coordinates "the

Figure 2.2
Classification of health record users into spheres



Source: GOS93 citing the U.S. Department of Health and Human Services Task Force on Privacy

tactics of everyday care: nursing care plans, input-output records ... and notes that coordinate one nursing shift to the next." [LIN92:4]

But providing patient care involves more than just physicians and nurses. Laboratory technicians, medical specialists, social workers, and pharmacists all participate in the delivery of care and their notes also contribute to the record. Support staff often maintain files independent of the document stored in the medical records department. Because departmental records often contain information unavailable in the central, paper file, the complete patient record is a compilation of many separate documents:

> [S]ocial service departmental files might contain information describing a patient's habits, finances, family crises, or other sensitive personal facts. Other ancillary service departmental files might similarly contain sensitive or technical information not housed in the primary health record. [IOM91:13]

"Information kept in one such file may also be of relevance in another, so that the patient's hospital record becomes several different files that may overlap and are often maintained in separate places." [OTA93:45] Moreover, because of the population's increasing age and mobility, the complete document may consist of records from laboratories, clinics, and hospitals throughout the country. Table 2.1 provides a more extensive list of primary users who access the record in the course of providing direct patient care.

Table 2.1a
Institutions who are primary users

Community clinics (includes public schools)	External laboratories	Nursing homes
Community Health Information Networks (CHINs)	Health Maintenance Organizations (HMOs)	Outpatient surgery
Correctional facilities	Home health care agencies	Pharmacies
Donor banks	Hospices	Private practitioners
Emergent care clinics	Hospitals	Psychiatric facilities
	Military services	Specialty care clinics
		Substance abuse programs

Sources: CHM92, HHS93b, IOM91, WED92 and WES76

Table 2.1b
Primary users within the primary use institutions

Assistant	Dentist	Pharmacist	Therapist
Clinical	Dietitian	Physician	Occupational
Nurse	Nurse	Social worker	Physical
Physician	Optometrist	Technician	Radiation
Chaplain	Patient	Laboratory	Respiratory
Dental hygienist	Patient's family	Radiology	

Sources: IOM91 and WES76

Secondary users, then, include all those other players who seek access to the patient record. To a current reader, the most familiar of these might be the third-party payer or medical insurer. "Patient data now are used for coverage decisions (e.g., preadmission review) as well as for payment" [IOM91:22] "The patient accounts department is responsible for obtaining patient-identifiable information, such as diagnostic and therapeutic items needed to determine benefits entitlement and to process payment claims for services provided." [BRC84:47]

As with primary users, the ranks of secondary users and list of uses is very diverse. Within the medical establishment itself, the uses of individual patient records for purposes other than that individual's care has been growing. "To develop budgets, measure productivity and costs and assess market position, managers of institutions seek to link financial and patient care information." [OTA93:31] "Quality assurance activities such as utilization review, infection control, health record review, risk management and drug surveillance are some examples of functional responsibilities for which record access is legitimate." [BRC84:34] "Such activities are a requirement for accreditation of hospitals by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO)." [IOM91:21] Table 2.2 provides a more extensive list of secondary users and their respective uses of the record.

Table 2.2a
Secondary uses of information

Accreditation/care management
Quality assurance - assess compliance with standards of care, compare health care institutions
Risk management - identify at-risk populations
Utilization review - perform outcomes and cost effectiveness research professional accreditation

Education
Continuing education for current professionals
Dental
Medical
Nursing
Public health

Evaluative decisions
Employment
Insurers - non-medical (e.g., life, automobile, fire, etc.)
Licensing
Social services

Information systems support
Maintenance
Upgrades

Legal
Investigations
Proceedings against a drug or equipment manufacturer (e.g., failure to warn, negligence, etc.)

Legal (cont'd)
Proceedings involving the patient (e.g., court ordered psychiatric evaluation, personal disputes, etc.)
Proceedings against the provider (e.g., malpractice)

Patient health care support
For the patient
For the patient's family

Public policy interest
Disease reporting (e.g., Center for Disease Control)
Social services (e.g., Aid to Families with Dependent Children, etc.)
Social welfare (e.g., births, deaths, etc.)
Violent crimes (e.g., suspected child abuse, knife and gunshot wounds, etc.)

Reimbursement
Federal
Private
State

Research
Public policy
Medical research
clinical trials
new products
Technology development
assess new technologies
marketing strategies

Sources: CHM92, HHS93b, IOM91, WED92 and WES76

Therefore, the complete patient health record is really a composite document. The patient-identifiable information that comprises the complete health record is either contained or duplicated in the files of numerous hospital departments, clinics, ancillary health care support institutions, accreditation organizations, government regulatory agencies and social service offices. Although the primary reason for maintaining patient

information remains the delivery of health care, the number and variety of secondary uses equals or exceeds the number and variety of institutions that store the information.

Table 2.2b
Secondary users corresponding to the secondary uses

Accreditation/care management
Accreditation organizations (e.g., Joint Commission on Accreditation of Healthcare Organizations)
Consultants
Professional organizations (e.g., American Medical Association)
Third party administrators

Education
Faculty
Health science journalists
Students

Evaluative decisions
Employers
Government agencies
Insurers - non-medical (e.g., life, automobile, fire, etc.)
Professional organizations

Information systems support
Developers
Staff
Technicians

Legal
Judges
Law enforcement authorities
Lawyers

Patient health care support
Support groups

Public policy interest
Media
Law enforcement authorities
Local, state and Federal officials

Reimbursement
Claims evaluators

Research, public policy
Alcohol, drug abuse and mental health administration
Center for Disease Control
Death registry
Food and Drug Administration
National Center for Health Statistics

Research, medical
Academic institutions
National Institute of Health
National Library of Medicine

Research, technology
Academic institutions
Equipment vendors
Pharmaceutical industry

Sources: CHM92, HHS93b, IOM91, WED92 and WES76

2.3 Confidentiality and integrity of the health record

Historically, the health care community has largely depended on the "'small village' property of the visible workplace. It is assumed that the staff that come together on a nursing floor know each other and are observant. ... Much has depended on trust." [LIN92:13] In an environment that shares information within and between institutions,

assumptions of trust can break down. The increasing demand for personal medical data, whether the information is represented in electronic format or not, raises many challenges to maintaining the confidentiality and integrity of the record.

Confidentiality concerns, which include redisclosure and over disclosure, are particularly vulnerable to the breakdown of trust. When information is shared between two parties, redisclosure is the unauthorized release of the shared data, whether accidental or intentional, by the recipient to some other user. [WED92; BRC84] "Ultimately, the use or abuse of a system is a function of the human beings who operate it," and human error is a leading cause of security breaches. [BRC84:106; CEC93] Moreover, third-party recipients may not be subject to the same legal or ethical constraints.[7] Redisclosure underlies the common strategy of seeking secondary sources if initially thwarted.

Over disclosure is a second hazard of information sharing. "With existing paper systems, requests for information often result in the release of data that are not pertinent to the current request, as total documents are photocopied and/or faxed to users. [GOS93:2491] Many users with a legitimate need to access specific portions of the record have neither the need nor the authority to access the complete record. Medical researchers are often prohibited from viewing information that would reveal the identity of a human subject. At the extreme, mental health records are a subset of the complete patient file that are restricted, even under subpoena, to all but a few users. [TIN90] While delivering the complete medical record rather than selected notes may not appear to pose much of a risk, the nature of the threat is clarified when considered in conjunction with the potential for redisclosure. Sharing only as much information as is necessary can limit subsequent harm.

The motivation to constrain disclosure is not absolute, however. A policy restricting access must be tempered by the reality that "even unauthorized personnel

[7]The issue of ethical and legal constraints is expanded upon in Chapter 3.

might need to have access to patient records under emergency situations." [HAM92a:13] Patient safety must always have priority over confidentiality.[8]

Threats to integrity due to information sharing are also related to trust. When preparing reports and forms, there is always the danger of making inadvertent errors. Information sharing exacerbates the risk because there is no guarantee that users in different institutions will conform to similar standards of behavior. Departments or institutions may write or update the record in unauthorized or inconsistent ways. Record entries may vary from a scattered collection of free form notes documenting a patient's status to a regimented list of diagnostic tests and results. For still others, the record may serve more for "correspondence and reports rather than as a well organized chronology of health care." [IOM91:19]

The danger of data corruption is tempered by regulations that mandate that, depending upon the state, the source institution must preserve the original record for a specified number of years or until the patient reaches their majority, whichever is longer. [ALP93] Additionally, the medical establishment has adopted the financial industries convention against erasure or overwriting. [BRC84] Consequently, if a patient returns from a hospital stay to her home clinic, at the very worst, only that documentation specific to the hospital stay would be inconsistent.

2.4 Automation of the patient record

To recognize the information security implications of sharing information in an electronic rather than a paper environment, it is helpful to first understand what automation entails. Consider the users and their respective uses of the record. The effect of automation on users and their respective uses noted earlier is experienced in changes to the record's form and content as well as the procedures by which the information is handled. Automation also introduces a new collection of users and uses.

[8]Note that medical emergencies as an exception to medical confidentiality is in direct contrast to the mandatory access control policy implemented by the Department of Defense which explicitly excludes exceptions to disclosure rules.

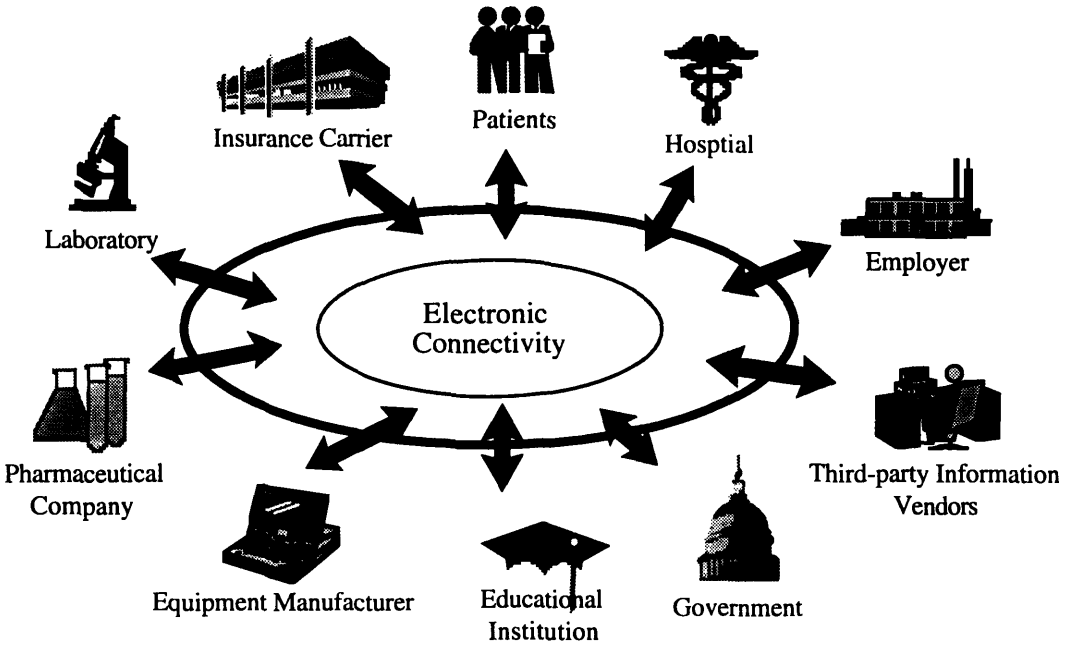
Changes to the form of the electronic record are exemplified by the presentation format. The flexibility of automated systems permits individual users to arrange and display information in the manner most suited to their needs rather than being bound to a generic, paper form. [IOM93; IOM94] Content, while largely unaffected in substance, more accurately reflects the longitudinal, composite nature of the document. As an individual patient ages, portions of the record become scattered throughout different clinics, medical specialists and private physicians' offices. Electronic communication networks permit multiple users to simultaneously, transparently access portions of the record that may be stored in disparate locations. This provides a complete, "longitudinal" view of the patient's health from birth to the present day. [GAB94] In exchange for increased openness, medical records personnel must alter their practices not only for storage of electronic rather than paper storage media but also for distribution of the record.

Automation also opens the record to new communities of users and enables new uses for medical information. Cross-matching and filtering are two extremely powerful functions supported by computerization that have created new markets for information. "Certainly there are those who would pay handsomely for a mailing list of individuals guaranteed to have hemorrhoids, but not so handsomely that someone would pour [sic] over relatively chaotic paper charts to surreptitiously compile it." [LIN92:7] Both old users such as medical researchers [IOM94] and a new industry of third-party, direct-marketing information re-sellers benefit. [LIN92; OTA93]

One set of new users is the direct result of procedural changes to how progress notes and test results are entered into the record. Handwriting and voice-recognition capabilities continue to be experimental at best. Instead, commercial automated medical records systems instruct physicians to record information on pre-set encounter forms. Medical transcriptionists then enter these handwritten notes and charts into an information system. [SHO90; WKS93] A second set of new users are a direct result of

the technology itself. The tasks of equipment installation, software implementation and support all require access to real data. [BRO93] Within the medical establishment, information systems divisions are a new set of users. Because not all problems can be solved in-house, equipment vendors and information systems consultants will also occasionally require access.

Figure 2.3
The computer patient record as a federation



Source: adapted from WED92:9

The integration of information technologies into the practice of health record sharing produces tradeoffs in information security threats. Over disclosure is mitigated because "[with] computerized systems, tailored selection of data items from an individual health record is easy, thereby making it possible to share only the information that is necessary to the inquiry at hand." [GOS93:2491] Likewise, automation supports integrity

by constraining user behavior. Administrators could enforce the restriction on erasure and limit those with the ability to update specific portions of the record.

Conversely, automation may exacerbate the risk of redisclosure. Electronic storage greatly simplifies the task of copying and re-transmitting an entire record or selected portions. Unlike access to a single paper record, an electronic record is a 'virtual' document that can reveal the patient's entire history, not just what is contained in one clinician's paper file. Moreover, access to a single electronic database is equivalent to accessing thousands of sensitive, 'virtual' documents:

> Ironically, it is this 'negative' aspect of the paper medium (its cumbersome nature that has minimized [the potential damages that could accrue from] breaches of confidentiality. Although a breach could occur if someone gained access to health records or insurance claim forms, the magnitude of the breach was limited by the sheer difficulty of unobtrusively reviewing large numbers of records or claim forms.
> [WED92:4-17]

That digital storage facilitates redisclosure may be tempered by the arguable effectiveness of audit trails that monitor and record behavior to deter illegitimate use.[9] [DRI93]

In summary, introducing automation extends access to a broader array of users and uses. Simultaneously, information systems foster novel changes to the form, content and procedures involved in record keeping. The resulting computerized record better addresses some of the previous threats to confidentiality and integrity while magnifying others.

2.5 Vision for the future electronic record

Simply automating the existing health record does not fully realize the promise of information technologies, however. Many patients are "beset by multiple problems simultaneously, and require, for example, not just prenatal care, but housing, drug treatment and vocational training as well.... [Care] received by such [patients] is likely to contain gaps and redundancies because no one provider can see the whole picture...."

[9] Define what an audit trail is and indicate that it is beyond the scope of this thesis.

[HHS93a:1] In its efforts to coordinate the delivery of health care and social services, the Federal Government envisions a much broader set of users and uses of the computerized patient record:

> [The government recognizes] the need for electronic data sharing and communications technologies that would allow community providers across diverse agencies and care modalities to communicate easily with one another and to redirect or shape their collective resources on a case-by-case basis to meet the complex needs of families who experience multiple dysfunctions.
>
> [HHS93b:2]

The future electronic record would therefore serve more than just the health care community. Data in the virtual document could support such programs as the Aid to Families with Dependent Children [AFDC] or the Department of Agriculture's Food stamps program. The Department of Justice [DOJ] could incorporate health records into criminal records such as drug and alcohol abuse, psychiatric evaluations, or treatments for violent crimes.[10]

As with any significant change, re-defining the electronic record by expanding the set of users and uses affects information confidentiality and integrity. Risk of redistribution is exacerbated due simply to the increased number of users with access. This risk is compounded by inconsistencies between the security requirements of the different institutions who contribute to and share the virtual document. For example, substance abuse records are subject to unique, more restrictive controls. [OTA93] In direct conflict to this mandate is the legitimate need of many users to review the entire patient health record. When portions of the medical history are incorporated into substance abuse records, whether individual privacy or the needs of the information user prevails is unclear.

As another example, records sealed under court order may prove accessible when defined as a portion of the medical history. That information unavailable in one venue is vulnerable to a persistent user who can simply look elsewhere is also related to the risk of

[10]The introduction of smart cards to enhance both the security and the portability of records is another element of the future electronic record that is beyond the scope of this thesis. See ALP93 and OTA93 for further references.

over disclosure. Automation permits the ability to tailor what information is released to a particular user for a particular purpose; but by approaching different users and combining the portions of the record for which each respective user is authorized, it may be possible to infer information that is not directly revealed.[11]

Problems related to the number of users are not unique to electronic record keeping. When sharing information, the paper records currently employed by health care and social services related organizations are similarly vulnerable to differences in conventions and malicious individuals who combine information from more than one user. However, electronic records magnify the problems. Information technologies simplify the coordination costs of increasing the number of institutions that contribute information to the virtual document. In doing so, communications technologies also increase the number of users with access to each patient record, thereby simplifying the malicious user's ability to derive confidential information through indirect means.[12]

Critical threats facing the confidentiality of information shared across a federation are related to disclosure and inference. Specifically, challenges include: over disclosure, redisclosure, inference and aggregation. Accordingly, the security objectives addressed in the remainder of this thesis are to control over disclosure and redisclosure and to limit opportunities for aggregation and inference.

---

[11]Loosely defined, obtaining confidential information through indirect means such as collecting pieces from different sources and inferring what is not provided is referred to as a covert channel.

[12]The extended computerized medical record will certainly also have significant implications for identification, authentication, audit, and other security issues that are beyond the scope of this thesis.

Chapter Three

Security Policy

Having identified relevant security objectives, this chapter reviews elements of a security policy to mitigate the risks of sharing sensitive, medical information in a federated environment. The chapter begins by surveying elements of existing, proposed and pending policies related to the protection of confidential patient information as an initial point from which to draw ideas. Issues that a security policy would have to address in order to meet the objectives are then elicited from this survey.

The role that technologies play in the policy making process is a thread which runs throughout this policy evaluation. As observed earlier, technology is only part of a comprehensive solution.[13] The rapid obsolescence of today's computers suggests the need for broad, general policy statements that do not rely upon or refer to specific technologies. Conversely, policies should be written with existing technological capabilities in mind. By acknowledging the technology, security policy writers attempt to ensure that their policies neither require unreasonable means to satisfy the objectives nor overlook new capabilities that simplify the task.[14] [OTA93; BRA92] Technology "can pre-exist any legal structure or be established as the result of one." [OTA93:86]

---

[13]People remain the greatest barrier. [NRC91]

[14]Brannigan cites the case of the 1976 Medical Device Amendments that called for the Food and Drug Administration (FDA) to regulate software through premarket approval or product standards. The legislation required "a technical tool that can test a given piece of software and determine how safe it is. Such a tool did not exist." [BRA92, 192]

3.1 Policy survey

Although computerized patient records are only now becoming a mainstream element of health care provision, information technologies have long existed both in government and in the health care arena.[15] As a consequence, concerns for the privacy and security of electronically stored information have already been addressed many times in previous policy initiatives. As a first step in considering policies for addressing the confidentiality objectives identified in this thesis, existing, model and proposed policies are compared and contrasted.

A total of ten different policies ranging from state and Federal legislation to codes of conduct are considered. The policies are summarized below. A more extensive analysis is included as Appendix A. The survey includes four Federal policies, three policies adopted state wide and three policies promulgated by industry. From the perspective of authority, four of the ten policies have been enacted by Federal or state

Table 3.1
Policies surveyed

The Privacy Act of 1974
The Computer Security Act of 1987
American Hospital Association Information Management Advisory on the Disclosure of Medical Record Information
American Health Information Management Association Health Information Model Legislation Language
Workgroup on Electronic Data Interchange Model Federal Legislation for the Confidentiality of Health Care Information
Medical Society of the State of New York Ethical Tenets for Protection of Confidential Clinical Data
State of Montana Uniform Health Care Information Act
Massachusetts State Code on Insurance Information and Privacy Protection
The Fair Health Information Practices Act of 1994, HR4077
The Health Security Act of 1994, HR3600

legislatures. Of the remaining six, two are currently before Congress, two are model

15Record keeping, billing , scheduling, patient directory information, and hospital census are only a few of the myriad services to which information technologies have traditionally been applied in the medical care setting.

language for legislation and two have been adopted and/or endorsed by professional organizations but do not carry the authority of legislation. The analysis of policy mechanisms intended to address disclosure and inference related threats in each of the policies surveyed is included as Appendix A. The policies themselves are summarized below.

Privacy Act of 1974

The Privacy Act of 1974 (5 U.S.C. § 552a) forms the centerpiece of all Federal legislation related to information privacy. The Privacy Act, which includes the Computer Matching and Privacy Protection Act of 1988 and subsequent amendments, "was designed to protect individuals from government disclosure of confidential information." [WED92:4-8] The fundamental premise is that individuals should control the use of information about themselves.

Structured around the five key principles of Fair Information Practices[16] identified by the U.S. Department of Health, Education and Welfare in 1973, the Privacy Act applies to the collection, storage, or use of any individually identifiable information maintained by any Federal agency on any storage medium. The scope of the Act includes "healthcare [sic] facilities operated by the Federal government: the Veterans' Administration, Department of Defense and Indian Health Service." [BRN93:60] Specifically, the Act requires that there "be a way for individuals to prevent information about them, obtained for one purpose, from being used or made available for other purposes without their consent." [OTA93:77]

---

[16]The basic principles of fair information practices were stated in *Computers and the Rights of Citizens*, a report published by the Privacy Commission of the U.S. Department of Health, Education, and Welfare in 1973. The report identified five key principles:

a. There must be no secret personal data record-keeping system.
b. There must be a way for individuals to discover what personal information is recorded and how it is used.
c. There must be a way for individuals to prevent information about them, obtained for one purpose, from being used or made available for other purposes without their consent.
d. There must be a way for individuals to correct or amend a record of information about themselves.
e. An organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuses of the data. [OTA93, 77]

Despite its intentions, however, the protections offered by the Privacy Act are far from absolute. The Privacy Act, as well as the subsequent and proposed legislation described below, acknowledge a greater social interest in permitting the disclosure of individually identifiable information in specific situations without the individual's consent. Public health statistics such as births and deaths, or release in response to judicial proceedings are two such instances. Appendix A provides a more complete listing of instances that might justify unauthorized disclosure.

Moreover, the Privacy Act applies only to information collected by the Federal government. "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 use and disclosure of patient information for research purposes." [WPR93:D7] As a second example, the Health Care Financing Administration (HCFA), under the broadly defined "routine use" clause,[17] authorized the release of the Uniform Clinical Data Set (UCDS) to researchers complete with patient names and identifiers. [WED92] The UCDS is comprised of patient records collected by Medicare Peer Review Organizations (PROs).

With regard to enforcement, the Privacy Act "places the burden of monitoring privacy in information and redressing wrongs entirely with the individual, providing no government oversight mechanism for the system." [OTA93:79] Moreover, "the Act contains no specific measures that must be in place to protect privacy so that it cannot be used to describe what *technical measures* must be taken to achieve compliance" [OTA93:79; BRA92]

Computer Security Act of 1987

The Computer Security Act of 1987 recognized the Federal government's increasing reliance upon computer systems and argued that "improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and

[17]See 5 U.S.C. § 552a(b)2.

hereby creates a means for establishing minimum acceptable security practices for systems ...." [15 U.S.C. 271:§2(a)] Specifically, all Federal agencies were required to: "(1) identify all developmental and operational systems with sensitive information, (2) develop and submit to NIST and NSA[18] for advice and comment a security and privacy plan for each system identified and (3) establish computer security training programs." [GAO90:2]

Provisions of the Act extend to health care data under the definition of "sensitive information." The Act defines "sensitive information" as "any information, the loss, misuse, or unauthorized access or modification of which could adversely affect ... the privacy to which individuals are entitled under section 552 of title 5, United States Code (the Privacy Act) ...." [15 U.S.C. 271:§20(d)(4)]

Unfortunately, the General Accounting Office (GAO) determined that, in the years following adoption, "[t]he planning and review process ... did little to strengthen computer security governmentwide [sic]." [GAO90:1] Moreover, at the time of the GAO study, little progress had been made beyond the planning stage. "[B]udget constraints and inadequate top management support – in terms of resources and commitment – were key reasons why controls had not been implemented."[19] [GAO90:2]

Weaknesses of the Computer Security Act include its vagueness and lack of enforcement. "Many agency officials misinterpreted or found the guidance unclear as to how systems were to be combined in the [security] plans, the definition of some key terms (e.g., "in place"), the level of expected detail ...." [GAO90:5] Moreover, the Computer Security Act imposes no criminal penalties for failure to comply. [GOR92] Because "[t]he costs of detection resistance and recovery can be both tangible and high ...

---

[18]NIST (National Institute of Standards and Technology, formerly the National Bureau of Standards) and NSA (National Security Agency).

[19]Specifically, 22 security plans collected from Federal agencies were reviewed. Of the 145 planned security controls contained in the 22 security plans, only 38% had been implemented as of January 1990. Of those remaining, "[o]nly 4% had implementation dates beyond January 1990." [GAO90:6]

[while] there are no generally applicable methods for estimating the potential costs" of security breaches, the incentive to comply is likely to be small. [CEC93:19]

American Hospital Association (AHA)

"A common theme emerging from the current legal and regulatory framework is that the obligation to protect confidentiality of healthcare information rests primarily with healthcare providers." [BRO93:44] Because of this theme, and perhaps partially in response to the increasing use of information technologies to maintain sensitive patient data, the AHA revised its *Guidelines on Institutional Policies for Disclosure of Medical Record Information* in 1990. The guidelines are independent of storage medium and address "both internal and external disclosures ... [and explicitly] indicate the situations in which medical record information may or may not be released ...." [AHA90:1]

As a professional organization, however, the AHA lacks the enforcement power of legislation. The AHA distributes guidelines, not edicts. Consequently, even within the community of medical institutions, identifiable patient information is not necessarily afforded consistent protection.

Additionally, because they do not carry the weight of regulation or law, guidelines promulgated by provider institutions apply only to providers. Meanwhile, health records today are "no longer simply a tool for health care providers."[20] [IOM94:4-4] Unless identical guidelines are adopted by each individual community of users, the security of the medical record from unauthorized disclosure and inference will be in a constant state of flux. Protection will be uncertain at best.

[20]See Chapter 2 for a discussion about the growing number of users and uses of patient information.

American Health Information Management Association (AHIMA)

Recognizing the hazards of inconsistent guidelines across the diverse community of patient record users, "AHIMA has developed model [Federal] confidentiality legislation to meet this need." [BRN93:60]

The 1993 AHIMA model language is "based on the patients' need to access their own health care information and the need for clear rules about disclosure of that information." [OTA93:77] It incorporates the Fair Information Practices from the 1973 Privacy Commission[21] and enumerates conditions for disclosure of patient information. Also, recognizing that users are no longer limited exclusively to the medical community, the AHIMA model language explicitly states that conditions expressed within the model text "shall apply both to disclosures of health information and to redisclosures of health information by a person to whom health care information is disclosed." [AHI93:§103(a)] "The model language also addresses proper use and disclosure of health care information by secondary users." [OTA93:77]

Like other efforts, however, the AHIMA proposal "provides for no oversight or enforcement mechanism for the system." [OTA93:77] Consequently, the rules may provide uniform coverage if observed; unfortunately, there is little incentive to abide by the regulations.

Workgroup on Electronic Data Interchange (WEDI)

WEDI grew out of a forum of national health care leaders convened by then Secretary of Health and Human Services Louis Sullivan in November 1991 to discuss alternatives for reining in the enormous administrative costs of providing health care. Specifically, WEDI was charged with realizing the benefits of electronic data interchange (EDI) for exchanging and processing all manners of health information including patient records. [WED92]

---

[21] See footnote reference number 16 on Fair Information Practices.

"Recognizing the inherent tension between the need for liberal interchange of identifiable, personal health information and the need to preserve the confidentiality of such information," WEDI called for and later drafted model Federal, preemptive legislation, "to facilitate and ensure the uniform, confidential treatment of identifiable information in electronic environments." [BRO93:42]

WEDI's model legislation, like that of other proposals and guidelines, explicitly enumerates conditions for disclosure. However, WEDI eases the conditions for disclosure between providers and payers to a par with disclosure between two health care providers involved in the immediate delivery of care. [WED93a:§3C] Therefore, unlike other proposals, although WEDI would require providers to maintain a log of disclosures, disclosure to payers would not be included in the log. [WED93a:§6B]

A second deviation WEDI takes from other proposals lies in its "use" restriction. Most proposals adopt the Fair Information Practices language from the 1973 Privacy Commission and limit use to the purposes for which the information was collected or received. WEDI loosens that restriction to permit any "legitimate purpose for which the individual has granted consent." [WED93a:§5B(2)] The significance of the distinction depends upon whether consent must be received prior to collecting the information and/or whether blanket consents are acceptable.[22]

Ethical Tenets of the Medical Society of the State of New York

The Ethical Tenets for Protection of Confidential Clinical Data were originally drafted as part of a Joint Task Force on Confidentiality of Computerized Records convened in 1968. The Tenets were subsequently adopted by the Medical Society of the State of New York. Although some sections are open to broader interpretation, "[u]nlike the more general approach of the Privacy Act, the Ethical Tenets speak directly to specific concerns encountered in the area of health care information." [OTA93:77]

---

[22]Neither scenario is addressed in the WEDI draft legislation.

Providers are bound to keep all treatment related information in strictest confidence. [ETH93:§2] Any use of identifiable information that is "not a part of the patient's treatment and not a part of professional communication to contribute to the care of the patient" qualifies as secondary use. [ETH93:§9] Use of secondary information is tightly bound "only for the original purpose for which [it was] generated and shall be promptly destroyed, or at least disidentified [sic], as promptly as possible." [ETH93:§10]

The Tenets are also extremely restrictive with respect to disclosure. The Tenets stipulate that "[i]dentified secondary clinical records shall receive confidential treatment" without specifying the terms or conditions of "confidential treatment." [ETH93:§9] Furthermore, for any public health or research use of secondary records, "the informed consent and explicit formal authorization of the patient or his guardian shall be sought and attained prior to such release." [ETH93:§10]

However, although it is unclear, the Tenets seem to apply only to providers.[23] Second, the requirement that secondary records receive confidential treatment is not accompanied by a definition of what constitutes "confidential treatment." [ETH93:§9]

As with any non-legislative solution, that the Tenets "have never had the force of law in any jurisdiction" weakens its authority. [OTA93:77] Lack of legislative clout is further compounded by non-uniformity. According to the Tenets, "[e]ach data center handling identified medical data shall formulate and maintain its own operational rules and practices," introducing the potential for inconsistent protection across providers. [ETH93:§12]

Montana State Uniform Health Care Information Act (UHCIA)

The National Conference of Commissioners on Uniform State Laws convened in the early 1980's "to stimulate uniformity among states on health information

[23]The Tenets explicitly apply to "all clinical data centers storing patient records ...." [ETH §8] However, as operationally defined, a 'clinical data center" ranges from "a solo practitioner's office computer to large hospital-based data centers and regional data systems, if these data centers regularly store patient records." [ETH §8]

management issues." [BRN93:60] The commissioners were motivated, in part, by the "'the use of health-care information for non health-care purposes; ... and the exponential increase in the use of computers and automated information systems for health-care record information ...' UHCIA Prefatory Note." [WED92:4-11] The Uniform Health Care Information Act that resulted is included in this survey as enacted by the State of Montana in 1987.

Like the broader Privacy Act, the UHCIA does not "focus specifically on the problems presented by computerization of [patient] information. Many of the provisions of the UHCIA are applicable in both a computerized or non computerized environment." [OTA93:77] Both vulnerabilities and possible solutions might be overlooked by failing to consider the existing technologies.

The UHCIA represents both an attempt to preserve the discretion of individual states in setting health care information legislation and an example of uniform state legislation to provide consistent regulation (as opposed to preemptive Federal legislation). Unfortunately, to date, "it has been adopted by only two states – Montana and Washington." [BRN93:60]

A second potential weakness of the UHCIA stems from the Commissioner's belief that "rules for use and release of health information should be developed according to the group that holds the information, not the type of information that is held." [WED92:4-11] Protection that does not single out types of information contrasts with existing practices such as state laws which explicitly single out AIDS related complications[24] or Federal statutes which "prescribe special confidentiality rules for the records of patients who seek drug or alcohol treatment at Federally funded facilities."[25] [WED92:4-9]

---

[24]See the discussion on the Massachusetts State insurance legislation that appears further into Chapter 3.
[25]See 42 U.S.C. §§ 290dd-3, 29033-3 (1988) and 42 C.F.R. § 2.12(3)(4) (1990).

Another consideration is the limited scope of the UHCIA. "The provisions of [the UHCIA] are limited ... to providers and hospitals in a relationship with the patient. It does not address secondary uses of health care information." [OTA93:77]

Massachusetts State Insurance Information and Privacy Protection Act

The Massachusetts State Insurance Information and Privacy Protection Act is "based in large part on model rules proposed by the National Association of Insurance Commissioners (NAIC)." [OTA93:76] The Insurance Act stipulates provisions for the acceptable use and disclosure of individually identifiable policy holder information related to claims and coverage.

"While this law was drafted specifically to address the problems of life, health and disability insurance information, many of the definitions, principles and provisions are equally applicable to providing privacy protection for health care information generally." [OTA93:76] Relevant portions of the Insurance Act offer a model for how to affect both disclosure and use.

As with acts devoted explicitly to health related information, the Insurance Act narrowly defines criteria for permitting the disclosure of individually identifiable information both with and without the subject's consent. No differentiation between electronic and paper records is made.

Of the policies surveyed, unique to the Insurance Act was the explicit identification of specific "uses" for insurance related information. Depending upon the "use", different disclosure guidelines are mandated. For example, recorded personal information and medical records are differentiated from investigative consumer reports which are, in turn, differentiated from personal or privileged information from insurance transactions. [MASS:§7, 8, 13]

Whether a cause or an effect, a related implication of categorizing permissions based upon use is the creation of different confidentiality classes of individually

identifiable information. In particular, AIDS and ARC[26] are singled out as being particularly sensitive and deserving of extra care. Gender, race and sexual preferences also qualify. Activities to aggregate or infer information about such personal characteristics are explicitly prohibited. [MASS:§2, 7(d)]

Fair Health Information Practices Act of 1994 (H.R. 4077)

Representative Condit introduced the Fair Health Information Practices Act of 1994 to the House of Representatives on March 17, 1994. The Act answers the perceived need for Federal action in response to "[t]he movement of individuals and health information across State lines, access to and exchange of health information from automated data banks and networks and the emergence of multistate health care providers and payers." [HR4077b:§2(a)(4)]

Unlike existing computer security and privacy legislation that applies only to Federal computer systems, H.R. 4077 relies upon the interstate commerce clause of the Constitution to promulgate a single, uniform set of rules and procedures governing the use and disclosure of identifiable patient health data in any institution. [HR4077b:§2(a)(4), 3(b)(3)(A)]

Similar to the AHIMA model language, the uniform protection offered by H.R. 4077 applies to the data itself rather than to the recordkeeper. Consequently, "[i]n general, protected health information remains subject to statutory restriction no matter how it is used or disclosed." [HR4077a] Whether the recipient of sensitive medical information is a provider, payer, researcher, or marketer, the same regulations apply.

Unique to H.R. 4077 among those policies surveyed is the separation of users into classes in a manner similar to the Massachusetts insurance legislation division of "uses". "Each class of trustee has a [sub]set of responsibilities and authorities that have been

[26]AIDS (Acquired Immune Deficiency Syndrome) and ARC (AIDS-related complex).

carefully defined to balance legitimate societal needs for data against each patient's right to privacy and the need for confidentiality in the health treatment process." [HR4077a]

Health Security Act of 1994 (HR 3600)

First introduced in late 1993, the Health Security Act attempts to address the multi-headed health hydra which includes exploding costs, inconsistent quality and inadequate coverage. The Health Security Act "establishes twin goals of electronic records and electronic data interchange" as part of the solution. [BRO93:40]

On the subject of health information security, however, the Act is vague. As with existing privacy legislation, the Act centers safeguards around a code of fair information practices that stipulates that "subjects of the health data collected, have the right to ... approve the uses to which the data are put; ... and have adequate assurance that data may be collected and used only for legitimate purposes." [BRO93:43] However, there is no notion of what constitutes a "legitimate purpose."

Protection applies to all individually-identifiable health care information:

- Whether it is part of the new health care system or exists outside it.
- With the same level of protection [for information about any] illnesses and disease [i.e., universal protection].
- Regardless of the form in which records are kept (paper, microfilm, or electronic), location (storage, transit, archive), owner, user or repository (government, health provider, private organization).

[HR3600:136]

However, how complete or extensive the universal protection will be is unclear. One objection to preemptive legislation that provides the same level of protection to all manners of health care data is that information security will be set to the lowest common denominator rather than being held to a higher standard. [OTA93] Moreover, even existing legislation acknowledges that some types of information (e.g., drug and alcohol abuse related information) is more sensitive than others. [WED92; WED93b]

Finally, the Act would "explicitly forbid the linking of healthcare [sic] and other information through the identification number." [BRO93:44] However, even the

Computer Matching and Privacy Protection Act of 1988 acknowledges a legitimate need for and use of matching in particular circumstances.

3.2 Policy analysis

Drawing on this analysis of the status quo and proposed policies, it is clear that a policy to ameliorate disclosure and inference related risks must address several issues. The decisive elements of a policy can be considered as a series of questions:

- Control access versus control use?
- Categorize information?
- Categorize users?
- Address electronic information exclusively or explicitly?
- Address patient information only?
- Promulgate Federal, state, or institutional policy?

Control access versus control use?

Of those surveyed, security policies tend to fall along a continuum between two general strategies: those that control access and those that control use. Policies of the former focus on who the prospective users are. Such policies are typified by trust. If an individual is authorized to look at a certain piece of data, the user is trusted to know and observe the privileges and policies associated with receiving that information.[27] Policies of the latter type rely upon limiting what a user may do either with or based upon the information that they have seen. For example, in the legal system, as a part of attempts to preserve impartiality, jurors can be recused if they have read or heard too much about the case being tried.

Disclosure and inference can be addressed by either policy. In the extreme case, using an access based policy, the source only relinquishes data if it does not care what the receiver will do with that information. Likewise, a sender makes data universally available under the general policy that no one can use any information that they receive.

---

[27] A subsequent chapter will elaborate upon the military, hierarchical access control scheme where users have clearances and information has sensitivity labels. Together, clearances and sensitivities determine to what information a specific user is authorized to have access.

Practically speaking, however, even if either extreme were enforceable, data released under such strict conditions would most likely be of little or no use to anyone; the information would either be too vague or serve no purpose because any practical use was prohibited.

Real policies occupy the middle ground. The challenge is to define some combination of access and use based control. In practice, status quo, paper-based medical records tend to rely formally upon access restrictions and informally upon use constraints:

> Access to a health record itself may be difficult to achieve – it requires physical presence at the site where the 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.
>
> [WPR93:D3]

Ethical codes of conduct ensure that data, once received, are only applied to and disclosed for legitimate purposes.[28]

As noted in Chapter 2, the migration to electronic records challenges the effectiveness of existing practices for controlling disclosure and inference related threats. For example, access is no longer constrained by the need for a physical presence. The efficiency gains from sharing records electronically also increase the likelihood that information unobtainable from one source may either be found or inferred by querying one or more other sources. Moreover, increasing the range of users with access to identifiable patient data increases the risks of abuse as well. Secondary users are less likely to have codes of conduct regulating information use. [GAB94]

Fortunately, "[c]omputerization poses problems for the protection of privacy and confidentiality, but it also offers new opportunities for protection." [IOM94:4-20] New policies should continue to mix access and use while recognizing that access to "defined parts of records can be granted, controlled, or adapted on a need-to-know (or function-related) basis; this means that users can be authorized to obtain and use only information

[28]See LEW93 which includes relevant portions of the American Medical Association 1992 Code of Medical Ethics.

for which their use is justifiable." [IOM94:4-20] Making use of this finer control, however, will require some categorization of both information and users.

Categorize information

The principle behind categorizing information is fairly straightforward. Whether for research, mitigating an insurance claim, administrative quality assurance, responding to a legal action, etc. the specific use in question may neither need nor justify access to all of the data contained in the medical record. Therefore, information should be separable so as to disclose only that which is relevant for the specified purpose.

Data contained in the medical record may be categorized across at least two dimensions: sensitivity and record characteristics. Sensitivity corresponds to the notion that some data is more valuable than others. The hierarchical military access control policy discussed in Chapter 4 classifies data based upon the threat posed to national security by the loss or unauthorized disclosure of said data. Record characteristics are the set of parameters that may be used to uniquely identify entries in the medical record. Parameters may vary across a spectrum from a chronological index based upon the date an item was entered in the record to a problem-oriented index based upon the DRG or ICD-9 classification.[29]

Record disclosure is already governed by sensitivity to some extent. "Certain types of information, such as AIDS, drug and alcohol treatment records, are considered more sensitive and thus receive heightened legal protection." [BRO93:42] Likewise, even traditional paper records are categorized to some degree. Tab inserts in the record partition progress notes from lab tests from billing information, etc.

Separating data based upon sensitivity can be problematic, however:

> [T]he sensitivity of data depends on the kinds of harm to which individuals are or believe themselves to be vulnerable if the information were known to others. Such assessments differ dramatically from one

[29]DRG (diagnosis related group) and ICD-9 (International Classification of Diseases, 9th edition) are standard identifiers for medical treatments and diseases in the medical literature.

> person to another, one circumstance to another, one place to another, and over time as cultural attitudes change.
>
> [IOM94:S14]

Moreover, "flagging information as having been blocked [for sensitivity] might in some circumstances defeat or even exacerbate the challenge to privacy; such a label or flag would alert anyone reviewing the material that it includes sensitive data." [IOM94:4-47]

Record characteristics raise equally complex questions. In particular, what data type does a characteristic uniquely identify? Depending upon its precision, an identifier may isolate individual sentences within a free-form progress note or do no more than single out a particular patient's record. A researcher may want all data entries related to a particular drug. Administrators may need a list of all of the procedures corresponding to a particular visit or to the treatment of a particular complication. Insurers may want all information related to a particular claim including histories of related conditions.

Specific identifiers that precisely isolate data like individual laboratory test entries are less problematic because users authorized to see large portions of the record may, through complex or repeated queries, eventually retrieve all of the information being sought. Systems that use broad separators like tabs in a paper chart present more complications. Even when carefully chosen, using general dividers to provide selective access is difficult. The autonomy sought in federated systems suggests that constituents should have discretion in selecting the specificity of characteristics that they use. Conversely, in a federation, information is often as vulnerable as the federation's weakest constituent. Therefore, one would not wish to grant federation participants too much latitude.

Categorize users

The analog to separating information is separating users. In addition to varying "from one person to another, one circumstance to another, one place to another, and over time as cultural attitudes change," an individuals' perception of sensitivity is also a

function of who holds the data. [IOM94:S14] Information that a patient might reveal to a personal physician might never be revealed to even a spouse or a sibling let alone an insurance claims evaluator or a researcher. Consequently, to accompany the separation of data, users are categorized and, depending upon the category, are authorized to access different portions of the patient record.

Depending upon the system, the categorization of users varies from a very coarse to a very fine granularity. At one end of the spectrum, every user is a member of the same category. Consequently, every user has the same rights. At the other extreme, each user could define his or her own category. Then, authorizations and rights are tailored to each specific user. As with access versus use based controls, neither extreme is very practical. If there is only one category, users will likely have either too much or too little discretion. At the same time, the administrative overhead of managing authorizations tailored to each user is too great.

The default for paper records appears to be a single category where, most often, users either get the entire record or else they get nothing. Claims evaluators, lawyers, consulting physicians, etc. often get the entire record even though only specific portions are requested or required. [WPR93; IOM94] Separating and sorting the paper record is simply too time-consuming. [GAB94; SZO94] Those that receive partial information such as some claims evaluators or public health officials recording births and deaths often do not see the entire record simply because they provide separate forms rather than requesting the record.

Although automation facilitates finer degrees of control, a trade-off exists between degree of control and ease of use. "In the more traditional healthcare [sic] provider relationship with employed physicians, nurses, technicians and other professional personnel, written confidentiality agreements generally have not been used to protect against unpermitted disclosures." [BRO93:46] Although information technologies make it possible to enforce access restrictions that differentiate between

physicians, nurses, etc., doing so might do more to adversely affect the quality of care by interfering with the daily workflow.[30] [SZO94] Therefore, when drafting security policies, writers must strike a careful balance between providing too much access and being too restrictive to the point of incapacitating health care workers.

Address electronic information exclusively or explicitly

While Chapter 2 pointed out that information technologies may exacerbate many of the threats to individually identifiable patient data, disclosure and inference have always posed some threat to the confidentiality of information. Therefore, it is unclear whether a policy to protect the confidentiality of computerized patient records should address specific technologies. The decision may depend, at least in part, on whether there is a significant difference between information which is collected, maintained, or distributed electronically versus information in any other medium.

The general consensus appears to be that "[t]he legal obligation of confidentiality does not vary with the medium in which data are maintained. The same confidentiality obligations apply to paper records and computerized records." [BRO93:42] Moreover, for health records in particular:

> One of the most fundamental aspects of the relationship between a patient and health care provider is the provider's obligation to maintain health information in a confidential manner. That obligation, which is defined by statute, common law, and professional ethics, is static. It does not change with the medium of health information transmission or storage, whether paper or electronic.
>
> [WED92:4-3]

However, the proliferation of specific, computer related crimes and the integration of information technologies into all aspects of the government has prompted the passage of numerous pieces of technology specific legislation. The Computer Matching and Privacy Protection Act of 1988, the Computer Security Act of 1987 and the Counterfeit Access Device and Computer Fraud Act of 1984 are three such examples. Clearly, while

[30]This issue is discussed further in Chapter 4.

confidentiality obligations may remain the same, "the electronic medium will potentially allow for remote and unauthorized review of unlimited health information. It will greatly increase the dimension of inadvertent and intentional breaches of confidentiality." [WED92:4-4]

Address patient information only

Several of the policies surveyed differed in scope, ranging from an exclusive focus on individually identifiable information in the patient–provider relationship to addressing all types of individually identifiable information, not just health care related records. As with policies that single out electronic media, whether policies to support the confidentiality of computerized patient records tend towards the former or towards the latter may depend, at least in part, on whether patient information is significantly different about any other individually identifiable information.[31]

General policies such as the Computer Privacy Act of 1974 or the Computer Security Act of 1987 make no specific mention of health care related information as having any greater need for protection or being at any greater risk than any other individually identifiable information. "[A]ny data element in medical records, and many data items from other records, could be considered either health-related or sensitive, or both. Where the boundaries for the protection of personal health information lie is not at all obvious." [IOM94:4-14] Furthermore, to the degree that sensitivity is dependent "on the kinds of harm to which individuals are or believe themselves to be vulnerable if the information were known to others," health care related information is not unique with respect to privacy. [IOM94:S14]

However, there seems little doubt that "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." [WPR93:D1]

[31]Other individually identifiable information might include financial records, judicial proceedings, and academic records.

Perhaps a more concrete distinction between any two types of information (not necessarily health related) relates to the categorization of information and users discussed earlier. Dividing information and separating users to simplify the administration and increase the effectiveness of security controls requires some boundary on the body of information a particular policy addresses. Otherwise, there is no effective context from which to divide users.

Promulgate Federal, state, or institutional policy

The policies surveyed traverse a broad spectrum of existing and proposed policies at the Federal, state and institutional levels. While it is possible that issues such as regulating access versus use or categorizing users should be addressed exclusively by only one of these levels, it seems far more likely that a comprehensive security policy will include actions at multiple levels.

In the status quo, responsibility for the confidentiality of health information is centered on the health care provider and regulated primarily by the states. [IOM94; WED92] Unfortunately, state regulations have many limitations. Within a state, "[t]he great variance in disclosure rules creates inconsistent standards for providers and offers inconsistent protection to patients." [WED92:4-17] "A brief review of state statutes indicated that in one state, more than 50 different statutes and regulations pertain to the confidentiality of medical information." [IOM94:4-33] The interstate nature of modern health delivery also defeats state action:

> Records will be routinely transmitted electronically across state lines, and may even be *created* simultaneously in two different states; ... although they are generally similar in their intent, [confidentiality laws] differ from state to state both in scope and application.
>
> [WPR93:D7]

As noted earlier, to date, efforts by the states to adopt uniform legislation have failed.[32] Finally, even if protection is applied consistently across the different states, more often

[32]Only Montana and Washington have adopted the Uniform Health Care Information Act.

than not, "such protection is no longer in effect once the data have left the recordkeeper's control." [IOM94:S13] Consequently, there is no control of redistribution.

As an alternative to the status quo, several of the proposed policies suggest that "Federal preemptive legislation is required to establish uniform requirements for the preservation of confidentiality and protection of privacy rights for health data about individuals." [IOM94:S13] Federal legislation could also "clearly establish that the confidentiality of person-identifiable data is a property afforded to the data elements themselves, regardless of who holds those data." [IOM94:S13]

Clearly, some level of Federal action is warranted. As suggested earlier, many of the issues raised in the policy survey might be better met at the national level. However, apart from political issues such as federalism[33], there remains the question of which issues require a national mandate and which should be reserved for individual states and institutions. Before speculating further, this thesis turns to the technology. What information technologies can do to support security policies may affect the nature of the policies that emerge.

[33]Federalism in the sense of separation of powers between the states and the national government.

Chapter Four

Access Controls

Having identified a set of security objectives and considered elements of a security policy required to meet the objectives, this chapter turns to mechanisms that implement the objectives and the policy. Specifically, this chapter analyzes logical and procedural elements of access control polices. Traditional discretionary and mandatory access control policies (DAC and MAC) may be insufficient for addressing many of the concerns raised in Chapter 2. Role-based access controls are introduced, and a description is given of how role-based access controls might be applied to the computerized patient record (CPR) environment. The chapter concludes by noting the limitations of role-based access controls and argues for a balance between technology-based and policy-based solutions to address the issue of information security.

As noted earlier, although they play a crucial role in providing a complete picture of security for the CPR, issues related to communications and maintaining consistency between the different constituents in the federation are not addressed. The remainder of the discussion also assumes that users have been properly identified, authenticated and that activities are audited. Identification and authentication refers to the log-on procedure of identifying who the user is and verifying that the user has permission to access the

system.[34] Auditing is the process of recording security relevant activities in a log of system events.[35]

4.1 What is DAC

Traditional DAC (discretionary access control) is defined in terms of subjects, objects, access modes and predicates. Subjects constitute the finite set S of users, groups of users, or processes that may execute on behalf of a particular user. Objects are the set O of elements to which users are granted access. For the CPR, each portion of the record (e.g. progress notes, lab results, demographic data, etc.) might be represented by a separate object, the union of which would constitute a complete patient record. The different ways in which a user may access an object, whether the user may *read* or *write* a specific portion of the patient record, form the set M of access modes. Finally, some access modes may be conditional. A physician might only be permitted to look at the records of patients under her direct care. P is the set of predicates that defines such conditions as logical statements.

An access rule is therefore a tuple consisting of $<s, o, m, p>$ where $s \in S$, $o \in O$, $m \in M$, $p \in P$. The rule explicitly declares that subject s may access object s_2 in the modality m subject to the constraint p. Once a user has logged onto a system and been identified and authorized, requests to manipulate information in the system would be tested against specific access rules. One rule might permit Dr. Smith to read and write progress notes for patients under his care. A different rule might restrict insurance agent

---

[34]Mechanisms for identifying and authenticating users typically involve some combination of three parameters: what the user knows, what the user owns, and who the user is. Passwords are included in the category of what the user knows. Cards or tokens presented to a security guard as identification for entry to a secure area are an example of something the user might own. Biometric devices that match fingerprints or retinal scans can identify users based upon physical characteristics who they are. Further references to identification and authentication may be found in [NRC91; OTA87; OTA93]

[35]The granularity of what activities are logged (e.g., record every keystroke or merely maintain which users logged on to or off of the system at what times) and to what purpose the log is applied have raised many questions concerning a user's privacy rights. Audit trails also tend to accumulate rapidly into large, unmanageable records. Please see [NRC91; OTA93] for further information on audit trails.

Smith to read-only access of a specific lab result in order to verify that a test for which reimbursement was being claimed was actually administered. [GRA93; NYA93; PER93]

Traditional DAC is commonly depicted as a matrix that separates subjects into rows and objects into columns. The cells that form the intersections of the matrix contain entries representing the modalities and authorizations that constrain the relevant subject's access to each respective object. [PER93]

A defining characteristic of DAC is that a user (or a program operating on a user's behalf) is permitted to specify the access modalities and constraints with which others may access objects owned or created by that user. [DOD85; NOT91] Stated differently, DAC permits a subject s_1 to pass an access right on an object $<o, m, p>$ accorded to s_1, to another subject s_2. The system trusts s_1's discretion.

4.2 What is MAC

MAC (mandatory access control) involves a hierarchical assignment of clearances to subjects and classifications to objects. Although clearance levels reflect the privilege of users while classification levels reflect the relative sensitivity of information, both clearances and classifications use the same metric (e.g., secret, top secret, etc.).

Traditional MAC assumes that users may perform one of two operations on data: users may read from or write to a data file (writing assumes the ability to read as well). As a policy, MAC is defined by two rules: *simple security* and the **-property* (read as the *star property*). Simple security mandates that a subject may *read* an object if and only if the subject's clearance level is greater than or equal to the object's classification level. [DOD85] The **-property*, also called the *confinement property*, governs *write* access. [DOD85] It states that a subject may only write to an object if the object's classification level is greater than or equal to the subject's clearance level.

Enforcement of MAC involves the process of comparing a user's clearance to the classification of the object for which access is being requested. [DOD85] The

combination of restrictions on read and write guards against the unauthorized disclosure of information by ensuring that users cannot gain access to information for which they are not cleared. 'Simple security' prevents a user from reading information marked with a higher classification and the '*-property' prevents a user from writing information at one classification level into a document with a lower classification, thereby making the document available to unauthorized users who would ordinarily be prevented by the 'simple security property'.

A hierarchical ordering of classifications and clearances might suggest that any user with a higher clearance could access all of the objects accessible to a user with a lower clearance. However, MAC recognizes that some classifications and some clearances may be equivalent. Resident A and Resident B may both have access to patient files, but each reads a different subset of patient files because different patients see different physicians. In recognition that equivalencies may exist, traditional MAC is satisfiable given a partial ordering on clearances and classifications. [NCS92]

As a policy, MAC is mandatory in that the 'simple security' and the '*-property' are always enforced on every subject and every object whereas DAC rules are tailored by and applied at the discretion of individual subjects. DAC rules are also mandatory to the degree that they are always enforced as specified. The distinction between MAC and DAC lies in a subject's ability to grant access rights. MAC does not provide subjects with the ability to grant rights.

DAC and MAC are not mutually exclusive, however. The simultaneous implementation of DAC and MAC uses the MAC rules to constrain the degree of discretion a subject may specify. For example, subject s_1 cannot grant read access on an object o to a different subject s_2 if the classification of o dominates the clearance of s_2. Doing so would violate the 'simple security policy.' Likewise, though a subject's clearance dominates an object's classification, access is not automatically granted.

Rather, subjects cleared under the MAC rules must still be granted access rights by the object's owner. This embodies the military concept of *need to know*. [NRC91; NCS92]

4.3 Limitations of traditional access control policies

Although DAC and MAC (discretionary and mandatory access control) are both well understood, from the perspective of the CPR, neither is particularly well suited to a federated environment in general nor to the medical environment in particular.

Many difficulties that DAC has with the federated environment are related to the large number of potential users in an environment that attempts to interconnect large numbers of users from heterogeneous systems:

- As the number of users increases, so too does the complexity of managing the different access constraints relating each subject and object. [PER93]
- While access constraints may be expressed as a tuple $<s, o, m, p>$, because federations attempt to preserve the autonomy of constituents, differences may exist between the granularity upon which objects are defined, access modes and the syntax with which predicates defining conditions governing access are expressed.[36]
- By interconnecting related systems, federations increase the risk of unauthorized logical inference. Subjects may either aggregate large amounts of data from a single source or query bits of information from many different sources to infer information that would otherwise be inaccessible. [MOR92]
- Systems that permit the discretionary granting of privileges are particularly vulnerable to Trojan Horse attacks where malicious code executes with all of a subject's privileges but without that subject's knowledge or consent. [GRA93; McC90; NOT91]

DAC's support of a subject's discretion in granting privileges complicates the ability to enforce a consistent security policy across the entire federation. Conversely, if implemented in its traditional sense, MAC would apply at the global level and apply uniformly across the federation. Using technology to enforce a global policy is also problematic, however: MAC is equally vulnerable to the heterogeneity of federation

[36] Is an object o equivalent to the entire patient record or more finely tuned to correspond to individual entries in the progress notes. Some systems may support the access modality *m(delete)* while others, like accounting software, might prohibit deletions altogether. [CLA87] Predicates p might be expressed in first-order predicate calculus in one system and as a table in another.

constituents. Different systems may use different terms in their classification and/or clearance hierarchy. Other systems may map classifications and clearances differently. [PER93; MOR92]

Even if patient records were not implemented in a federated environment, however, traditional access controls might not be suited to the medical context. In traditional DAC, the creator of an object is the subject with the right to transfer access to others. Who owns the information in a medical record and who should have the right to transfer access to others is not immediately clear. [TIN88; NOT91] Although intuition suggests that patients own the information and should determine disclosure, not all disclosures can or should require consent or notification of the patient.[37] In emergency situations, the patient might be unable to authorize a transfer of records. As part of an on-going criminal investigation or for public policy reporting requirements such as suspected child-abuse, requesting consent might be inadvisable. And in some cases, such as the public health reporting of deaths, consent might be impossible to obtain.

A second problem with DAC is that access constraints are not tightly bound to the data. "Thus, a user who is allowed only read access to a data object would still be able to make a copy of that object and pass it on to some other user." [NOT91:15] A user authorized for read only could still copy the record and redistribute it to subjects who were not originally granted access. [McC90]

The same problem exists, albeit to a lesser degree, for MAC. Without DAC support, a user with the appropriate clearance has the authority to read and write records provided the clearance and classification levels are consistent regardless of the "need to know". This is somewhat akin to permitting a professor to write on any student's grade report regardless of whether the student has taken the professor's class.

The problem of binding constraints to data is further exacerbated in a federated environment. Once information resides in another system, there is no practical, technical

---

[37]Please see Chapter 3.

mechanism for ensuring that the receiving system has either the means or the inclination to enforce the sender's constraints on disclosure and/or modes of access. For both DAC and MAC, the alternatives are:

1. Permit each constituent of the federation to personally conduct a technical evaluation of all participating systems to verify the security measures.
2. Refuse to disclose any information and withdraw from the federation.
3. Blindly trust participating constituents.

For each constituent to fully preserve its own autonomy would suggest alternative 1 or alternative 2. Because neither is practical, in practice, constituents must adopt a middle ground, sacrificing some autonomy and exercising some degree of trust in exchange for realizing the benefits of collaboration. [McC90]

One of the greatest limitations of traditional MAC is the requirement that at least a partial order exist on clearance and classification levels. As with many non-military environments, a partial ordering cannot necessarily be defined for the medical domain. [BIS90] For medical records, administrators may have permission to view non-individually identifiable patient information for quality assurance or utilization review purposes; but physicians have access to identifiable, diagnostic portions of the record. Conversely, administrators view patient-identifiable billing information for reimbursement purposes while physicians have no reason to know a patient's insurance status. This anecdotal evidence suggests that there is no clear sense of order regarding clearances or classifications in the medical environment. A survey conducted by Grizalis et. al. confirms that not all user classes and information labels are hierarchical. [GRI91] Some contexts are better represented as a table than as a graph structure. [GRI91; BIS90]

As a consequence of the limitations of DAC and MAC, researchers have focused on developing access controls that may prove more flexible in adjusting to the requirements of environments beyond the traditional, military domain. In particular, one such body of work, generally referred to as role-based access control, shows promise as a technology for supporting confidentiality requirements of CPRs. After introducing and

defining role-based access control, this chapter will question its advantages, apply it to the medical record environment and conclude by raising some limitations of role-based access control.

4.4 What is role-based access control

The need for and concept of role-based access stems from two simple observations:

- The workplace is a social environment. The introduction of information technologies such as CPRs into the medical center may disrupt the standard workflow and patterns by which employees accomplish their routine tasks. "Many systems, satisfactory from a technological point of view, have failed because of a too limited consideration of social factors." [CAS92:146]
- The workplace is a dynamic environment. Both the users seeking access to information and the data itself are in a constant state of flux. The absence of one employee due to sickness or vacation will affect the activities, responsibilities and information needs of others. [CAS92]

These two observations suggest the need for controls that more accurately reflect the nature of the workplace being automated. Moreover, adopting such controls could facilitate the evolving structure of a networked health care system. Role-based access control recognizes that a user's need for information is not inherent to the user's person. Rather, the need for access is a function of what tasks the user is performing. [THO91:166] For example, in Figure 4.1, user s_1 has no inherent need to record a patient's vital signs. To fulfill the duties and obligations of a physician, however, s_1 may need to collect and make note of a patient's health status. Moreover, role-based access control recognizes that multiple users can play a single role, and that likewise, a single user may assume many different roles at different times.[38]

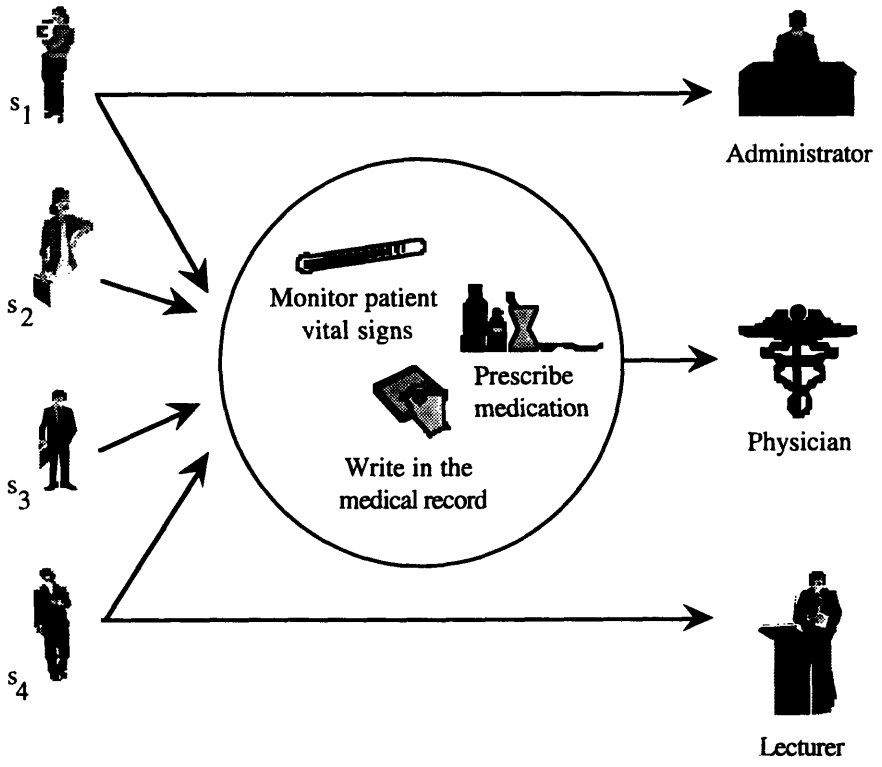
More formally, role-based access control may be defined using the constructs originally defined for DAC: The finite set S of users, groups and processes that execute

[38]Whether a single user can assume multiple roles at any one time is taken up later.

on behalf of a specific user, objects O, access modes M and predicates P Let an *access right* be defined as the tuple $<o, m, p>$ where $o \in O$, $m \in M$, $p \in P$.[39]

Definition: A role is a named collection of access rights. It consists of a name *RN* and a list of tuples *AL* of the form $<o, m, p>$. [NYA93]

Figure 4.1
Many-to-many mapping between users and roles



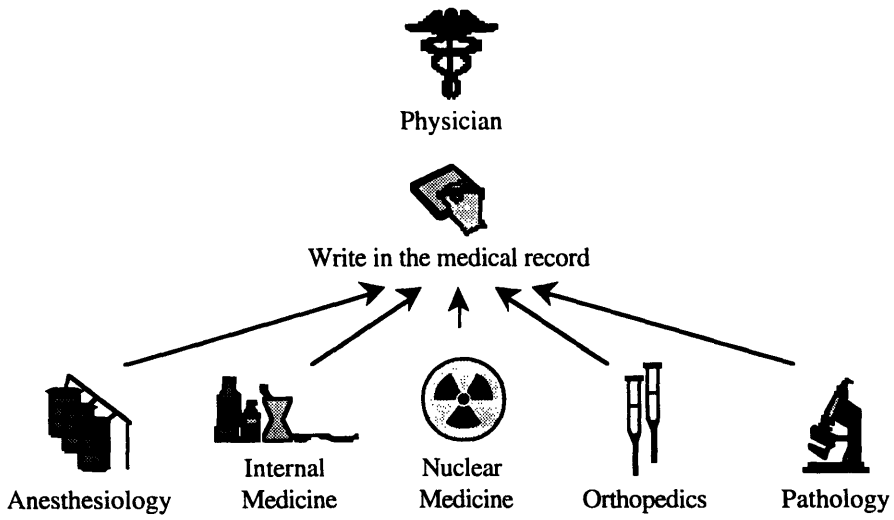
Subjects may only access objects through a role. The many-to-many mapping of subjects to roles and assignment of access rights to a particular role is a system function reserved for the role of the system administrator. Subjects themselves may not grant the

[39]Note that the phrase *access right*, as used here, is also referred to as a *capability* in some of the information security literature. Because the term *capability is* not necessarily used consistently, however, it is intentionally omitted to avoid ambiguity and confusion.

right to assume a role to another subject. Likewise, roles may not reassign access rights to roles except as explicitly defined as a characteristic of the role itself. For example, the role of system administrator has the right to assign access rights to roles.

No ordering is assumed on roles. However, it is possible to order roles hierarchically. Hierarchical ordering enables the inference of access rights. [NYA93] Inference is a technique for simplifying the administration of complex access rights. When two or more sub-roles $RN_{1 \ldots n}$ share a set of access rights, rather than administering the access right for each user separately, the system administrator creates a generalized role RN_g with access rights AL_g *where* $AL_g = \cap\{AL_{1 \ldots n}\}$. Thereafter, a user acting in role RN_i, $(1 \leq i \leq n)$ who wishes to exercise a right in AL_g derives the right from the relationship between RN_i and RN_g. For example, in Figure 4.2, the medical specialists share the right to write in a patient file. An anesthesiologist infers the authorization to write in the medical record through the association between the role "anesthesiologist" and the role "physician."

Figure 4.2
Inheritance and hierarchical ordering of roles



Subjects may assume only a single role at any one time. Roles may not be combined to yield a greater set of rights. The distinction between inferring rights and combining roles is often subtle. Inference is defined by the hierarchical relationship between roles. However, such a relationship is not always present. Equivalence classes where no one role dominates any other is one such instance. In Figure 4.2, inference corresponds to the relationship between each respective specialty and the general role titled "physician." Combining roles would correspond to an anesthesiologist attempting to simultaneously attempt to perform as a pathologist or an orthopedic surgeon.

Role-based access control is really no more than an extension of traditional DAC (discretionary access control). First, DAC is often defined simply as anything that is not traditional MAC. [McC90] Second, it is important to recognize that roles are really just another representation of the conventional access control construct called a *group*. As with groups, roles are a way of combing users with equivalent rights, thereby simplifying the administration of security. [NYA93] Recognizing that role-based access control is simply a variant of DAC, this chapter next addresses some advantages of role-based access control.

4.5 Why use role-based access control

There are at least two reasons to consider role-based access control in the patient record environment. First, role-based access control can, to varying degrees, mitigate many of the weaknesses of DAC and MAC (discretionary and mandatory access control) noted earlier:

First, role-based access control simplifies the management of security constraints. System administrators have two levels for managing and tailoring access to user requirements by designating what roles a user may assume and limiting what rights a particular role may exercise. [NYA93]

Roles also offer some relief from possible syntactic and semantic differences between constituents in the federation. "[Roles] permit the identification and development of security controls specific to user's data access functions required for the applications tasks." [TIN88] Focusing on users and the roles shifts the focus away from individual, participating systems to the overarching federation. The federation, in turn, provides a common framework from which to formulate constraints. [MOR92]

Third, roles limit inference attacks in at least two ways. Roles are independent of users and so can be defined and managed across the federation more easily. Because access rights are bound to roles, a user, under the constraints of a single role, could not derive confidential information by making independent queries to separate systems. The use of predicates in role-based access controls are another method for limiting inference attacks related to aggregations or sums. For example, hospital administrators may need access to aggregate figures for internal purposes. If the number of data points is too small, however, an administrator can isolate and infer individual figures based upon the aggregate. [LIN92; TIN90]

Fourth, role-based access controls can prevent some classes of Trojan Horse attacks. To the degree that users are constrained by the privileges of a particular role, users may not assume multiple roles simultaneously, and roles may not grant access rights except in limited circumstances (such as the role of the system administrator), role-based access controls can be configured to limit the effects of a Trojan Horse attack much as MAC does. [THO91]

Fifth, roles make it possible to conceptually divorce the creator of the stored object from the data contained in the stored object. In DAC, by default, the creator of an object has discretionary authority over who may have access to the object. Separating the two more accurately reflects the social environment, however. For example, admitting clerks initialize the medical record, but each medical record is about individual patients and it is not clear whether patients or clerks should control the record. [OTA93]

Sixth, no ordering on subjects or objects is implied or assumed in a role-based access control scheme. As with the distinction between creators of information objects and the individuals about whom data in the objects is about, the lack of an enforced order permits role-based access control schemes to be much more flexible in how they adapt to the social environment.

A second, and perhaps more important, reason to consider role-based access control is its ability to adapt information security constraints to the dynamic, social environment of a health care federation.

The importance of tailoring security constraints to the user community cannot be overemphasized. Szolovits [SZO94] recounts the story of an experimental system installed in a large, Massachusetts teaching hospital for prescribing medications electronically. Because the system so interfered with the daily workflow by requiring internists to have prescriptions counter-signed by attending physicians in certain circumstances, the system was removed within days. Shortliffe et. al. also make the point that because they were too dogmatic and inflexible, several extremely promising systems are no longer in use. [SHO90] Role-based access control integrates well into most organizations because roles are a typical means for classifying employee duties. [CAS92]

4.6 Role based access control and the CPR

To apply role based access control in support of a security policy for computerized patient records (CPRs), the respective sets of subjects, objects, access modes and predicates must first be specified. Next, roles are defined in terms of $<o, m, p>$ tuples. Finally, subjects are assigned to roles. Throughout the entire process runs the common thread that the CPR defines both a social and a dynamic environment. Accordingly, roles should provide security without interrupting the flow of information or the delivery of care.

Although subjects are simply the individuals who use the information system, the objects accessed by those subjects are not so easily isolated. Simply equating an object $o \in O$ to a stored object such as a file does not appear to provide the granularity of control necessary to support the uses in Chapter 2 while meeting the security objectives related to disclosure and inference. Instead, govern access based upon content. [WIS90]

For every user and every use, there exists a different way of dividing the record. Researchers may want all observations relevant to the administration of a particular drug. Insurance evaluators may wish to have all of the information relevant to a specific claim including current care and previous treatment(s) for related events. For utilization review, all of the procedures corresponding to a particular visit or to treatment for a specific complications might be relevant.

Access modes and the predicates that modify them determine whether and how users may access and modify the record.[40] In the broadest sense, users may read from or write to the record. Finer degrees of control might permit some users to overwrite existing data, limit others to write-once, or enable computer matching across records.

The users and uses of the record listed in Chapter 2 correspond to different roles that are definable for the computerized patient record. The challenge is not necessarily to identify all of the roles that exist but to recognize that just because information technologies enable the enforcement of fine distinctions between different roles does not mean that system administrators should enforce all of those distinctions. For example, although, in principal, there is a very real difference with respect to access rights between a primary and a consulting physician, in practice, there may be no difference at all. [HU93; GRI91] The effects of tighter security constraints must be weighed against the potential impacts on the social, dynamic environment of the CPR community:

First, to some degree, a trade-off exists between the number of roles and the response time. Increasing the number of roles to which a user might belong and the

[40]Access modes and the predicates that modify them are also critical components of integrity constraints. Access modes can support integrity by limiting record modification to well-understood transactions. [CLA87]

permissions that correspond to each role creates more work for the federated system every time a user attempts to access information or perform a data operation. Efficiency declines.[41] The performance degradation could ultimately overshadow the motivation for using information technologies to streamline the delivery of care.

Second, and perhaps more serious, is the effect on workflow. Although information technologies can support the strict enforcement of security constraints, doing so could significantly decrease productivity, at least in the short term. Fine distinctions between users could preclude common practices such as "filling in for someone who is ill" or temporarily trading-off duties. [BRY91].

Third, as noted earlier, confidentiality constraints in the medical environment are further complicated by the understanding that patient care and safety are paramount. In a medical emergency, disclosure rights are waived to ensure that care givers have access to all of the critical, clinical information. [HAM92a; HAM92b]

4.7 Limitations of role-based access control

Despite its adaptability, role-based access control is not a complete answer to the vulnerabilities originally introduced in Chapter 2. The technology is not without its shortcomings:

Although it provides some relief, role-based access control is still vulnerable to semantic differences between participants in the federation. Two federation members may use the same role name RN_n but ascribe different sets of access rights to that name. Primary users may have different rights in Institution A than in Institution B.

Differences in how roles are defined are one factor that limits the ability of role-based access to control inferences. A second factor is the reality that most users will likely be authorized to assume multiple roles. Although a user may only act in a single

[41] Faster processors and more efficient access control implementations have made response time less of a limiting factor.

role at any given time, there is nothing to prevent someone from making inferences off-line, beyond the scope of the computer system.

Just as risks from unauthorized inferences are not wholly prevented, neither are the threats from Trojan Horse attacks eliminated. Although subjects do not have discretionary authority, some roles may have limited authority to grant rights to other roles. The ability of role-based access to constrain Trojan Horse attacks will range along a continuum from DAC to MAC depending upon the rigidity of role definition.

The tremendous flexibility of roles can also obfuscate rather than simplify the management of access rights. Because a partial ordering on roles is not required, use of practices like inferring rights to minimize administrative overhead can result in cycles that complicate rather than clarify the security administrator's duties.

Perhaps the greatest limitation of role-based access controls, as with any access control scheme, is its inability to extend control beyond the system boundaries. Once information is transferred to a participating constituent in the federation, the autonomy of each federation member and the absence of a single, monolithic security authority prevents the sender from using technical mechanisms to enforce particular constraints upon the recipient.

In a general sense, the limitations of role-based access control merely reinforce the fact that technology, in and of itself, is not a complete solution. Instead, technology must work in concert with both physical and procedural measures to satisfy the desired security objectives.

With respect to the specific threats facing the patient record environment, the limitations of role-based access control require procedural support to control redistribution and inference. At the limit, role-based access control cannot enforce constraints beyond system boundaries. As a consequence, other measures are required to contain the potential harm from those who draw inferences from information stored within their biological memory or redistribute physical copies of information.

Chapter Five

Recommendations

This chapter draws upon the earlier discussions about security policy and access control to outline a strategy for reducing the risk of disclosure and inference related threats to the confidentiality of individually identifiable patient information in a federated environment. After reviewing the general principles of the strategy, recommended measures at the Federal, state and institutional levels are presented.

The strategy calls for a combination of access and use controls applied uniformly across all of the states. Despite the apparent conflict between instituting a uniform security policy and preserving the autonomy of federation participants, the general strategy consists of a single, consistent security policy that divides responsibilities among the Federal and state governments and individual institutions.

Although new vulnerabilities introduced by automation are reflected in the policy language, the general strategy divorces the security policy from specific technologies. The premise for doing so is the recognition that the policy should remain as flexible as possible in the face of rapidly evolving technologies.

5.1 At the Federal level

The elements of the security policy at the Federal level satisfy the need for a uniform policy. In particular, at the Federal level, the policy explicitly defines the conditions for disclosure of identifiable patient information without the subject's consent by indicating who (which users) may have access to what information (which portions of the record) for what purpose (what may the users do with the information they collect or receive). As noted earlier, security policy at the Federal level attempts to avoid references to specific technologies.

Recommendation F1: Use preemptive Federal legislation to impose a uniform security policy to protect automated records.

As described in Chapter 3, the need for preemptive Federal legislation stems from the inadequacy of the current patchwork of state and Federal protection:

> Confidentiality obligations are not uniform from state to state, and they often vary widely and sometimes conflict within the same state. If confidential data are transmitted across state lines, it is sometimes unclear which state's confidentiality laws apply and which state's courts have jurisdiction if there is a dispute. [BRO93, 42]

To satisfy the need for some degree of uniformity, the Federal government would most likely rely upon the Interstate Commerce Clause of the Constitution of the United States. [HR4077] As a consequence, the security policy must limit itself to the health care context. Although other information that routinely crosses state boundaries could also be folded into the scope of these recommendations, such a discussion is beyond the scope of this thesis.[42]

[42]Consumer credit histories are an example of other types of information that have qualified for uniform Federal protection under the Interstate Commerce Clause. Preemptive Federal legislation could also be justified (although probably not in the case of patient records) in the context of national security.

Recommendation F2: Explicitly note that protection is afforded to the information and not to the record holder.

A second dimension of uniformity is the need to explicitly note that confidentiality restrictions apply to the information rather than to the record holder. "[C]urrent state protections often apply duties of confidentiality to the recordkeeper (e.g., the hospital) ...." [IOM94, S13] Disclosure is not regulated beyond the provider's control. By making confidentiality restrictions a property of the data itself, recipients of sensitive medical information are equally bound to protect against disclosure and inference related confidentiality violations.

*Recommendation F3: Explicitly note each **use** for which disclosure of individually identifiable patient information is permissible without specific patient authorization.*

As reviewed in Chapter 3 and in Appendix A, there are legitimate reasons for disclosure of individually identifiable patient information without patient authorization. However, a policy at the Federal level that approves the disclosure of identifiable patient information without that patient's authorization should do so in terms of use rather than attempting to identify specific users, user roles, or portions of the record. The federal level is too broad and general for identifying specific users or portions of the record for at least two reasons.

First, autonomy within the federation yields semantic heterogeneities. Different institutions may operationally define the same role with non-identical sets of access rights. Alternatively, institutions might use different standards for assigning users to roles. In either case, the same user, seeking the same data, for the same reason, may receive different privileges from two different institutions.

Second, limiting disclosure and inference related threats requires content based access controls to ensure that potentially sensitive data that is irrelevant to the purpose at hand is not unnecessarily disclosed. However, there are innumerable ways of sub-

dividing data in the medical record – too many to specify explicitly in legislation or administrative guidelines.

While interpreting a particular use may also be subject to some ambiguity, when combined with roles and a record divided in some consistent manner (as would be required at the institutional level), use provides more nuanced control of confidentiality.

Recommendation F4: Limit the disclosure of identifiable patient information without patient authorization to that which is required for the approved use.

Releasing unnecessary amounts of data magnifies the threat from inference and aggregation. Consequently, if the patient's authorization has not been obtained, the amount of information disclosed should be limited to that which is necessary for the given purpose.

Admittedly, there is a great deal of ambiguity in determining how much information is *necessary* for a given purpose. Moreover, whether a particular datum is relevant or not may also depend upon the individual who made the notation (e.g., the specificity and scope of a comment in the progress note).

Recommendation F5: Limit the use of identifiable information disclosed without patient authorization to the purpose(s) for which it was collected or received and require the prompt return, destruction, or removal of identifiers of said information.

Use is arguably the most critical of the constraints that may be placed at the Federal level. Because of the uniquely personal nature of medical information, there is some amount of harm inherent from any unauthorized disclosure. However, most quantifiable harm derives from the many possible unauthorized uses to which information may be applied.[43]

---

[43]See OTA93, GOS93 and ALP93 for numerous anecdotes on the quantifiable harms to individuals from unauthorized inferences or discloures of information.

There is an important distinction between restricting use to the purpose(s) for which information was collected or received and restricting use to legitimate purpose(s). As elaborated upon in Appendix A, there are legitimate uses for confidential information without patient consent. However, without consent, information should only be released for specified purposes. Therefore to complement the disclosure condition, identifiable information should only be kept (or remain identifiable) as long as that initial purpose warrants. Otherwise, data could be saved and "re-used" at a later date.

Researchers or other users who might benefit from maintaining records over time could do so after removing identifiers. The need to associate data belonging to a single patient collected over time (e.g., a longitudinal record) could be met by attaching anonymous identifiers. The list matching patients to anonymous identifiers would be stored in a separate location and maintained independently of the data.

By making restrictions a property of the data rather than of the recordkeeper, it is possible to argue that permitting the recipient to store and "re-use" data without authorization at a later date is no longer problematic. However, doing so may not be advisable for data consistency reasons independent of confidentiality.

Moreover, while important in principal, use restrictions are currently virtually impossible to enforce. For example, it is difficult to mandate that a user may not aggregate information stored within their personal, human memory over time. Therefore, permitting recipients to unnecessarily store identifiable patient information in the expectation that it may have some use at a later date is not acceptable.

Recommendation F6: Specify what constitutes a valid patient authorization.

This thesis addresses issues related to unauthorized disclosure and use of the patient record. However, the definition of what constitutes a valid patient authorization (e.g., is oral approval sufficient? must the patient sign a formal, written statement) is crucial because doing so establishes the scope of the earlier recommendations. In

particular, the above recommendations apply to any use or disclosure of information that has not satisfied the explicit conditions of a valid authorization.

Recommendation F7: Avoid references to specific technologies.

As discussed in Chapters 1 and 4, technologies can support many aspects of security policy. However, as with semantic heterogeneities, autonomy within a federation also results in syntactic heterogeneities. The array of technologies from which a federation member may construct an information system is extended by legacy systems and the evolution of technologies over time. Technologies may also exacerbate or mitigate particular threats, but the underlying objectives and the policy of limiting how much information a particular individual receives for a specific purpose persist.

Recommendation F8: Impose joint and several civil and criminal sanctions against violators.

A primary problem with confidentiality is that confidentiality is a zero-sum game. Once sensitive information, is disclosed or inferred, that information is extremely difficult to recapture. Consequently, it is better to rely upon deterrence and prevention rather than to attempt *ex post* corrective measures.

The judicial system is a forum for redressing real and perceived damages. However, a combination of civil and criminal penalties could also serve as a deterrent to would-be violators who might consider unauthorized disclosure for personal gain. The additional stipulation of joint and several liability extends responsibility from individuals to the institutions that gather, maintain and distribute information. Extending penalties to the institutions serves as an incentive to federation members which might otherwise be unwilling to invest in ensuring the security of computerized patient records (CPRs).

Legal recourse suffers from at least two drawbacks. First, initiating legal action to redress a real or suspected violation of confidentiality requires a violation of

confidentiality. [WPR93; IOM94] Potentially all of a plaintiff's sensitive medical data, even elements of the record not named in the suit, could be subpoenaed and placed in the public record. Second, to initiate legal action, the subject must first know that a violation has occurred. An individual may never know that a loan was denied or a promotion withheld as a result of information contained in their health record. [WPR93; IOM94]

5.2 At the state level

The general strategy at the state level is to fill the middle ground between the need for uniformity satisfied at the Federal level and implementation specific policies and technologies at the institutional level.

Recommendation S1: Do not expand or contract the scope of Federal legislation.

Although the use of "preemptive" Federal legislation implies the override of state policy, this recommendation explicitly notes that states should not have the authority to exceed either the floor or the ceiling on confidentiality established by security policy at the Federal level. Although this statement ventures into the realm of federalism which is beyond the scope of this thesis, this recommendation is justified by the need for consistent policy to facilitate confidentiality protection.

To provide consistent security, the need to prohibit the states from permitting weaker confidentiality restrictions than those imposed at the Federal level seems intuitive. Preventing more restrictive state action is equally important, however. Health records (as defined in Chapter 2) of residents within a state with more restrictive boundaries would likely be incomplete. Sharing records generated within the state would either expose the record to the less restrictive regulations of the federation or, if the federation attempted to honor the restrictions, result in the patchwork of regulations that exists in the status quo today.

5.3 At the institutional level

Institutions act as gatekeepers to individuals seeking access to data within the computerized patient record federation. "Because the nature of any inquiry is determined by its purpose, the kind of information involved and the requesting party, the policy of the health care institution should be the final outcome of assessing these factors." [BRC84, 24] Consequently, implementation specific policies and technologies are reserved for the individual institutions participating in the federation.

Recommendation I1: Identify the users of the information.

Patients who are the subject of a health record access information through a medical institution. Insurance claims evaluators access federation data through a payer institution. By first identifying each user and subsequently assigning a role(s) to each user, the institution manages the flow of information across the institution.

Recommendation I2: Identify legitimate uses of the information.

A second element of the gatekeeper's responsibility is to identify legitimate uses of the information. By limiting the uses of information, data release is confined to legitimate purposes.[44] To the degree that use restrictions are enforceable, the potential harm incurred from even unauthorized disclosures may be minimized.

Recommendation I3: Define the set of access rights.

Defining access rights is critical to regulating disclosure As one example, institutions can limit disclosure by prohibiting users with read-only access from copying data. For paper records, this restriction might correspond to photocopying. In an electronic environment, a prohibition against copying might prevent users from reading one file and writing to a different file.

[44]Unfortunately, as with any situation, even legitimate use can have unintended side effects or negative repercussions for the subject of health information. Legal proceedings are one example.

When modified by predicates, access rights can also reduce the risks of inference and aggregation. For example, a predicate might require a set of at least x patient files in order to perform data aggregations.

Finally, for disclosure purposes, access restrictions such as write-once and write-only ensure the record's admissibility as evidence in a court of law. [HAM92a; GRA93] Access restrictions ensure admissibility because they preclude unauthorized modification of patient files.

Recommendation I4: Determine what objects are shared with the federation.

As discussed in Chapter 2, a fundamental part of federation participation is for members to determine how much data they would like to share with other members of the federation. This may be specified in two ways.

First, members can explicitly divide the record in one or more ways and define a clear set of rules delineating what is shared. For example, the record could be divided chronologically and any information less than three years old is shared. Alternatively, the record could be divided based by subject such as patient directory information, laboratory test results, progress notes, etc. A medical laboratory information system might be limited to accessing laboratory test results and patient directory information.

However, explicitly dividing the record provides a coarse granularity of control. Different access requests divide the record in different ways. Attempting to account for every request and every record division *a priori* is hopelessly complex. A second strategy might be to define a set of rules for negotiating what information may or may not be shared in real-time. When one member requests information from another, a query-response process is automatically invoked to determine the legitimacy of the request and the scope of the subsequent disclosure. [HEM85; ALO91; McC94] Negotiation in real-time is a subject of current research on federations.

Recommendation I5: Confine users to exercising a single role at any one time.

Many users will interact with the federation in more than one role. For example, many physicians also conduct medical research, review cases for medical claims evaluators, or serve as expert witnesses in legal proceedings. Because of the danger of misuse, users should never be permitted to access data through more than one role simultaneously. Roles do not aggregate. Cross-over is not allowed.

Admittedly, there is a trade-off in perceived convenience versus security that might seem overly restrictive. However, while most individuals do perform multiple tasks at once, the hypothesis is that users tend to do so in a single context. For example, physicians who are also researchers would not simultaneously see patients and work on a research problem.[45] This is a subject for further investigation.

Recommendation I6: Formalize disciplinary proceedings to respond to confidentiality violations.

Each institution acts as a gatekeeper. Therefore, independently of civil or criminal sanctions, each institution should take steps to ensure that confidentiality violations across the federation do not occur through that institution. Education, warnings and dismissal are all tools that the institution might wield.

[45]Clinical research defines a gray area in this example. However, the contention is that even in clinical research, when treating a patient, the patient physician relationship is defined only in the context of patient care. Data is analyzed separately.

Conclusion

This thesis has reviewed both policies and technologies to address the security of computerized patient records (CPRs). The concept of a federation is presented as a model for the automated health records. The model supports multiple institutions, each with different users and uses, which retrieve data from a composite record that consists of information shared between each of the federation members.

Based upon this model, redisclosure, over-disclosure, inference and aggregation are identified as specific threats to the confidentiality of the CPR that arise from sharing data across a federation. From the threats, a set of security objectives emerges. Existing, proposed and pending legislation and guidelines that address confidentiality of CPRs are surveyed; traditional access control policies are reviewed.

This thesis concludes that the protection afforded by existing, proposed and pending efforts is incomplete. Each policy merely adds another layer to the inconsistent patchwork of regulations and tenets that already exists to support confidentiality. Traditional access control measures are also not well suited to the characteristics of a CPR federation. Traditional measures rely upon support that does not exist in a federation and are either too permissive or too inflexible.

Elements of a security policy that might better address disclosure and inference related threats to patient record confidentiality are presented as a series of recommendations. Separate recommendations are drafted for the Federal government, the states and the individual institutions such as hospitals, payers and social services agencies who wish to share the data in the CPR.

Role-based access control is introduced as a better alternative for supporting disclosure and inference related threats to the confidentiality of the CPR. The recommendations are intentionally phrased to facilitate role-based access controls as a logical mechanism to support policy implementation.

There are several limitations to this analysis, however. In particular, the initial assumption of a federated model may affect the applicability of the conclusions. There are also many policy related and technology related issues that remain untouched and are areas for future work.

A federation is only one possible model for the CPR. Perhaps most notable as an alternative is the health data organization (HDO) or regional repository as proposed in The White House Domestic Policy Council's Health Security Act legislation. [HR3600] Although many of the issues they discussed addressed the computerization of health records in general, the Institute of Medicine's 1994 report entitled *Health Data in the Information Age: Use, Disclosure, and Privacy* was directed specifically at HDOs.

With respect to security policy, three significant issues stand out. First, the scope of the policies considered, while broad, omits many significant players. In particular, many professional and peer review organizations are not included. The American Medical Association (AMA) and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) are two. Moreover, the final recommendations do not address the significant role that these institutions play in the CPR federation.

The breadth of policies compared could also be widened to include the global community. As transportation and information technologies continue to eliminate

physical and cultural barriers between nations, healthcare information will follow populations in flowing across borders. The role of individuals has also not been addressed. What can be said about the behavior and responsibilities of specific users?

Aside from automation, health care policy reform has introduced many other principles that may impact confidentiality. The proposal to introduce a uniform patient identifier is one.

Federalism is also not discussed. The recommendations separate Federal activities from state actives. While preemptive Federal legislation may better satisfy confidentiality concerns, the implications for the Constitutional division between the Federal and state governments is unclear.

With respect to technology, there are four significant limitations to the analysis. First, several crucial dimensions of the technology are simply assumed. Communications security and operating system support for identification, authentication and other technologies to support networked use of computerized patient records are potentially significant tools for enhancing the security of CPRs. Patient health cards is another. Independent of health care reform, information security is an Administration priority with respect to the developing information infrastructure. How application level information security dovetails with lower level security mechanisms with respect to the overarching information infrastructure is an area for research.

A second limitation of the technical analysis is that no benchmarks for evaluating access controls are presented. Many qualitative reasons for adopting role-based access controls are advanced. However, quantitative measures such as response time are not discussed in the evaluation of role-based access control versus mandatory and discretionary access control.

Third, existing work in the area of role-based access control or health information security is not surveyed. Researchers have been exploring application level health

information security issues and role-based access control in particular for a number of years. While this body of literature is referenced, a literature review would be helpful.

Even if all of the limitations noted above were accounted for, the conclusions would still be tempered by the fact that, in a shared environment, information security is impossible to guarantee. This is due, at least in part, to the tradeoff between security and convenience. Even procedural measures such as education are expensive in terms of lost time and perceived decreases in efficiency due to security measures that alter workflow. [NRC91] Moreover, human error will always exist as a vulnerability. [CEC93] The tradeoff is then complete security without any of the advantages of information sharing.

While being questioned by the authorities, Dr. Kimball's classmate, colleague and betrayer said of Dr. Kimball, "You'll never catch him. He's simply too smart for you." Many security threats are impossible to prevent outright. There will always be those who, like Dr. Kimball, are too smart to catch. However, a well-balanced security policy that distributes responsibility across many levels and is supported by role-based access controls may prevent many unwanted "fugitives" from finding out too much about you.

Appendix A

This appendix compares and contrasts existing, proposed, and pending policy alternatives for providing information security. The analysis focuses on selected elements of 10 policies related to disclosure and inference related threats to the confidentiality of individually identifiable health care information. Disclosure of information within an institution or sharing non-identifiable information between institutions is not a part of this analysis. 'Institution' is used in this context as the user community of information systems administered by the same central authority.

A.1 Methodology

Analysis proceeds by way of tables. Each column of the table represents one of the 10 policies listed in Table A.1. Each row of the table is numbered and delineates a policy parameter. A description of the parameters follows each table. Policy parameters are expressed as questions (e.g., Does the policy apply only to Federal agencies?). The intersection of a row and a column is called a table cell. Table cells list section numbers of the respective document except in the case of the AHA where no section numbers are provided and a "Y" signifies that the characteristic holds. An empty table cell is interpreted as a "No" to the question posed in the corresponding row.

Table A.1
Policies surveyed

1974	The Privacy Act of 1974
1987	The Computer Security Act of 1987
AHIMA	American Hospital Association Information Management Advisory on the Disclosure of Medical Record Information
AHA	American Health Information Management Association Health Information Model Legislation Language
WEDI	Workgroup on Electronic Data Interchange Model Federal Legislation for the Confidentiality of Health Care Information
NY	Medical Society of the State of New York Ethical Tenets for Protection of Confidential Clinical Data
MT	State of Montana Uniform Health Care Information Act
MA	Massachusetts State Code on Insurance Information and Privacy Protection
HR4077	The Fair Health Information Practices Act of 1994, HR4077
HR3600	The Health Security Act of 1994, HR3600

A.2 Scope

The first step of the analysis is to address the question of scope. What is the breadth of subjects covered by each of the surveyed policies?

(1) *Federal agencies only.* Does the policy apply to Federal agencies only?

(2) *Health information only.* In this information age, an entire industry has emerged around the collection and resale of information. There is a great deal of individually identifiable information that may warrant protection in addition to health information (e.g., credit data). Does the policy address health information only or other individually identifiable information as well?

(3) *Electronically stored/transmitted data only.* Many of the threats to information security have long existed and are not unique to the electronic storage media. Does the policy apply only to electronic data or to any medium?

(4) *Disclosure without the record subject's authorization.* The assumption is that individuals should have control over the use and disclosure of information about themselves. There may be some limits to this right, however. Does the policy make provisions for disclosure without the record's subject authorization?

(5) *Storage institution bears security responsibility.* Who is responsible for the confidentiality of the record? Traditionally, the recordkeeper or storage institution is responsible for safeguarding the information within their sphere of influence.

(6) *Responsibility extends in-kind to all recipients.* In some instances, responsibility for safeguarding information is a property of the data and not a property of the recordkeeper. In such a case, the recipient inherits the responsibility to safeguard as well as the right to use the information received.

(7) *Responsibility in-kind to Federal recipients.* In the case of Federal legislation, it may only be possible to impose a responsibility to safeguard information on Federal entities.

(8) *Responsibility in-king limited to medical institutions.* Some policies that focus explicitly on health information may elect to focus solely on the medical institutions that produce the health data. In such an instance, separate policies would be required to address the confidentiality of information disclosed to non-health care institutions.

Table A.2.
Scope

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)	(a)(1,8)	2(a)	a				b	c		
(2)			Y	103(a)	2A	P6	504		2b	16(a)
(3)		2(b)1			2A	P6				
(4)	(b)		Y	105	6D		529		Part 2	
(5)	(e)		Y	105(b)		8	511			
(6)			Y	103(a)	2A				3B3	16(a)
(7)	d									
(8)							504			

[a] This policy does not apply to any Federal agency.
[b] This is state legislation and does not apply to Federal agencies.
[c] This is state legislation and does not apply to Federal agencies.
[d] See sections (a) and (o)(1)(h). Explicit prohibitions on redisclosure suggest that, at least in the case of computer matching, responsibility does not necessarily transfer in-kind to all recipients.

A.3 Preemption

Given their intended scope, several of the proposed or pending policies will have a significant impact on the distribution of authority between the Federal and state governments.

(1) *Supersedes all relevant state legislation.* Is all state authority superseded with respect to the scope of the policy as defined in Table A.1?

(2) *Supersedes specific state legislation.* To limit encroachment upon state's rights, some policies carefully define the boundaries of preemption.

(3) *Does not interfere with state legislation.* Some policies may go so far as to note explicitly that in specified conflicts between state and Federal policy, the state prevails.

Table A.3
Preemption

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)										
(2)	(a)12			e	2C					f
(3)				304						

[f] See section 16(a). Preemption is implied but not explicitly mandated.

A.4 Disclosure without patient authorization

Disclosure for specific uses without patient authorization is summarized in this table. Subsequent tables will elaborate on each of the users and uses listed below.

(1) *State or Federal public policy interest.* Are there public policy interests that warrant disclosure to a state or Federal official without authorization?

(2) *Family member, close friend.* How is disclosure by or to a family member regarded? Do family members have a compelling interest to warrant disclosure without authorization?

(3) *Audit/accreditation purposes.* May information be disclosed for audit or accreditation activities without consent?

(4) *Patient management.* May administrators use identifiable patient information without consent for patient management activities?

(5) *Judicial proceedings and law enforcement.*

(6) *Employer evaluations.* May employers use identifiable patient information in the employer-employee relationship?

(7) *Reimbursement of medical care.*

(8) *Provision of medical care.* May information be disclosed to a provider who seeks to provide care to the patient?

(9) *Education.*

(10) *Research.*

(11) *Archival purposes.*

(12) *Maintenance.* May employees or contractors to the recordkeeping institution access identifiable records in the course of their normal duties?

(13) *Transfer of recordkeeper.* Over the course of time, record-keeping institutions may exit the health records market requiring a new entity to assume control of the identifiable health data.

(14) *Routine use.*[g]

Table A.4
Disclosure without patient authorization

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)	(b)(1,2)		Y	105(h)	6D7	h	530(2)	13(6)	125	
(2)				105(f)	6D5		529(4)		124a	
(3)	(b)(4)[i]		Y	105(i)	6D8			13(4)	123a3	
(4)			Y	105(i)			529(2)			
(5)	(b)(7)		Y	108[j]	6D11		530	13(6)	127	
(6)			Y							
(7)			Y		k		529(2)	13(2)	123a2	
(8)			Y	105(d)	6D3		529(1)		123a1	
(9)							529(2)			
(10)	l		Y	105(j)	6D9		529(6)	13(9)	128	
(11)	(b)(6)									
(12)			Y	105(c)	6D2			13(2)		
(13)				105(g)	6D6		529(5)	13(10)		
(14)	(b)(3)									

[g] 'Routine use' is defined here to mean any use which is defined in the Federal register or is a standard relationship (such as between a payer and a provider) that any patient would reasonably expect.
[h] See sections 7, 8, 10 and 16.
[i] Includes the General Accounting Office (GAO) and the Census Bureau. See also (b)(10).
[j] See also 105(l, m).
[k] Payers [sic] are not included as an "external disclosure". This point is further elaborated upon in subsequent tables.

A.5 Disclosure without authorization for a public policy interest

In the next several sections, the analysis examines, more closely, conditions for disclosure without the consent of the record subject.

(1) *Public health interest.* Public health interests include disclosure for communicable diseases, etc.

(2) *Public policy interest.* Public policy interests include reporting of births and deaths as well as stabbings, shootings, suspected child abuse, domestic violence, etc.

(3) *Public policy interest.* Public policy interests also include disclosure if there is any reasonable suspicion that failure to disclose could cause harm to any individual including the patient.

Table A.5
Disclosure without authorization for a public policy interest

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)			Y	105(h)2	6D7a		530(2)		125a	
(2)			Y	105(h)1	6D7b		530(4)		125a	
(3)	(b)(8)		Y	105(e)	6D4				126	

A.6 Disclosure without authorization to a family member or close friend

(1) *Disclosure by a family member.* In some instances, the patient's family members and not representatives of the recordkeeping institution will disclose information.

(2) *Well-being.* In many instances, disclosure to the family is a significant element of care and is important for the patient's overall well-being.

Table A.6
Disclosure without authorization to a family member or close friend

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)				105(b)	6D1					
(2)				105(f)	6D5		529(4)		124a	

A.7 Disclosure without authorization for audit or accreditation

(1) *Limit duration of disclosure ex ante.* Authorize disclosure without patient consent for only a fixed time period.

(2) *Require information to be destroyed upon completion of use.* If information must be destroyed, the recipient cannot archive the information for later use.

(3) *Require information to be stripped of identifiers upon completion.* This is much less restrictive than (2). Recipients may retain the data, perhaps for epidemiological studies that do not require patient identification.

(4) *Redistribution/publication is prohibited.* No report that utilizes identifiable patient information may be distributed or published.

(5) *Redistribution/publication is permitted as necessary.* In particular, audit is often used to detect fraud or abuse. Publication of identifiable data is permitted to the extent that the audit may be carried to completion. Prosecution that arises as a result of the audit justifies further disclosure.

Table A.7
Disclosure without authorization for audit or accreditation

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)								m		
(2)										
(3)				105(i)	6D8a		529(7)a			
(4)										
(5)				105(i)	6D8b		529(7)b			

[m] Disclosure without consent for audit purposes is permitted in section 13(4)(iii). However, conditions upon that disclosure are not discussed.

A.8 Disclosure without authorization for patient care management

In this context, patient care management may be taken to mean:

(1) *Utilization review.*

(2) *Performance review.*

(3) *Quality assurance.*

Table A.8
Disclosure without authorization for patient care management

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)			Y				n			
(2)			Y					13(15)		
(3)			Y					13(15)		

[n] Disclosure to medical administrators without consent is permitted in section 529(2). However, specific patient care management practices are not identified.

A.9 Disclosure without authorization for law enforcement

Judicial action may require access to identifiable health records for several reasons including:

(1) *Judicial action against the patient.* In most instances, medical records are considered privileged and receive consideration. However, in particular circumstances, as defined in the indicated sections, medical records may be used in legal action against the patient.

(2) *Judicial action against the provider.* In investigations of fraud, abuse, mis-use, etc. identifiable patient information may be necessary to form a case against the provider.

(3) *Response to warrant, subpoena, etc.*

(4) *Court-ordered examination of an individual.* Involuntary commitment proceedings are a specific example referred to in (1) where records may be used against the patient.

(5) *Identification of a deceased individual.*

Table A.9
Disclosure without authorization for law enforcement

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)				105(m)	6D10a				141	
(2)				108(a)7	6D10a		535(1)g		129a	
(3)	(b)7,11		Y	105(l)	6D11		530(3)	13(8)	130	
(4)				105(m)	6D12		535		127a4	
(5)				105(n)	6D13				127a5	

A.10 Disclosure without authorization for employer-employee evaluation

Because employers are increasingly being called upon to shoulder an increasing percentage of the health care burden, the employer's access to sensitive employee health data increases as well.

(1) *As a payer or provider only.* Because of the fear that employer's could use health information to discriminate against employers (e.g., use in hiring or firing decisions), many prefer that the employer's access be limited to reimbursement.

(2) *Preventative intervention.* Because employers have access to and control over an individual's work environment, employers are in a good position to identify potential problems and administer early intervention or preventative care.

(3) *Employment decision explicitly prohibited* Because of the fears raised in (1), some policies may wish to explicitly prohibit the use of sensitive health information for particular uses such as employment decisions.

Table A.10
Disclosure without authorization for employer-employee evaluation

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)					6C2				123a2	
(2)										
(3)										

Table A.11 Disclosure without authorization for reimbursement

In particular, disclosure for reimbursement purposes concerns disclosure to public and private insurers. Insurers, in turn, may have several uses for the data including:

(1) *Evaluate claims for reimbursement purposes.*

(2) *Preventative information.* As with employers, insurers may often be in a unique position to provide early warning of potential complications and to prescribe preventative intervention.

(3) *Decision to insure explicitly prohibited* As with employers, there is a real fear of abuse by insurers. Consequently, some policies may wish to explicitly prohibit certain uses.

Table A.11
Disclosure without authorization for reimbursement

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)							529(2)	13(4)i		
(2)								13(4)ii		
(3)										

A.12 Disclosure without authorization for providing patient care

(1) *Current care provider.*

(2) *Previous care provider.*

(3) *Pending care provider.*

Table A.12
Disclosure without authorization for providing patient care

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)			Y	105(d)	6D3		529(1)		123a1	
(2)							529(3)			
(3)										

A.13 Disclosure without authorization for education

(1) *Education.* While the use of identifiable patient information in the education of health care professionals is standard practice, controversy arises over the use of sensitive information without the consent of the patient. Is education sufficiently important to warrant disclosure without authorization?

Table A.13
Disclosure without authorization for education

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)							529(2)			

A.14 Disclosure without authorization for research

Medical research includes not only laboratory medicine but also clinical trials and the development of health care technologies. Regardless of the particular application, real patient data is a valuable input for producing meaningful results. To ensure adequate protection of confidentiality, however, several measures may be required.

(1) *Requires approval by an independent review board.* To provide oversight and to ensure against abuse, many institutions that approve use of identifiable information for research purposes without consent require the approval of an independent body of scientific peers. The board must determine whether the potential benefits of the research in question outweighs the patient privacy interest.

(2) *Pre-set time limit on duration of disclosure.* In some instances, use without authorization is only approved for a fixed amount of time.

(3) *Require information to be destroyed upon completion of use.* If information must be destroyed, the recipient cannot archive the information for later use.

(4) *Require information to be stripped of identifiers upon completion.* This is much less restrictive than (3). Recipients may retain the data, perhaps for epidemiological studies that do not require patient identification.

(5) *Redistribution/publication is prohibited.* Some policies might specify that, under no circumstances, may identifiable information be recirculated.

(6) *Redistribution/publication is permitted as necessary.* In some circumstances, if identifiable information is an integral part of the research and is required as part of the scientific process of knowledge dissemination, publication may be permitted.

(7) *Redistribution/publication requires sender's approval.* Some institutions may condition a research project's redisclosure as part of a publication etc. upon the sender institution's review. In this way, the sender attempts to continue to exercise responsibility for disclosure.

Table A.14
Disclosure without authorization for research

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)				105(j)1			529(6)		128a	
(2)										
(3)				105(j)1	6D9e				128b	
(4)				105(j)1	6D9e		529(6)e	13(9)ii	128b	
(5)				105(j)2						
(6)					6D9f		529(6)d			
(7)								13(9)iii		

A.15 Disclosure with a record subject's authorization

The definition of what constitutes a valid patient authorization (e.g., is oral approval sufficient? need the patient sign a formal, written statement) is crucial because doing so determines what constitutes a disclosure without authorization. In particular, any use or disclosure of information that does not satisfy specified conditions is unauthorized.

(1) *Physical document/signature is necessary.* Despite the movement towards electronic records, many state jurisdictions refuse to accept as a legal authorization, anything but a physical, signed document. [WED92; OTA93]

(2) *Physical document/signature is sufficient.* Recognizing the shift towards electronic documentation, many jurisdictions continue to accept physical documents but also recognize alternative forms of authorization.

(3) *Electronic record/signature is necessary.* Although electronic formats are not required as a standard anywhere, digital signatures may become the future norm.

(4) *Electronic record/signature is sufficient.* Many institutions and jurisdictions now accept electronic authorization as legal and binding.

(5) *Received prior to disclosure.* Must authorization be received prior to disclosure? As discussed further in Table A.16, may authorization be received *ex post*?

(6) *Authorization form must be separate and independent.* Some institutions use standard forms for authorization. In some cases, blanket authorization granting broad disclosure authority is incorporated or hidden within other forms. [MASS]

(7) *Name the individual whose data is being disclosed.* Must the authorization name the individual whose data is being disclosed? In some cases, authorization is not obtained from the patient as in the case of a minor or a patient who is incapacitated.

(8) *Identify the source of the data by name.* Must the authorization explicitly identify an institution for which the authorization is valid or does the authorization extend in-kind to any holder of the information?

(9) *Identify the source of the data in general.* Rather than explicitly naming an institution or individual, may the authorization grant authority by describing the disclosure?

(10) *Identify the recipient by name.* Must the authorization explicitly name the recipient? This may require explicitly noting the location to which the information is disclosed.

(11) *Identify the recipient in general.* May the authorization simply describe the recipient as in the case of granting disclosure to the insurance claims evaluator assigned to a particular claim?

(12) *Describe the information disclosed explicitly.* Must each item of information for which authorization is granted be identified explicitly?

(13) *Describe the information disclosed in general.* Recognizing that health care information may be divided in an infinite number of ways and is often difficult to specify, a general description of the information disclosed is often sufficient.

(14) *Describe the purpose of the disclosure explicitly.* Why is authorization for disclosure being requested?

(15) *Describe the purpose of the disclosure in general.* If the purpose of the disclosure is difficult to specify, is a general description of the use acceptable?

(16) *Pre-specify the duration of the disclosure.* For how long is the duration valid? Is there a fixed time limit or, if not, must the authorization explicitly state that there is no time limit?

(17) *Authorization record is kept.* Must each authorization be kept for some specified amount of time?

(18) *Authorization record is a permanent part of the data.* Does each authorization record become a permanent part of the patient health file?

(19) *Disclosure record is kept.* In addition to the authorization for disclosure, is a record of all disclosures kept?

(20) *Disclosure record is a permanent part of the data.* Does the disclosure log become a permanent part of the patient health file?

(21) *Revocation of authority.* May authorization be revoked once granted?

Table A.15
Disclosure with a record subject's authorization

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)	o		Y				525(1)	13(b)	122b1	
(2)				104(a)6	6C1f					
(3)										
(4)				104(a)6	6C1f					
(5)										
(6)									122b2	
(7)			Y	104(a)1	6C1a					
(8)										
(9)									122b3	
(10)			Y	104(a)3						
(11)					6C1c				122b4	
(12)			Y							
(13)				104(a)2	6C1b				122b6	
(14)			Y						122b5	
(15)				104(a)4	6C1d					
(16)				104(a)5	6C1e					
(17)					6C3				122h	
(18)					6C3				122h	
(19)					p				114a	
(20)				104(c)					114b	
(21)			Y	104(b)	6C2				122e	

[o] The requirements for authorization are specified for use in computer matching only.

[p] See section 6B. Disclosure to a payer is not part of this disclosure record. WEDI defines disclosure to a payer as within the scope of an 'institution' as defined for this appendix.

A.16 Requirements for auditing or recording disclosures

Regardless of whether or the patient has explicitly consented to the disclosure, most policies recommend some means for documenting the disclosure of records. From the perspective of disclosure and inference related confidentiality threats, a record of all disclosures is a preventative measure intended to deter attempts to access or use sensitive information for illegitimate purposes.

(1) *Note the date of the disclosure.* When did the disclosure occur?

(2) *Name the individual whose data is being disclosed.* What individual(s) are identified in the disclosure?

(3) *Identify the source of the data by name.* Knowing the source may be particularly important for maintaining consistency throughout all records on the same individual(s). As the record moves across the federation, the original source may become difficult to identify.

(4) *Identify the source of the data in general.* If the source cannot be explicitly named for whatever reason, can the source be described in general?

(5) *Identify the recipient by name.* Who received the individually identifiable record(s)?

(6) *Identify the recipient in general.* If the recipient is an institution or is unknown at the time of disclosure, must the recipient be described in general (e.g. as in the case of an insurance claims evaluator for a particular reimbursement request)?

(7) *Identify the location to where the disclosure was made.* Must the physical location to where the data was sent be explicitly noted in addition to identifying the recipient?

(8) *Describe the information disclosed explicitly.* Must each item of information which was disclosed be identified explicitly?

(9) *Describe the information disclosed in general.* Recognizing that health information may be divided in an infinite number of ways and may therefore be difficult to identify explicitly, is a general description of what was disclosed sufficient?

(10) *Describe the purpose of the disclosure explicitly.* Why was the information disclosed?

(11) *Describe the purpose of the disclosure if possible.* If a specific purpose is not identifiable, can the use be described in general terms?

(12) *Specify the duration of the disclosure.* In some instances, institutions may disclose information for a fixed period of time or release information subject to certain conditions. Once time has expired or the particular conditions have been satisfied, the authority for retaining information disclosed without patient authorization terminates.

(13) *Disclosure record is kept.* Must a log of all disclosures be kept for some specified amount of time?

(14) *Disclosure record is a permanent part of the data* Does the disclosure record become a permanent part of the patient file?

Table A.16
Requirements for auditing or recording disclosures

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)	(c)1a		Y				525(2)		114a1	
(2)			Y	103(b)						
(3)										
(4)										
(5)	(c)1b		Y	103(b)			525(2)		114a2	
(6)										
(7)									114a3	
(8)	q									
(9)	(c)(1)a		Y	103(b)			525(2)		114a4	
(10)	(o)(1)b			103(b)					114a1	
(11)	(c)(1)a									
(12)	(o)(1)f									
(13)	(c)(2)		Y		r		525(2)		114b	
(14)			Y	103(b)					114b	

[q] See section (o)(1)c. Subsections of section (o) relate to computer matching only.
[r] See section 6B15. Disclosure to a payer is not part of this disclosure record. WEDI defines disclosure to a payer as within the scope of an 'institution' as defined for this appendix.

A.17 Restrictions on inference or computer matching

While admittedly difficult to enforce, explicitly noting restrictions at least codifies the intention. Moreover, while existing technologies are limited in their ability to anticipate and constrain inference related activities, clearly setting forth the policy establishes guidelines for the technology to reach towards.

(1) *Requires approval by an independent review board.* Does the disclosure of information for computer matching purposes require the approval of an independent review board?

(2) *Limit use to reason for which data was collected.* Is information use limited the reason for which the data was originally collected? Note that this requirement does not state that patient consent is necessarily required.

(3) *Limit use to reason for which data was received.* In many policies, confidentiality obligations are not a characteristic of the information. Instead, responsibility is

ceded to the recordkeeper. In such instances, the policy must explicitly state the responsibilities of the receiver.

(4) *Limit use to purposes for which consent is obtained.* The distinction between (2) and (4) is that information can be archived and consent can be requested *ex post.* In (2), *ex post* use of archived information is not provided for.

(5) *Limit use to purposes for which consent is obtained ex ante.* (5) is a more formal variation of (2) and (4). The patient must authorize all uses *ex ante.*

(6) *Limit use to purposes for which consent is obtained ex post.* (6) is a more formal variation of (2) and (4). Explicit patient consent is still required, but consent may be obtained *ex post.*

(7) *Explicitly prohibit inference of AIDS or ARC.*[s] Some information such as drug and alcohol abuse and treatment program data is already explicitly protected by Federal law. Are there other categories of information which require explicit consideration?

Table A.17
Restrictions on inference or computer matching

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)	(o)(3)						529(2)a			
(2)				106(b)5		10	529(2)a	3,11,12	121a	
(3)						10		3,11,12	121a	
(4)					5B2			3,11,12		
(5)	(o)(3)					7,8,10				
(6)										
(7)								2,7(d)		

[s] AIDS (Acquired Immune Deficiency Syndrome); ARC (AIDS Related Complex).

A.18 Penalties for non-compliance

One of the greatest limitations of current policy is a lack of penalties to provide incentives for protecting security.

(1) Civil remedies specified.

(2) Civil penalties specified.

(3) Criminal penalties specified.

Table A.18
Penalties for non-compliance

	1974	1987	AHA	AHIMA	WEDI	NY	MT	MA	4077	3600
(1)	(g)(1)			110	11		553	18	161	t
(2)	(g)(2-4)			111	12		553	18	163	
(3)	(i)(1)			112	13		551		164	

[t] An intention to provide enforcement is stated in 16(b) but no enforcement is specified.

References

ADL92 Arthur D. Little, Inc. 1992. *Telecommunications: Can It Help Solve America's Health Care Problems?* Report no. 91810-98. July.

AHA90 American Hospital Association. 1990. *Management Advisory: Information Management on Disclosure of Medical Record Information.* Chicago, Illinois: American Hospital Association Publishing, Inc.

AHI93 American Health Information Management Association. 1993. *Health Information Model Legislation Language.* in Office of Technology Assessment. 1993. *Protecting Privacy in Computerized Medical Information.* OTA-TCT576. Washington, D.C.: Government Printing Office, (November).

ALO91 Alonso, R., D. Barbará and S. Cohn. 1991. Data Sharing in a Large Heterogeneous Environment. *Proceedings. 7th International Conference on Data Engineering.* Los Alamitos, California: IEEE Computer Society Press. 305-13.

ALP93 Alpert, S. 1993. Smart Card, Smarter Policy: Medical Records, Privacy, and Health Care Reform. *Hastings Center Report*, 13-23(November-December).

BIS90 Biskup, J. 1990. Protection of privacy and confidentiality in medical information systems: problems and guidelines. in *Database Security, III: Status and Prospects*, ed. D.L. Spooner and C. Landwehr. Amsterdam, Netherlands: North-Holland. 13-23.

BLA94 Blaustein, B.T., K.P. Smith, C.D. McCollum and L. Notargiacomo. 1994. Secure Data Sharing Among Collaborating Organizations. to appear in *Proceedings of the Concurrent Engineering Research and Applications Conference*, (August).

BLU91 Blum, B.I. 1991. Computer Security in a Clinical Environment. in *Database Security, IV Status and Prospects*, ed. S. Jajodia and C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 1-12.

BNA93 Bureau of National Affairs. 1993. *Health Care Electronic Data Report* 1068-3798/93. Washington, D.C.: Government Printing Office, (September 10).

BRA92 Brannigan, V.M. 1992. Protecting the Privacy of the Patient: Information in Clinical Networks: Regulatory Effectiveness Analysis. in *Annals of the New York Academy of Sciences,* ed. D.F. Parsons, C. Fleischer, and R.A. Greene, 670:190-201.

BRC84 Bruce, J.A.C. 1984. *Privacy and Confidentiality of Health Care Information.* Chicago, Illinois: American Hospital Publishing, Inc.

BRG92 Brüggemann, H.H. 1992. Rights in an Object-Oriented Environment. in *Database Security V. Status and Prospects*, ed. C.E. Landwehr and S. Jajodia. Amsterdam, Netherlands: North-Holland. 99-115.

BRN93 Brandt, M. 1993. Confidentiality Today: Where Do You Stand? *Journal of the American Health Informatics Association*, 64(12):59-61(December).

BRO93 Broccolo, B.M., D.K. Fulton and A. Waller. 1993. The Electronic Future of Health Information: Strategies for Coping with a Brave New World. *Journal of the American Health Informatics Association*, 64(12):38-51(December).

BRP93 Bruening, P.J. 1993. *Protecting Privacy in Computerized Medical Information.* Testimony before the House Information, Justice, Transportation, and Agriculture Subcommittee of the Committee on Government Operations. 103rd Cong., 1st sess., (November 4).

BRS94 Branstad, D. 1994. Working with the author. (January 4-21).

BRY91 Brynjolfsson, E. 1991. The Productivity of Information Technology: Review and Assessment. Center For Coordination Science Technical Report #130, Sloan School Working Paper #3417-92, Cambridge, Massachusetts: MIT Sloan School of Management.

CAS92 Castano, S. and P. Samarati. 1992. An Object-Oriented Security Model for Office Environments. *Proceedings of the IEEE 1992 International Carnahan Conference on Security Technology: Crime Countermeasures*, New York, NY: IEEE Press. 146-152.

CEC93 Commission of the European Communities. 1993. *Green Book on the Security of Information Systems*, DRAFT 3.7. for the Directorate General XIII: Telecommunications, Information Market and Exploitation of Research, Directorate B: Advanced Communications Technologies and Services, (October 5).

CHM92 Benton International. 1992. *Community Health Management Information System (CHMIS): General Overview.* New York, New York: John A. Hartford Foundation.

CLA93 Clark, D.P. 1993. Meeting with the author (April 13).

CLA87 Clark, D.P. and D.R. Wilson. 1987. A Comparison of Commercial and Military Computer Security Policies. *Proceedings of the IEEE Symposium on Security and Privacy*, Los Alamitos, California: IEEE Computer Society Press. 184-94.

DAV93 Davis, R. 1993. Telephone conversation with the author (December 17).

DOD85 Department of Defense. 1985. *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD. Washington, D.C.: Government Printing Office, (December).

DRI93 Drislane, D. 1993. *Technology and the Confidentiality of Personal Health Care Information.* Testimony before the House Information, Justice, Transportation, and Agriculture Subcommittee of the Committee on Government Operations. 103rd Cong., 1st sess., (November 4).

ECM88 European Computer Manufacturers Association. 1988. *Security in Open Systems: A security framework*, ECMA TR/46 Geneva, Switzerland: ECMA, (July).

EIC92 Eichinger, S. and G. Pernul. 1992. Design environment for a hospital information system: meeting the data security challenge. in *MEDINFO 92: Proceedings of the Seventh World Congress on Medical Informatics*, ed. P. Degoulet, T.E. Piemme, O. Rienhoff. Amsterdam, Netherlands: North-Holland.

ETHI93 *Ethical Tenets for Protection of Confidential Clinical Data.* 1993. as drafted by E.R. Gabrieli in Office of Technology Assessment. 1993. *Protecting Privacy in Computerized Medical Information.* OTA-TCT576. Washington, D.C.: Government Printing Office, (November).

FAN94 Fanning, J. 1994. Telephone conversation with the author (April 5).

FOR94 Ford, W. 1994. *Computer Communications Security: Principles, standard protocols and techniques*, Englewood Cliffs, NJ: PTR Prentice Hall.

FRA94 Frawley, K. 1994. Telephone conversation with the author (Spring).

FRA93 Frawley, K. 1993. Testimony before the House Information, Justice, Transportation, and Agriculture Subcommittee of the Committee on Government Operations. 103rd Cong., 1st sess., (November 4).

GAB94 Gabrieli, E.R. 1994. Meeting with the author, (March 3).

GAO93 General Accounting Office. 1993. *Communications Privacy: Federal Policy and Actions*, GAO/OSI-94-2, Washington, D.C.: Government Printing Office, (November).

GAO91 General Accounting Office. 1991. *Medical ADP Systems: Automated Medical Records Hold Promise to Improve Patient Care*, GAO/IMTEC-91-5, Washington, D.C.: Government Printing Office, (January).

GAO90 General Accounting Office. 1990. *Computer Security: Governmentwide Planning Process Had Limited Impact*, GAO/IMTEC-90-48, Washington, D.C.: Government Printing Office, (May) in the CPSR Privacy/Information Archive.

GLD93 Goldman, J. 1993. *Statement Regarding the Confidentiality of Health Records*. Testimony before the House Information, Justice, Transportation, and Agriculture Subcommittee of the Committee on Government Operations. 103rd Cong., 1st sess., (November 4).

GOR92 Gordon, M.L. and J.M.R. Pechette. 1992. The Selected Impacts of Electronic and Computer Technologies on Law. in *Annals of the New York Academy of Sciences,* ed. D.F. Parsons, C. Fleischer, and R.A. Greene, 670:180-89.

GOS93 Gostin, Lawrence O., J. Turek-Brezina, M. Powers, R. Kozloff, R. Fade and D. Steinauer. 1993. Privacy and Security of Personal Information in a New Health Care System. *Journal of the American Medical Association*, 270(20):2487-93(November 24).

GRA94 Graubart, R.D. 1994. Meeting with the author (March 16).

GRA93 Graubart, R.D. 1993. Security and Integrity Issues in Health Care Information Systems. *DRAFT*, June 14, 1993.

GRI92 Gritzalis, D. and S. Katsikas. 1992. Data Confidentiality and User Access Rights in Medical Information Systems. in *MEDINFO 92: Proceedings of the Seventh World Congress on Medical Informatics*, ed. P. Degoulet, T.E. Piemme, O. Rienhoff. Amsterdam, Netherlands: North-Holland.

GRI91 Gritzalis, D., A. Tomaras, S. Katsikas and J. Keklikoglou. 1991. Data security in medical information systems: the Greek case. *Computers & Security*, 10(2):141-59(April).

GRY93 Gray, G. 1993. Meeting with the author (December 28).

GUP94 Gupta, A. 1994. Meeting with the author (April 6).

HAM92a Hamilton, D.L. 1992. Application Layer Security Requirements of A Medical Information System. *Proceedings of the 15th National Computer Security Conference*, Baltimore, Maryland: National Institute of Standards and Technology.

HAM92b Hamilton, D.L. 1992. Identification and evaluation of the security requirements in medical applications. *Proceedings. Fifth Annual IEEE Symposium on Computer-Based Medical Systems*, Los Alamitos, California: IEEE Computer Society Press.

HEM85 Heimbigner, D. and D. McLeod. 1985. A Federated Architecture for Information Management. *ACM Transactions on Office Information Systems*, 3(3)253-78(July).

HHS93a Public Health Service. 1993. *The Community Services Workstation™ Network Project Summary*, U.S. Department of Health and Human Services, (August 5).

HHS93b Public Health Service. 1993. *Community Services Workstation™ Task IV: Summary Evaluation and Final Report,* U.S. Department of Health and Human Services, (June).

HR3600 White House Domestic Policy Council. 1993. *The President's Health Security Plan: The Clinton Blueprint*, New York, New York: Times Books. also cited as the Health Security Act of 1994 (H.R. 3600).

HR4077a U.S. Congress. House. Committee on Government Operations. Subcommittee on Information, Justice, Transportation, and Agriculture. *Executive Summary - Fair Health Information Practices Act of 1994*, (H.R. 4077), 103rd Cong., 2nd sess., (March 17) as contained in the CPSR Privacy/Information Archive.

HR4077b U.S. Congress. House. Committee on Government Operations. Subcommittee on Information, Justice, Transportation, and Agriculture. *Fair Health Information Practices Act of 1994*, (H.R. 4077), 103rd Cong., 2nd sess., (March 17) as contained in the CPSR Privacy/Information Archive.

HU93 Hu, M.-Y., S.A. Demurjian and T.C. Ting. 1993. User-Role Based Security Profiles for an Object-Oriented Design Model. in *Database Security VI, Status and Prospects*, ed. B.M. Thuraisingham and C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 333-47.

IOM94 Institute of Medicine. 1994. *Health Data in the Information Age: Use, Disclosure, and Privacy - Prepublication Copy - Uncorrected Proofs,* ed. M.S. Donaldson and K.N. Lohr. Washington, D.C.: National Academy Press.

IOM91 Institute of Medicine. 1991 *The Computer-Based Patient Record: An Essential Technology for Health Care*, ed. R.S. Dick and E. B. Steen. Washington, D.C.: National Academy Press.

JOH93 Johnson, R. 1993. Testimony before the House Information, Justice, Transportation, and Agriculture Subcommittee of the Committee on Government Operations. 103rd Cong., 1st sess., (November 4).

KAH67 Kahn, D. 1967. *The Codebreakers: The Story of Secret Writing*. New York, New York: MacMillan.

KIN90 Kinoshita, H. and T. Shigeo. 1990. Information Security of Database Networks. *Systems and Computers in Japan*, 21(13):22-9.

KLU93 Kluge, E.-H.W. 1993. Advanced patient records: some ethical and legal considerations touching medical information space. *Methods of Information in Medicine*, 32(2):95-103(April).

LEW93 Lewers, D.D. 1993. *Health System Reform: Health Records, Computers and Confidentiality*. Testimony before the House Information, Justice, Transportation, and Agriculture Subcommittee of the Committee on Government Operations. 103rd Cong., 1st sess., (November 4).

LIN93 Lincoln, T.L., D.J. Essin and W.H. Ware. 1993. The Electronic Medical Record: A Challenge for Computer Science to Develop Clinically and Socially Relevant Computer Systems to Coordinate Information for Patient Care and Analysis. *Information Society*, 9(2):157-88.

LIN92 Lincoln, T.L. and D.J. Essin. 1992. The Computer-Based Patient Record: Issues of Organization, Security and Confidentiality. in *Database Security V. Status and Prospects,* ed. C.E. Landwehr and S. Jajodia. Amsterdam, Netherlands: North-Holland. 1-19.

LOC88 Lochovsky, F.H. and C.C. Woo. 1988 Role-Based Security in Data Base Management Systems. in *Database Security: Status and Prospects*, ed. C. Landwehr. Amsterdam, Netherlands: North-Holland. 209-27.

MAR91 Martin, M. and J.E. Dobson. 1991. Enterprise Modelling and Security Policies. *Database Security, IV Status and Prospects*, ed. S. Jajodia and C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 117-49.

MASS Massachusetts State Code, 175*I*. 1993. *Insurance Information and Privacy Protection* . in Office of Technology Assessment. 1993. *Protecting Privacy in Computerized Medical Information.* OTA-TCT576. Washington, D.C.: Government Printing Office, (November).

McC94 McCollum, C.J. 1994. Telephone conversation with the author (April 6 and 8)

McC90 McCollum, C.J., J.R. Messing and L Notargiacomo. 1990. Beyond the Pale of MAC and DAC–Defining New Forms of Access Control. *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, Los Alamitos, California: IEEE Computer Society Press. 190-200.

McD92 Morris, P. and J. McDermid. 1992. The Structure of Permissions: A Normative Framework for Access Rights. in *Database Security V. Status and Prospects*, ed. C.E. Landwehr and S. Jajodia. Amsterdam, Netherlands: North-Holland.

MER93 Meredith, M. 1993. Meeting with the author (December 30).

MIC94 Micali, S. 1994. Meeting with the author (February 10).

MONT Montana State Code, 16(5). 1993. *Uniform Health Care Information Act.* in Office of Technology Assessment. 1993. *Protecting Privacy in Computerized Medical Information.* OTA-TCT576. Washington, D.C.: Government Printing Office, (November).

MOR92 Morgenstern, M., T.F. Lunt, B.M. Thuraisingham and D.L. Spooner. 1992. Security Issues in Federated Database Systems: Panel Contributions. *Database Security V. Status and Prospects*, ed. C.E. Landwehr and S. Jajodia. Amsterdam, Netherlands: North-Holland. 131-48.

NCS92 National Computer Security Center. 1992. *A guide to understanding security modeling in trusted systems,* NCSC-TG-010, Version-1. Washington, D.C.: Government Printing Office, (October).

NOT91 Notargiacomo, L. and R.D. Graubart. 1991. Health Delivery: The Problem Solved? *Database Security, IV Status and Prospects*, ed. S. Jajodia and C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 13-26.

NRC91 National Research Council. 1991. *Computers at Risk: Safe Computing in the Information Age.* Washington, D.C.: National Academy Press.

NYA93 Nyanchama, M. and S. Osborn. 1993. Role-Based Security: Pros, Cons & Some Research Directions. *ACM SIGSAC (Special Interest Group on Security, Audit and Control) Review*, 11(2):11-7(Spring).

ORR93 Orr, G.A. and B.A. Brantley, Jr. 1993. Development of a model of information security requirements for enterprise-wide medical information systems. *Sixteenth Annual Symposium on Computer Applications in Medical Care*, ed. M.E. Frisse. New York: New York, McGraw-Hill.

OTA93 Office of Technology Assessment. 1993. *Protecting Privacy in Computerized Medical Information.* OTA-TCT576. Washington, D.C.: Government Printing Office, (November).

OTA87 Office of Technology Assessment. 1987. *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information.* OTA-CIT-310. Washington, D.C.: Government Printing Office, (October).

PAN93 Pangalos, G.J. and A.R. Bakker. 1993. Medical Database Security Policies (and Response). *Methods of Information in Medicine*, 32(5):349-57(November).

PER93 Pernul, G. Canonical Security Modeling for Federated Databases. 1993. *Proceedings of the IFIP WG2.6 Database Semantics Conference on Interoperable Database Systems (DS-5)*, ed. D.K. Hsiao, K. David, E.J. Neuholdand, R. Sacks-Davis. Amsterdam, Netherlands: North-Holland. 207-22.

RAN94 Randall, K. 1994. Telephone conversation with the author (March 31).

SHE90 Sheth, A.P. and J.A. Larson. 1990. Federated Database Systems for Managing Distributed, Heterogeneous, and Autonomous Databases. *ACM Computing Surveys*, 22(3)183-236(September).

SHO90 Shortliffe, E.H., L.E. Perreault, G. Wiederhold, and L.M. Fagan, eds. 1990. *Medical Informatics: Computer Applications in Health Care.* Menlo Park, California: Addison-Wesley Publishing Co.

SPO89 Spooner, D.L. 1989. The Impact of Inheritance on Security in Object-Oriented Database Systems. *Database Security, II: Status and Prospects*, ed. C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 141-150.

STO89 Stoll, Clifford. 1989. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York, New York: Simon and Schuster.

SZO94 Szolovits, P. 1994. Meeting with the author (April 4).

THO91 Thomsen, D.J. 1991. Role-Based Application Design and Enforcement. *Database Security, IV: Status and Prospects*, ed. S. Jajodia and C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 151-66.

TIN92 Ting, T.C., S.A. Demurjian and M.-Y. Hu. 1992. Requirements, Capabilities, and Functionalities of user-Role Based Security for an Object-Oriented Design Model. *Database Security, V: Status and Prospects*. ed. C.E. Landwehr and S. Jajodia. Amsterdam, Netherlands: North-Holland. 275-296.

TIN90 Ting, T.C. 1990. Application Information Security Semantics: A Case of Mental Health Delivery. *Database Security, III: Status and Prospects*, ed. D.L. Spooner and C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 1-12.

TIN88 Ting, T.C. 1988. A User-Role Based Data Security Approach. *Database Security: Status and Prospects*, ed. C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 187-208.

WAL91 Waller, A. 1991. Legal Aspects of Computer-based Patient Records and Record Systems. in *The Computer-Based Patient Record: An Essential Technology for Health Care*, ed. R.S. Dick and E. B. Steen. Washington, D.C.: National Academy Press. 156-79.

WAN87 Wang, C.-Y. and D.L. Spooner. 1987. Access Control in a Heterogeneous Distributed Database System. *Proceedings, Sixth Symposium on Reliability in Distributed Software and Database Systems*, Washington, D.C.: IEEE Computer Society Press. 84-92.

WAT93 Watson, B.A. 1993. Telephone conversation with the author (December 10).

WAT92 Watson, B.A. 1992. *Barriers to the Development of the Computer-Based Patient Record*. Master's Thesis, Ohio State University.

WED93a Workgroup for Electronic Data Interchange. 1993. Model Federal Legislation: Confidentiality of Electronic Health Care Information. in *Workgroup for Electronic Data Interchange: Report*. Chicago, Illinois: Blue Cross and Blue Shield Association, (October).

WED93b Workgroup for Electronic Data Interchange. 1993. *Workgroup for Electronic Data Interchange: Report*. Chicago, Illinois: Blue Cross and Blue Shield Association, (October).

WED92 Workgroup for Electronic Data Interchange. 1992. *Workgroup for Electronic Data Interchange: Report to Secretary of U.S. Department of Health and Human Services.* Chicago, Illinois: Blue Cross and Blue Shield Association, (July).

WES76 Westin, A.F. 1976. *Computers, Health Records, and Citizen Rights.* National Bureau of Standards Monograph Number 157. Washington, D.C.: Government Printing Office.

WIL93 Wilber, K. and H. Dennis. 1993. Privacy in the Electronic Age. *HMO Magazine.* 63-5(November/December).

WIS90 Wiseman, S.R. 1990. On the Problem of Security in Data Bases. *Database Security III: Status and Prospects*, ed. D.L. Spooner and C.E. Landwehr. Amsterdam, Netherlands: North-Holland. 301-310.

WKS93 Weeks, K. 1993. Meeting with the author. (August 23).

WOR81 Worthley, J.A., ed. 1981. *Managing Computers In Health Care.* Washington, D.C.: Association of University Programs in Health Administration Press.

WPR93 Work Group on the Computerization of Patient Records. 1993. *Toward a National Health Information Infrastructure: Report of the Workgroup to the Secretary of the U.S. Department of Health and Human Services.* Chicago, Illinois: American Hospital Association.

5 U.S.C. 552a *Privacy Act of 1974 and Amendments (as of January 2, 1991)* (5 U.S.C. §552a). in the CPSR Privacy/Information Archive from GPO US Code on CD-ROM (GPO S/N 052-001-004-00439-6).

15 U.S.C. 271-278h *The Computer Security Act of 1987.* PL100-235. in the CPSR Privacy/Information Archive