AN ANALYSIS OF COMPUTER SECURITY IN AN AMBULATORY MEDICAL CARE FACILITY

by

Bruce E. Stangle

A.B., Bates College

(1970)

SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF

SCIENCE

at the

MASSACHUSETTS INSTITUTE OF

TECHNOLOGY

June, 1974

Signature of Author.....
Alfred P. Sloan School of Management, May 10, 1974

Certified by.....
Thesis Supervisor

Accepted by.....
Chairman, Departmental Committee on Graduate Students

Abstract

Thesis Title: An Analysis of Computer Security in An Ambulatory Medical Care Facility

Author: Bruce E. Stangle

Submitted to the Alfred P. Sloan School of Management on May 10, 1974 in partial fulfillment of the requirements for the degree of Master of Science.

The use of computers in health organizations raises questions as to the privacy and confidentiality of automated information. Results of several site visits are forwarded as a means for establishing the state of the art in medical information systems. The literature on the subject, sparse as it is, is reviewed. A framework for analyzing the matter of data security is described. The major problem with medical data security is taken to be the uncertainty surrounding the decision as to the required level and degree of security. In order to investigate the dimensions of the problem several hypotheses are tested with the aid of a Security Attitude Survey which was administered to a sample of physicians and managers.

The results of the questionnaire are analyzed and lead to the following conclusions. First, physicians, much more so than managers, perceive automated data as more susceptible than other data to either accidental or intentional disclosure, modification or destruction. Second, managers do not believe that confidentiality is threatened by computers, while physicians are more indifferent on this question. Third, there will be a great demand for secure systems in the future. This is so because (1) those most familiar with current systems view them as less than totally secure, and (2) most users see the role of the computer in health as expanding dramatically. Fourth, general agreement exists as to the nature of automated data. The most sensitive data should be the freest from interference and the least open to access.

Thesis Supervisor: John F. Rockart

Title: Associate Professor of Management

ACKNOWLEDGEMENTS

Much of the work presented here would not have been possible if it were not for the help of friends, associates, and family. My thanks to John Rockart and Stuart Madnick for thoughtful direction, to members of the Sloan Information Systems Security Project for comments on earlier drafts, and especially to my daughter, Alissa, and wife, Emily, for motivation and moral support.

TABLE OF CONTENTS

LIST OF EXHIBITS

LIST OF TABLES

1.1 INTRODUCTION

The use of computers in health systems is becoming more extensive. Currently, computers are used in such varied application areas as payroll and patient monitoring systems. Because health expenditures form such a large part of the U.S. Gross National Product (GNP) and since medical costs have recently risen so rapidly, it will be important for this sector to develop even more effective means for applying computer technology in the future.[1] It seems increasingly important in these times of growth and innovation to evaluate the scope and breadth of automation so that fundamental institutions and relationships are maintained despite technical change. As applications of computers increase, one must recognize that computers can be subverted for means which were never intended. The aim of this thesis is to analyze and discuss some of the issues relating to data and information security in the medical environment. This analysis will include an assessment of the state of the art in computer usage, a brief review of the literature, a framework for analysis, a statement of the problem, hypotheses, a discussion of the questionnaire that is used to test these hypotheses in a medical setting, and,finally, the analysis of the data and presentation of conclusions.

---

1 U.S. health expenditures were 7.4 percent of the GNP in 1971. Furthermore, health-care costs have been rising at a rate that is twice the average increase in costs in the economy. This is a more rapid rise than any other component of the consumer price index.

Before proceeding further it is best to define some of the terms that will be used. Data security is a term that denotes safety or freedom from any threat. Data, itself, can have several states or qualities. Data can be private, confidential, operational, or public knowledge. Common threats to data are disclosure, modification or destruction whether they be accidental or malicious. Often, such countermeasures as passwords, encryption, and physical security are employed against these threats. In Exhibits 1 and 2 these terms are defined.

At this point it also is useful to provide the reader with some examples of threats to medical information systems. The following three scenarios are suggested as possibilities:

1. Many medical facilities have large automated files of patient demographic information. Suppose a computer programmer who was heavily in debt decided to sell all patient names and addresses to a direct mail advertising firm.

2. The use of automated patient scheduling systems is expanding especially in outpatient or ambulatory clinics. Doctor's schedules are stored in the computer and can be accessed or updated via a CRT or television like device. Consider the impact of appointment information leaks. Suppose a business firm sends their employees to a clinic and one of the patients

Exhibit 1

Key Definitions and Concepts in Data Security

Private: Data are private if they relate to a specific individual and should not be known by anyone but that individual. For example, one could claim that the amount of one's contribution to a charitable fund was a private matter of concern to no one else.

Confidential: Data are confidential if they can be shared openly within the context of a professional relationship, i.e., doctor-patient, manager-employee, etc. However, the data should not be available to anyone outside this professional relationship.

Operational: Data are operational if they are needed for the normal functioning of a business. The information should be available to all personnel who require the information in order to perform adequately their job(s).

Public Knowledge: Data are public knowledge if they can be openly known by all persons either within or outside a business.

Exhibit 2

Common Security Threats and Countermeasures

Common threats against data security are computer installation sabotage, accidental system breakdown, fraud, embezzlement, interception errors, disclosure of data, theft, sabotage or unauthorized copying of data. Data security can be created and maintained by some or all of the following elements:

Technical Protection (automated):

-computer system integrity (operating system, backup power, fire protection)
-remote access control (terminal authorization, user identification)
-data encoding (encryption).

Procedural Protection (manual):

-physical access control (guards, badges, locks, etc.)
-data handling rules (offsite storage, written requisition of storage volumes)
-program modification rules
-input/output separation
-input/output controls
-audit.

Personnel Protection:

-preemployment screening
-supervision
-division of responsibility.

notices on the CRT screen that his boss is scheduled to see a psychiatrist.

3. Many medical facilities are automating patient medical records. Assume a patient were allergic to penicillin but for some reason (data input error, accidental modification, or deliberate tampering) the patient's automated record reports no such allergy. The patient goes into shock and dies after a penicillin innoculation administered by a doctor who thought the medical record was correct.

These scenarios are meant to offer a context in which to view the medical data security problem. They represent threats to information which are possible. It should be noted that many of these same threats would pertain to non-computer systems as well. The difference is that with computerized systems one may be able to bring data security under tighter control and thus successfully deter these threats.

1.2 STATE OF THE ART IN MEDICAL INFORMATION SYSTEMS

Before analyzing medical data security, it is necessary to assess the extent to which computers are actually being used by those in the medical community. (For a general overview of current computer applications in medicine, see Ryan and Monroe (11).) In order to make

a thorough assessment of the state of the art in computer usage a series of field interviews were conducted. Sites were chosen so that a reasonably diverse set of organizational criteria could be observed. This diversity will become apparent as one reads through the brief site visit summaries that follow.

1.2.1 MEDICAL CENTER 1 (MC1)

MC1 is a large, fee-for-service, specialty clinic that has used computers for many years to improve the delivery of ambulatory medical care. Numerous applications have been undertaken on both the medical side and the management side of operations. Examples of each are:

Medical	Management
- Medical History	- Appointment Making
- Diagnosis History	- Billing
- Laboratory	-Accounts Receivable
- Research	- Payroll and Personnel
- Minnesota Multiphasic Personality Inventory	- Patient Data Base
- Other Test Results	- Budget

One of the most important systems for any outpatient facility is its appointment-making function. Because the amount of physician time

available for scheduling with patients is a critical resource, the organization must effectively manage this area or face a loss of revenue. MC1 has developed an online appointment system that permits coordinators to query doctor availability files while talking on the phone with patients. Key features of the system are the dynamic update capability and the automatic generation of numerous hard copy reports such as the doctor's daily schedule. This system alone has allowed MC1 to provide service to many more patients without having to increase manpower substantially.

1.2.2 MEDICAL CENTER 2 (MC2)

MC2 is a university health plan serving over 10,000 students, staff, and faculty. Currently, MC2 is converting to a new information system with the following planned features:

1. A patient master file for storing details on all patient activities. Data included would be medical history, diagnosis, treatment, and follow-up.

2. A pseudo-diagnostic routine would match patient symptoms with a medical reference file and would suggest to the physician the possible diagnosis and tests.

3. A general analysis system would scan subsets of the history file for trends in the health of the patient population and would evaluate the effectiveness of certain drug treatments.

4. Anonymous information would be made available to university researchers who might want to use the clinical data base.

1.2.3 MEDICAL CENTER 3 (MC3)

MC3 is a newly established, prepaid, group practice or more popularly a health maintenance organization (HMO). HMOs are an emerging mode of delivering health services that stresses the aspects of preventive health maintenance and comprehensiveness. An important application at MC3 is the online medical record system. This is an heroic undertaking which has not been successfully implemented at more than a handful of the nation's medical institutions, primarily because of the unwieldy nature of most medical records. The MC3 approach has been to segment the record into two parts -- encounter reports and status reports. The former detail the results of any physician visit and the latter summarize the up-to-date health of the patient.

1.2.4 MEDICAL CENTER 4 (MC4)

MC4 is a large, urban, voluntary hospital. Within MC4 are two separate information processing centers. One unit focuses entirely on

medical applications, while another develops administrative systems. For the past decade both groups have been working on innovative methods of applying computer technology to delivering in-patient medical care. An important product of this effort is a high-level, interpretative, computer language with special hospital-related features. Some of the representative systems tackled by the MCH medical unit are:

- Clinical Laboratory System
- Sequential Problem Solving
- Computer-Based Examinations for Medical Students
- Radiology Report Generation System
- Computer-Based Medical Record for Intensive Care Unit
- Computer-Assisted Acute Respiratory Care
- Diabetic Ketoacidosis Program

Many of these systems although initially developed at MCH are now being implemented at other medical centers throughout the country.

These, then, are the four organizations that were visited. The sites were selected both for their diversity in objectives and for their pursuit of effective computer applications to medicine. These visits demonstrated that a dichotomy exists in most medical information systems between applications primarily in support of management or administration and applications primarily in support of delivery of medical care. The knowledge gained from these visits facilitated the construction of a

framework suitable for analyzing the security issue in medical organizations. Before we consider this framework, however, a brief review of the literature of medical data security is needed.

1.3 PAST EFFORTS IN MEDICAL DATA SECURITY

Not a great deal of work has been done specifically in the realm of data security in the medical community. The majority of the efforts to date have a strong legalistic bent and expound upon the importance of maintaining basic patient rights to privacy.

Curran et al. (2) advocate the adoption of a code of ethics and clearly defined rules and regulations to govern the protection of information in all health data systems. A similar recommendation is made by the U.S. Department of Health, Education, and Welfare (HEW) in its request for a Code of Fair Information Practice (8). The key safeguard requirements of this proposed HEW code are:

> - There must be no personal data record-keeping systems whose very very existence is secret.
> - There must be a way for an individual to find out what information about him is in a record and how it is used.
> - There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
> - There must be a way for an individual to correct or ammend a record of identifiable information about him.
> - Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. (8, p.18)

Debate on the merits of these recommendations is under way in Congress, and reliable opinion is that a law may be passed soon in this area.

Freed (4) takes an in depth look at the legal aspects of using computers in medicine. He expresses that because hospital record systems offer less valuable returns than such computer crimes as check or credit forgery, less rigorous security systems will probably be acceptable in automated health systems.

Two instances of private institutions analyzing the problem of information security have been reported by Hulac (6) and Davis (3). The former describes an urban, comprehensive, health system in Denver, Colorado. A list of standards for ensuring the proper handling of patient data is presented. The latter reports on the Kaiser-Permanente Health System, a large, nationwide, prepaid, group practice, that has been very active in the application of computer technology to medicine.

Except for the above, the area of medical information security has received little further attention (1,7,10,12,13,16,17,18). Our present intention is to provide a more systematic analysis of the requirements for data security in the medical industry. To achieve this end it is necessary to compile a framework suitable for analyzing health information systems.

2.1 ANALYTIC FRAMEWORK

From a study of numerous user sites in various industries, an MIT Sloan group (14) developed a framework consisting of these major components:

1. Organizational Environment
2. Data Environment
3. Technological Environment

The major policy variable to be analyzed is the amount of requisite security for any given information system. Security features have some cost associated with them. The amount of time and money expended on security by an organization is strictly a function of the three independent variables: organization, data, and technology. By carefully examining the dependent variable, security requirements, in this manner one is then able to make comparisons across organizations and across groups within the same organization.

At least four means are available for expressing the organizational variable. These measures are organizational activity, organizational size, organizational goals, and organizational structure. In the health sector a great diversity exists across each of these measures. For example, although all medical organizations are concerned with the improvement or maintenance of health, this goal can be met by any number

of activities. Some organizations serve only a small group of patients; others try to meet the needs of entire communities. Many organizations are active in providing inpatient (hospital-based) care and others concentrate on outpatient or ambulatory care.

With respect to the second independent variable, data, there are two dimensions which describe its nature. These are data types and data attributes. Data types refer to data which are either personal (i.e., medical histories) or not personal (i.e., software). The distinction here is sharp: either data are personal or they are not. Data attributes, on the other hand, are more relative as they refer to the private, confidential, operational, or public nature of the data (see Exhibit 1). In health systems there are generally large files of personal data relating to all aspects of a patient's medical and financial history. With the high demand for these data by different groups with varying needs-to-know, it becomes an important matter if one can differentiate on a confidentiality scale between personal data relating to diagnoses and personal data relating to payments. In other words, to construct the data access rights for any information system, one must, first, determine who the individuals or groups are that require access, second, the attributes of the data must be rigorously specified, and third, the links between data attributes and individuals can then be mapped out.

The third independent variable, technology, is included because it is clear that the need for security can be to a large extent dictated

by the type of installed configuration. For example, a time sharing system using remote terminals connected to a computer via telephone lines has a number of security threats to deal with that do not exist in a batch system which is physically isolated from the outside world. Similarly, the operating systems of the major computer manufacturers generally are more or less vulnerable to different threats.

This then is a framework which facilitates data security analysis. The three key independent variables of organization, data and technology are the major determinants of a user's requirements for data security. We now turn to an application of this framework.

2.2 METHODOLOGY

Any scientific investigation moves from initial observations about some condition to more refined, general statements that attempt to explain the nature of a system. This process of defining the problem, testing the hypotheses, and stating the theory has been employed in this analysis as well. Before we could adequately define the problem, however, it was necessary to talk at length with those in the field who were working with medical information systems. Numerous interviews were conducted with physicians and managers in health organizations actively involved in automating the process of delivering medical care. From these discussions emerged a good feeling for the problems concomitant with using computers in medicine. The best way to state the problem is that current users of computer technology are uncertain as to what

level of security is needed for their system. This uncertainty exists because computer growth in the industry has been rapid with an attendant lack of planning for security. Uncertainty also exists due to the general lack of experience with data security risks.

2.2.1 HYPOTHESES

In order to examine the dimensions of this problem a number of hypotheses were developed. Some of the hypotheses are general in that they apply to data security in any context whether it be the financial, educational, or medical setting. Other hypotheses relate more specifically to the problem of medical data security. The more general hypotheses are:

G.H.1: Security demanded by a user is a function of the user's awareness of security as a problem.

G.H.2: In an organization an individual's proximity (in terms of job function) to the computer system will determine his awareness of security as a problem.

G.H.3: Differences in levels of security awareness and in approaches to the security problem are a function of the nature of processing in an industry and the perceived value of the information being processed.

These hypotheses have been discussed at length elsewhere (5,15), and they will receive only light treatment here. Rather this thesis investigates the special problems of security in the medical environment. From our work in the field, it became clear that the following areas warranted further study:

-The threat of computers to confidential relationships,

-The perceived adequacy of present medical data security systems,

-The sensitive nature of medical data, and

-The access rights of different individuals to medical data.

These four areas of concern capture the essence of the uncertainty problem.

The above areas can be stated more formally as testable hypotheses. These are the hypotheses specific to the medical industry:

M.H.1: Computers by their very nature are perceived as a threat to confidential relationships, e.g., physician-patient, manager-employee.

M.H.2: As medical computer usage expands, there will be an ever increasing need for security.

M.H.3: In a Medical/Management Information System numerous types of data are processed and stored from employee payroll to patient diagnosis. These data items are fundamentally different in nature and content, some being public knowledge and others being highly confidential.

It is hypothesized that:

1) these different data types can be identified
2) the different data types have varying needs for security due to their various degrees of sensitivity, and
3) the access rights of an employee to different types of data is a function of his need to know and the relative sensitivity of the data.

In addition to the above, an analysis will be made of any underlying differences in the responses of the sample population, i.e., do managers and physicians have similar attitudes with respect to data security?

2.2.2 PRINCIPLES OF MEASUREMENT

In order to test these hypotheses, many of which deal with attitudes, it was necessary to construct a measurement tool. This tool had to adhere to a prescribed set of principles. Let us examine these principles briefly before going on to consider the tool itself. (For a more detailed discussion of this entire subject see Oppenheim(9, p.120) which is summarized below.)

1. Undimensionality or homogeneity -- One thing at a time must be measured not three. If one is measuring length then you cannot measure temperature or viscocity. A problem with attitudes is that questions may stimulate numerous unmeasurable (or unanticipated) responses.
2. Linearity and equal intervals or equal-appearing intervals-- A scale should follow the straight line model and a scoring

system should be devised with interchangeable units. Attitude scales assume linearity (although this may be inadequate), but the creation of scoring units is difficult, and they are not generally interchangeable.

3. Reliability -- Measurements taken today and next week should be identical provided the object has not changed. Consistency can be achieved by greater length and diversity in attitude scales, but complete consistency is difficult to achieve since people are bound to react differently to a scale when they are confronted with it a second time.

4. Validity -- Are we measuring what we thought we were measuring? One may obtain unidimensionality by keeping only those items which intercorrelate highly, yet the scale may not measure what we want it to measure. For example, instead of measuring authoritarianism it may just be a measure of acquiescence.

5. Reproducibility -- This principle relates to a continuum of attitudes and cumulative scaling. This may not be required when dealing with constant and interchangeable units, such as pounds or inches, but, say, if one is dealing with symptoms of a disease it is helpful if the symptoms could be scaled in terms of seriousness. In that way the presence of symptom D would dictate that a patient also must have symptoms A, B, and C.

In attitude research with questionnaires these five principles must be

observed. Now, we proceed to consider the actual measurement tool.

2.3 THE SECURITY ATTITUDE SURVEY

We have stated the problem with respect to data security in medical information systems, and we have presented a list of hypotheses to be tested. The actual test of these hypotheses is achieved by administering a set of questions to those who work directly in the medical community. We have put together a five-part Security Attitude Survey which assesses the needs of a particular organization for data security (see Appendix I for the complete document). The questionnaire is divided into sections as follows:

1. Computer utilization -- this section reveals the extent of the subject's familiarity with computers and any biases pro or con they may have toward computers in medicine.
2. Security and Privacy in the 1970's -- these questions deal with general topics about perceived threats of computers to confidential relationships and the security of computerized data *vis à vis* other forms of data.
3. Computer Security at the Medical Center -- this section asks the subject to specify the nature of a given number of data items. The respondent must differentiate between data which are private, confidential, operational, and public knowledge. Next, the need for securing each data item is rated on a

scale from extremely important to extremely unimportant. Finally, an access control matrix is presented which requires that a type of access be specified for each person to each data item. For example, all employees may be permitted to have access only to summaries of patient diagnoses. This is the most crucial section of the questionnaire.

4. Respondent Profile -- Job functions and years of employment are queried.
5. Comments.

This tool was extensively pre-tested to eliminate ambiguity in wording and to further refine the measures.

Results of several site visits have been forwarded as a means for establishing the state of the art in medical information systems. The literature on the subject, sparse as it is, has been reviewed. A framework for analyzing the matter of data security has been described. It was stated that the major problem with medical data security is the uncertainty surrounding the decision as to the required level and degree of security. A number of general and specific hypotheses have been advanced which seek to explain the data security problem. These hypotheses are tested by a Security Attitude Survey which was designed to

conform to a set of measurement criteria. We now proceed to a consideration of the results of this survey.

3.1 The Site--Medical Center 1

The Security Attitude Survey was administered to a group of physicians and managers at Medical Center 1 (MC1), a large specialty clinic that was founded in the 1920's. Currently MC1 employs about one hundred physicians, twenty managers, and six hundred support personnel. Patient volume is on the order of seven hundred per day. Computer systems have been used by MC1 for nearly a decade to assist in the process of delivering quality medicine. At present there is an on-line appointment system that consists of twenty-five computer terminals connected to the central processing unit. In the future it is anticipated that several additional systems will allow on-line enquiry of the MC1 central data base. As this development proceeds the issue of data security will become more important because of the sharp increase in the number of users of the various systems. This section presents an analysis of the responses to the questionnaire shown in the Appendix. It should be noted that aside from the theoretical issues raised here, the Security Attitude Survey also provides the management of MC1 with a means for:

(1) identifying the nature of the different types of automated data,

(2) determining the relative need for security among these data types, and

(3) specifying who should have access to what types of information.

3.2 Sampling

There are approximately twenty managers and one hundred physicians at MCl. Because the time involved in completing the questionnaire was nontrivial, a limited sample was necessary. An important consideration in this regard is the confidence that one can put in any results derived from a small sample. A simple formula for deciding on an appropriate sample size is

$$n = x^2 s^2 / L^2$$

where

n = required sample size

x = number of standard deviations within which estimate will lie

s = population standard deviations

L = limit of error that can be tolerated.

In order to determine n, the other parameters must be guessed at or supplied. For the purposes of this study there should be a probability of .8 that an estimate lie within L. If one assumes further that the population standard deviation is equal to 1.0 and that L should be small, say 0.3 or less, then n would be equal to 25.

$$n = (1.5)^2 (1.0)^2 / (.3)^2$$
$$= 2.25/.09$$
$$= 25$$

A sample of 26 was drawn, composed of 14 managers and 12 staff physicians. Since the total management complement is about 20, this

group represented approximately a 70% sample. Within the staff group a balance was struck between medical and surgical specialists. In short, it is assumed that the sample size is large enough to permit a thorough analysis and that sampling,although not total, has been sufficiently random.

3.3 Results and Analysis

A key part of the analysis of questionnaire data is the researcher's assumption with respect to the distribution of responses. Continuous distributions permit an analysis of the means and variances of responses. Discrete distributions are not suitable for mean-variance analysis and, thus, must be analyzed in terms of classes of data. In the case of this study one can assume that Likert scales (e.g. agree-disagree, as shown in Q#1-9) approximate a continuous distribution. However, the remaining two hundred and twenty-six questions (Q#10-235) are distributed discretely in that the responses are more of a qualitative than a quantitative nature. With this in mind we now proceed to consider the results of the survey and to determine the admissability of the hypotheses that were proposed in section 2.2.1.

The means and standard deviations of all the questions are shown in Table 1. Recall that for Q#10-235 the mean is not a "true mean" since this is not measurement data. This qualitative mean does convey, however, a sense of which discrete response dominates. These results underly the following summary statements about the overall sample:

Table 1

Responses to Security Attitude Survey

Question Number (Q#)	Mean(S.D.)	Question Number (Q#)	Mean(S.D.)
1	1.69 (1.09)	24	4.42 (0.70)
2	6.31 (1.12)	25	4.54 (0.65)
3	2.44 (1.47)	26	4.42 (0.86)
4	3.08 (2.10)	27	4.50 (0.76)
5	3.19 (1.77)	28	3.89 (1.07)
6	4.62 (1.88)	29	2.92 (1.20)
7	4.65 (1.85)	30	4.04 (0.96)
8	4.88 (2.23)	31	4.58 (0.90)
9	3.68 (2.08)	32	3.73 (1.22)
10	2.23 (0.51)	33	3.23 (1.28)
11	2.46 (0.76)	34	4.04 (0.87)
12	2.35 (0.49)	35	3.08 (1.35)
13	2.04 (0.45)	36	3.00 (1.52)
14	2.73 (0.45)	37	4.31 (0.84)
15	2.92 (0.48)	38-51	2.63
16	2.58 (0.50)	52-65	2.20
17	1.96 (0.72)	66-79	2.30
18	2.89 (0.43)	80-93	2.62
19	3.04 (0.34)	94-107	2.14
20	2.77 (0.51)	108-121	2.04
21	3.15 (0.54)	122-135	2.13
22	3.46 (0.76)	136-149	3.25
23	2.35 (0.49)	150-163	1.90

Table 1 (continued)

Question Number (Q#)	Mean (S.D.)
164-177	1.99
178-191	2.72
192-205	1.79
206-219	1.43
220-233	3.23
234	1.54
235	3.52

1. Computer Utilization--Most of the respondents felt that they worked in close contact with computerized information. It was believed that computers offered a significant benefit to the medical community in general, and that their role would be expanding at MCl in the near future.

2. Security and Privacy in the 1970's--There seemed to be a wide range of opinion on the concern for threats to security, and, in general, the response appears to be indifferent. There appeared to be only a moderate indication that computerized information was more vulnerable to security threats than other forms of data. Most seemed to feel that computers did not pose a threat to confidential relationships.

3. Computer Security at MCl--Once again there was a wide range of responses as to the adequacy of present safeguards for the MCl computer system. Respondents indicated that medical data was somewhat more confidential in nature than administrative data, but the most private item of data was payroll information. Answers to questions on the importance of securing one type of data over another also demonstrated that, in general, it is more important that medical data be secure from interference. The trend emerging from the access control matrix is that only certain physicians should have the most unrestricted access to data,whereas, the general public should have little, if any,

access to automated data. In between these two extremes lies a continuum which specifies which individuals or groups should have what type of access to specific types of data.

Before we can draw any final conclusions from these data, however, a more detailed analysis of the physicians' and managers' responses is required. To determine this for Q#1-9 a test of the null hypothesis that the mean response of managers was equal to the mean for physicians was made. The results of this analysis are shown in Table 2. These results clearly show for four of the first nine questions that there is a statistically significant difference (at the .10 level or better) between the mean response for a manager as opposed to that of a physician.

Doctors appear to be more skeptical of the use of computers in health organizations. Physicians were more strongly in agreement with the statement that computerized information was more vulnerable to threats. Managers were more strongly in disagreement with the two statements (Q#6-7) on the effect of computers on confidential relationships.

The answers for Q#9 tend to support the second general hypothesis that was asserted in section 2.2.1. It was stated that an individual's proximity in terms of job function to the computer system will influence his awareness of security as a problem. The fact that managers see themselves as working somewhat more closely in contact with computerized information would seem to explain why they are more familiar with the shortcomings of present security mechanisms. However, these responses also point to a central paradox in these results. Physicians are more

Table 2

Test of H_o: Mean Response for Staff Equal to Mean Response for Management.

Q#1	Staff Mean (S.D.)	Management Mean (S.D.)	$P_{u1 = u2}$*
1	1.75 (.96)	1.64 (1.22)	.80
2	6.08 (1.50)	6.50 (0.65)	.39
3	3.00 (1.79)	2.08 (1.04)	.12
4	3.08 (1.98)	3.07 (2.27)	.99
5	2.42 (1.56)	3.86 (1.70)	.03
6	3.92 (2.19)	5.21 (1.37)	.09
7	3.75 (1.91)	5.43 (1.45)	.02
8	4.33 (2.46)	5.36 (1.98)	.26
9	2.92 (1.68)	4.38 (2.22)	.07

* Two-tail probability from t-test with separate variance estimate.

concerned about the vulnerability of computer systems and the possible threats posed to confidentiality, but they are also more satisfied with present security safeguards. From the viewpoint of the other group, managers are not very concerned about these threats, but they do feel that present security is less than totally adequate.

As for the questions on the nature of data and the access rights of users to it, several important results emerge. First, in most cases medical data appear to rank ahead of administrative data in terms of sensitivity. Second, the more sensitive the data type is, the more important it is that this data type be secure from interference. Third, the more sensitive the data type, the more restricted the access is to this piece of information. These conclusions can be drawn from Table 3 which shows a rank ordering of the overall mean responses for answers to this set of questions. As you may note, payroll data ranks first in terms of all indicators of security. In other words, it is the most private information, it is the most important to protect from any threat, and it is the type of data that should have the most restricted access. After payroll data, however, the trend is that the majority of medically related items appear to be more confidential in nature than administrative data. On the other end of the spectrum, it is not surprising to note that prices of services are seen as the most public of all the data.

There does not appear to be a great deal of disagreement between managers and physicians as to the nature of these data types. A series of cross tabulations of job function against all other discrete responses revealed few statistically significant differences of opinion. These

Table 3

Rank Order of Data Types for Sets of Questions on Sensitivity, Importance, and Access

Data Type	Sensitivity (Q#10-23) Mean	Rank	Importance (Q#24-37) Mean	Rank	Access (Q#38-233) Mean	Rank
Responses to Automated Medical History	2.23	3	4.42	4	2.63	4
Patient Diagnoses	2.46	6	4.54	2	2.20	7
Lab test results	2.35	4	4.42	5	2.30	6
Personality inventory results(MMPI)	2.04	2	4.50	3	2.62	5
Services rendered to a patient	2.73	8	3.89	9	2.14	8
Name and address of patient's local MD	2.92	11	2.92	14	2.04	10
Patient surgical procedures	2.58	7	4.04	7	2.13	9
Payroll data--name, check amount, etc.	1.96	1	4.58	1	3.25	1
Patient names, addresses, phone numbers, etc.	2.89	10	3.73	10	1.90	12
Appointment data--MC MD, availability, bookings	3.04	12	3.23	11	1.99	11
Patient billing and payment history	2.77	9	4.04	8	2.72	3
Blue Shield codes for Medical Center services	3.15	13	3.08	12	1.79	13
Prices of all Medical Center services	3.46	14	3.00	13	1.43	14
Total revenue generated by each staff member	2.35	5	4.31	6	3.23	2

Table 4

Results of Cross-Tabulation of Job Function (Q#234) vs. All Other Discrete Responses (Q#10-233).

Q#	Significance Level From Chi-square test
10	.07
36	.09
52	.05
101	.09
108	.10
114	.04
116	.09
128	.09
138	.05
139	.06
150	.01
156	.04
211	.10
228	.05

Table 5

Rank Order of
Access Rights of Different Groups to
Medical and Administrative Data Types.

Access Table Group	Medical Data		Administrative Data	
	Mean	Rank	Mean	Rank
A. Director of Clinical Research	1.52	4	2.32	7
B. MCl Staff Department Chairman	1.29	2	1.58	1
C. All MCl Physicians	1.42	3	2.02	5
D. Only Certain MCl Physicians	1.14	1	1.69	2
E. All MCl Nurses	2.28	9	2.62	11
F. Only Certain MCl Nurses	1.60	5	2.38	8
G. Director of Data Processing and Appointment Office	2.01	6	1.80	4
H. Director of Clinical Laboratory	2.15	7	2.48	9
I. All MCl Managers	3.10	12	2.52	10
J. Only Certain MCl Managers	2.15	8	1.74	3
K. All MCl Employees	3.67	13	3.23	13
L. Only Certain MCl Employees	2.55	10	2.12	6
M. General Public	3.92	14	3.43	14
N. Only Certain Outside Parties	2.76	11	2.69	12

results are shown in Table 4.

One final generalization can be made from these results. In terms of access rights of different groups to different data types, it appears that certain managers and certain employees have higher access rights to administrative data than they do to medical data. Table 5 shows the mean and rank order of access rights for each group or individual to the two different groups of data types, medical and administrative. As one may note the access rights of the managerial and employee groups is less restrictive for administrative data. Conversely, medical groups, doctors and nurses, tend to have more of a routine access to medical data than to administrative data. These results seem to indicate that a perception of one's need to know determines his access rights.

3.4 SUMMARY

This thesis has dealt with data security in the medical environment. It has been proposed that the primary problem with medical data security is the uncertainty surrounding the decision as to the required level and degree of computer security. In order to explore the dimensions of this problem, several hypotheses were advanced. The results support the following contentions:

- physicians, much more so than managers, perceive automated data as more susceptible than other data to either accidental or intentional disclosure, modification or destruction.
- managers do not believe that confidentiality is threatened

by computers, while physicians are more indifferent on this question

- there will be a great demand for secure systems in the future. This is so because (1) those most familiar with current systems view them as less than totally secure, and (2) most users see the role of the computer in health as expanding dramatically.
- general agreement exists as to the nature of automated data. The most sensitive data should be the freest from interference and the least open to access.

These conclusions lend support to two(M.H2 and M.H3) of the three hypotheses that were made for the medical community. Given these results, much research remains to be done on the actual construction and implementation of a secure medical information system.

BIBLIOGRAPHY

1. Carl Berkley, Privacy and the Patients' Right to Information. Medical Research Engineer, 10, (January/February, 1971), 3.

2. William J. Curran, B. Stearns, and H. Kaplan. Privacy, Confidentiality and Other Legal Considerations in the Establishment of A Centralized Health-Data System. New England Journal of Medicine, 281:5, (July 31, 1969), 241-248.

3. Lou S. Davis. Data Security Considerations in a Medical Data System. Kaiser-Permanente Medical Care Program, unpublished note, (March 30, 1973).

4. Roy N. Freed. Legal Aspects of Computer Use in Medicine. Law and Contemporary Problems, 32, (1967), 674-706.

5. Torben Gronning. Data Security and the Financial Community, forthcoming in Sloan Management Review, (Spring, 1974).

6. Shel Hulac. Some Legal Requirements for Maintaining Confidentiality of Patient Care Information in an Urban Comprehensive Health Care Information System. A Health Data Management Systems, Inc. Staff Report, (March, 1972), 1-57.

7. James J. McNamera. Legal Aspects of Computerized Medical Records, Journal of American Medical Association, 205:9, (August 26,1968), 153-4.

8. Records, Computers, and the Rights of Citizens, US Department of HEW, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, M.I.T. Press, (1973), 1-344.

9. A.N. Oppenheim. Questionnaire Design and Attitude Measurement, Basic Books, Inc. Publishers, N.Y., (1966), 1-300.

10. Privacy and Computers, Canadian Departments of Communication and Justice, Information Canada, Ottawa, (1972), 1-236.

11. G.A. Ryan and K.F. Monroe. Computer Assisted Medical Practice: The AMA's Role. American Medical Association, Chicago, (1971), 1-87.

12. Gordon Samuels. Infringements of Individual Privacy, Medical Journal of Australia, 2, (August 12, 1972), 355-357.

13. Eric W. Springer. Automated Medical Records and the Law, Health Law Center, Aspen Systems Corp., Pittsburg, Pa., (1971), 1-177.

14. User Requirements Survey, Sloan Information Systems, Security Project, MIT, unpublished report, (July, 1973), 1-165.

15. User Requirements Survey--Book II, Sloan Information Systems Security Project, MIT, unpublished report, (January, 1974).

16. Alan F. Westin, editor. Data Banks in a Free Society: computers, record-keeping and privacy, New York Quadrangle Books, (1972).

17. Douglas Whalan. Computers, Professional Responsibility and the Privacy of the Individual, Medical Journal of Australia, 2, (August 12, 1972), 357-361.

18. J. Ivan Williams. Privacy and Health Care, Canadian Journal of Public Health, 62, (November/December, 1971), 490-495.

APPENDIX

Security Attitude Survey

The Medical Center (MC)

As you know the Medical Center has been doing things with computers for a number of years. Currently the computer is used to help in such different areas as printing the payroll, assisting in the appointment scheduling processing, and recording answers to patient medical histories. It is probably quite likely that you have had several experiences in the past with the Medical Center computer system.

This questionnaire is designed to survey your attitude on some of the important issues raised by the use of computers in medical organizations. Please complete the questions as carefully as possible. Less than thirty minutes of your time will be required to finish the survey.

Part 1--Computer Utilization.

1. My work is such that I often come in contact with computerized information. (Circle one.)

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#1

2. The use of computers in medicine offers little promise for providing a higher level of care to patients and for achieving greater efficiency in managing health institutions.

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#2

3. In the next few years at the Medical Center, the computer will play a larger and larger role in assisting in the delivery and management of health care.

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#3

Part 2--Security and Privacy in the 1970's.

1. In general, I am quite concerned about such things as security leaks, bugging, and the invasion of privacy.

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#4

2. The computerization of information increases the liklihood that such data will be used for unintended purposes. In other words, automated data is more susceptible than other data to either accidental or intentional disclosure, modification or destruction.

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#5

3. The use of computers in health organizations poses a threat to the confidential relationship between a doctor and patient.

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#6

4. The use of computers in health organizations poses a threat to the confidential relationship between a manager and employee.

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#7

5. If you want to make sure that information is kept from the knowledge of others then it is better to keep information in written form and lock it in your desk rather than storing the information in a computer.

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#8

Part 3--Computer Security at the Lahey Clinic.

1. As far as my experience with the present Medical Center computer system goes, the security of automated information appears to be totally adequate.

Strongly Agree	1	2	3	4	5	6	7	Strongly Disagree	Q#9

2. In the Medical Center computer system there are basically two types of information, medical and administrative. The two columns at the bottom of this page present examples of these data types. One method of ranking the sensitivity of a particular item of data is shown in lettered code below. How would you scale the sensitivity of each type of data? In answering this question use the following code by putting the correct letter next to each data type.

Code Letter	Code Description
A (1)	These data are private in that they relate to a specific individual and should not be known by anyone but that individual. For example, one could claim that the amount of one's contribution to a charitable fund was a private matter of concern to no one else.
B (2)	These data are confidential in that they should be shared openly within the context of a professional relationship, i.e. doctor-patient, employee-manager, etc. However, the data should not be available to anyone outside of this confidential relationship.
C (3)	These data are operational and are necessary for the normal functioning of the Medical Center. The information should be available to all personnel who require the information in order to perform adequately their job(s).
D (4)	These data are public knowledge for all persons either within or outside the Medical Center.
E	None of the above.

	Medical Data			Administrative Data	
	Code Letter	Data Type		Code Letter	Data Type
Q#10	___	Responses to Automated Medical History	Q#17	___	Payroll data--name, check amount, deductions, etc.
Q#11	___	Diagnoses	Q#18	___	Patient names, addresses, phone numbers, etc.
Q#12	___	Lab test results	Q#19	___	Appointment data--MC MD, availability, bookings

Medical Data		Administrative Data	
Code Letter	Data Type	Code Letter	Data Type
Q#13 ___	Personality inventory results (MMPI)	Q#20___	Patient billing and payment history
Q#14 ___	Services rendered to a patient	Q#21___	Blue Shield codes for MC Services
Q#15 ___	Name and address of patient's local MD	Q#22___	Prices of all MC services and procedures
Q#16 ___	Patient surgical procedures	Q#23___	Total revenue generated by a staff member

3. Computers like people, are both fallible and vulnerable. For instance, it is possible to intercept or disrupt the transmission of computerized data. As protection certain security mechanisms have been developed which can deter the threat of accidental or intentional disclosure, modification, or destruction of information.

   You have just scaled the relative sensitivity of several data items. The next question is, how important is it that these same data items be secure from interference of the above mentioned threats? To answer this, enter a number from 1 to 5 which signifies the relative importance of security for the particular data type.

Extremely Important _____ Extremely Unimportant

5 4 3 2 1

Medical Data		Administrative Data	
Code Number	Data Type	Code Number	Data Type
Q#24 ___	Responses to Automated Medical History	Q#31___	Payroll data--name, check amount, deductions, etc.
Q#25 ___	Diagnoses	Q#32___	Patient names, addresses, Phone numbers, etc.
Q#26 ___	Lab test results	Q#33___	Appointment data--MC MD, availability, bookings
Q#27 ___	Personality inventory results (MMPI)	Q#34___	Patient billing and payment history

	Medical Data			Administrative Data	
	Code Number	Data Type		Code Number	Data Type
Q#28	___	Services rendered to a patient	Q#35	___	Blue Shield codes for Medical Center Services
Q#29	___	Name and address of patient's local MD	Q#36	___	Prices of all Medical Center services and procedures
Q#30	___	Patient surgical procedures	Q#37	___	Total revenue generated by a staff member

4. In many computer systems security mechanisms exist whereby certain types of data can be assigned different kinds of access according to various functions, "needs to know", or levels of authority. For example, technological capabilities are such that an automated record can be fully disclosed to one individual, while only a portion of the same record is displayed to another person. One can easily conceive of a situation in which this capability would be useful; on a newspaper it is likely that a sports editor would need to have access to different information than a fashion editor. Keeping in mind the needs and constraints of the Medical Center, what types of information would you allow each type of person named in the matrix on page (50) to access?

   In order to complete this final (but most critical) question, please fill in the matrix on the next page. The rows in the matrix correspond to the data types of the previous two questions, and the columns refer to those who either should or should not have access to each particular type of data. Enter the appropriate number in the box under each "type of person" according to the type of access which you believe should apply to that type of data.

   To indicate your opinion as to the access rights of each type of person please use the following codes.

Code Number	Code Description
1	This type of person should have routine access to any of this data.
2	This type of person should have routine access only to summarized data of this class, e.g. data which could not be connected to a particular person.

Code Number	Code Description
3	This type of person should have special access to some of this class of data provided appropriate authorization has been granted for a particular case only.
4	This type of person should have absolutely no access to this type of data at any time.

If the list of codes seems inadequate for a certain situation, then simply leave that box blank or make any comments you wish.

To illustrate how this coding might work a portion of a completed matrix is shown below. In this particular case it was felt that all MC employees (as a class) should not have access to patient diagnoses or lab test results. Thus there are "4" (no access) codes next to these data types. Also it was felt that MC prices could be widely known by all employees, so there is a "1" (routine access) code for that item..

Now go on to the next page to complete the matrix.

	K.
Patient diagnoses	4
Lab test results	4
Price of MC services	1

ACCESS TABLE*

DATA TYPE	A. B. C. D. E. F. G. H. I. J. K. L. M. N.
Responses to Automated Medical History	Q#38 . . . . . Q#51
Patient Diagnoses	Q#52 . . . . . Q#65
Lab test results	Q#66 . . . . . Q#79
Personality inventory results (MMPI)	Q#80 . . . . . Q#93
Services rendered to a patient	Q#94 . . . . . Q#107
Name and address of patient's local MD	Q#108 . . . . . Q#121
Patient surgical procedures	Q#122 . . . . . Q#135
Payroll data--name, check amount, etc.	Q#136 . . . . . Q#149
Patient names, addresses, phone numbers, etc.	Q#150 . . . . . Q#163
Appointment data--MCI MD, availability, bookings	Q#164 . . . . . Q#177
Patient billing and payment history	Q#178 . . . . . Q#191
Blue Shield codes for [illegible] services	Q#192 . . . . . Q#205
Prices of all [illegible] services	Q#206 . . . . . Q#219
Total revenue generated by each staff member	Q#220 . . . . . Q#233

* See following page for explanation of access table codes.

ACCESS TABLE CODES

A. Director of Clinical Research

B. MCl Staff Department Chairmen

C. All MCl physicians

D. Only certain MCl physicians*

E. All MCl nurses

F. Only certain MCl nurses*

G. Director of Data Processing and Appointment Office

H. Director of Clinical Laboratory

I. All MCl managers

J. Only certain MCl managers*

K. All MCl employees

L. Only certain MCl employees*

M. General public

N. Only certain outside parties*

---

*"Only certain ...." refers to those who in the course of their job would be intimately concerned with a particular situation whether it be treating a particular patient, managing a particular employee, etc.

Part 4--Respondent Profile.

1. Position with Medical Center (check one).

__ Staff __ Management

2. Years of employment with Medical Center.

__ less than 1 year __ 1-2 years __ 2-5 years

__ 5-10 years __ over 10 years

Part 5--Comments.

Thank you for taking time to complete this questionnaire. If you are interested in the results, I would be glad to supply you with a copy.

Any additional comments you might have on this survey will be appreciated and can be made below.