Abstract

The growing number of automated medical data bases has focused attention upon the problems associated with privacy and security of patient data. This paper briefly reviews some of the approaches to data base protection and then describes the solution to these problems which have been implemented in the Johns Hopkins Oncology Center Clinical Information System.

Background

"Data protection" in health information systems has been defined (1) to consist of two components:

- **Data Safety** which includes protection against destruction of the data base, manipulation or falsification of the data, and theft of recording media. Primarily concerned with the physical media, data safety protects against the loss of data, the introduction of invalid data, and/or the deliberate misuse of data.

- **Data Security** is defined to be the protection against theft of the contents of the recording media, unauthorized access to the media, and unintentional access to the media. Data Security is directed to the contents of the recording media; it protects against deliberate or unintentional misuse of the data.

The tools and procedures designed to provide data safety include data base backup, configuration control of operational programs, and limited access to the computer room and data storage areas. Data security is managed by controlling the users of the information system and its outputs (both online displays and printed reports). In this paper we shall only address the problem of data security.

The need for data security in medical information systems has been given considerable attention in recent years. Westin (2) has reviewed the large number of settings in which partially computerized medical records and health data are being used. He concludes that we "will have to make increased use of computer technology to manage the rivers of data that will be generated" and warns that "basic citizen rights cannot be made a casualty of technology-assisted health systems."

In the context described by Westin, data security may be divided into two components:

- **Intrafacility security** related to the control of information by authorized users within a health care facility.

- **Extrafacility security** concerned with the linkage and use of information by authorized organizations in receipt of data not generated by that organization.

It should be noted that one of the most powerful capabilities of a computer system is its ability to link and combine individual items of data to produce information not generally available through the use of manual procedures. Thus, authorized access to a set of individual elements may be misused to produce information for which access would normally be denied. For example, recently a student used unclassified materials to produce the design of a nuclear weapon which then became classified thereby denying him access to it.

Considerable attention is being devoted to the question of extrafacility security (3). This paper is concerned only with security within a single (or extended) facility. Within this facility, there are three components which affect security:

---

*Also Applied Physics Laboratory and Department of Biomedical Engineering, JHU.

This work was supported in part by the following grants:

NIH-NCI-CA-06973 and NIH-NCI-CA-17470.

Implementation of the system is also supported by a grant from the Educational Foundation of America.
problem. Thus, the medical system is designed hostile threat which justifies the cost of a high level of protection. In the hospital, on the other hand, are generally typified by easy entry, limited (if any) personnel screening, and data access primarily controlled by the professional and ethical standards of the users.

The difference between the defense community, and the medical environment is related to the fact that in the former, there is a known hostile threat which justifies the cost of a high level of protection. In the hospital, on the other hand, the risk of deliberate penetration of the security system is not a major problem. Thus, the medical system is designed to instill discipline and avoid accidental or casual penetration. To attempt to do more might incur unwarranted expenditures, and lead to a decrease in patient care related use of the system, thus defeating the purpose of the system.

If one limits the data security component of a medical information system to the protection from unauthorized access to programs or data, then there are two basic approaches to implementation. The use of one or both in combination depends heavily upon the system requirements and philosophy which the security component is to support.

The first method uses a password or other user identifier (e.g., badge or bar code strip) to identify the user prior to each session. In the case of a hospital information system which processes orders for medical treatment, the physician password (i.e., his computerized signature) is required to indicate authority to issue new orders. Multiuser, time shared systems use this technique to assure that individuals have access to only that data to which they are entitled.

The second approach considers the information system a general utility which is available at a specific station. In this case, the system is always "on" and any user at the station may use it. For example, consider a CRT in an admissions or information area which allows access to the current hospital census. Users do not log on by password for each query; anyone at that station may use the system independent of how it was initially logged on. In this case, security is normally provided by limiting the functions that a terminal can perform to those which are appropriate for the station in which the terminal is located.

In summary, the following general requirements for a computer based medical information system security system can be defined:

1. The computer security system must be considered a component of a larger institution data security system. Its objective shall be to avoid the introduction of new avenues for unauthorized access to medical information.

2. The computer security system operates in a generally friendly environment. Thus implementation of expensive procedures must be weighed against the risks of data misuse.

3. Data security must be integrated with the medical information system and must be supportive of the general system philosophy.

The Oncology Clinical Information System

The Johns Hopkins Oncology Center is one of eighteen Comprehensive Cancer Centers established throughout the country as part of the National Cancer Plan initiated by the National Cancer Act of 1971. The Center has major programs in laboratory and clinical research, education at all levels of training and collaborative activities with community physicians.

As part of its clinical activities, the Center provides specialized care to patients with cancer utilizing advanced techniques for chemotherapy, radiation therapy, surgery and combined modality treatment plans. The treatment of adult patients is centered in a 56 bed facility which also has the capability of serving 500 outpatients per week. Additional patient treatment is carried out in other portions of the Johns Hopkins Hospital and through an outreach program in cooperation with community hospitals.

The Oncology Clinical Information System (4) has been designed to:

- Support patient management by providing timely data displays in formats which assist in decision making.
- Prepare daily care plans based upon predefined treatment plans and current patient status, and organizing and scheduling of clinical tasks.
- Assist in the management and administration of patient care by maintaining an outpatient appointment system, producing census of patients treated, operating an institution-wide registry of patients with malignant neoplasms, producing reports on average requirements for care and blood products by disease, and sup-
porting special functions such as patient
insurance management and discharge
planning.

- Provide support throughout the Oncology
Center to users such as radiation
therapy which uses the system to maintain
engineering data on the therapy machines;
clinical engineering which uses the sys-
tem to record utilization of the patient
monitoring equipment; and the research
office which uses the system for record
keeping, searches and analysis.

A two year development cycle to implement
the above functions is now half complete, and the
following capabilities are in use:

- Each of the four inpatient units has a
terminal which displays the current
census and allows online access to plots
and flow sheets of clinical data such as
medications, test results, vital signs,
use of blood products and bacteriology
reports.

- The physicians' outpatient area has a
terminal allowing access to the above
information for all outpatients plus
the ability to display schedules for
appointments or tests by patient,
provider or clinic.

- Data entry terminals are used for
entering test results and current
status from physician generated encounter
forms and other data collection sheets.

- Limited access programs are available to
clinical data coordinators in patient
areas and are used for defining outputs
and selecting the processing required for
each patient.

- The Tumor Registry has terminals used for
maintaining a clinical abstract on each
Johns Hopkins Hospital patient diagnosed
as having cancer. Functions performed by
the Registry include initial screening
of newly diagnosed patients, follow-up
of patients treated at Johns Hopkins and
searches for special studies requested
by medical personnel.

- The Hemopharesis Unit which maintains a
platelet and white cell donor list which
is HLA matched to patients for the trans-
fusion of blood products. The system
manages the donor pool, does the match-
ing, and maintains a record of hemo-
pharesis machine utilization and patient
response.

- The Appointment Registrar has a terminal
used for scheduling new appointments and
maintaining the appointment file.

- The Insurance Coordinator has a terminal
for processing insurance information and
entering new patients into the census.

- Radiation therapy has terminals used for
quality control and equipment calibra-
tion.

- General search terminals are available to
investigators.

System users include:

- Clinical data coordinators trained in the
use of the complete system. These per-
sons generally train less experienced
general users.

- Housestaff and nursing who use the
clinical data for patients on a specific
nursing unit or in a specific clinic.

- Faculty and researchers who - depending
upon their interests - may become quite
proficient in the use of the system and
its many tools.

- Support personnel who use computer pro-
grames designed for their specific appli-
cations.

Given this mix of users and system func-
tions, a security system was required which
satisfy the following criteria:

- Access to data should be limited to that
data which is generally available in hard
copy form in the area where the terminal
is maintained. Thus, for example, the
computer should allow easy access to
clinical data on all patients in a
nursing unit because the paper record
containing that data (the chart) is
available at that station.

- In locations where data access is
authorized, it should always be avail-
able through use of the computer. That
is, individual logons should not be
required. This facilitates the use by
housestaff who consider the system an
extension of the paper chart.

- Access to information not normally avail-
able at that location in the Center must
not routinely be available from the sys-
tem terminal at that site.

- Users with authority to view specified
information within the system must be
allowed to access that information from
any terminal in the Oncology Center.
After terminating the session by that
authorized user, however, the terminal
must revert back to the previous access
mode.

- The privacy of individual patients must
be protected. For example, patient
identification should be suppressed
except in cases where it is needed. In
particular, general searches of the data base must be carried out with patient identification suppression.

Security Component Description

Our basic system philosophy is one of "functional terminals" where each terminal is considered a resource to support a specific set of functions. As a resource, the terminal is always available and requires no special logon. Through software control, the terminal provides access to all data (and only that data) required to perform that set of functions. In general, the functions which are supported use only that data which is normally available in hard copy form in that area. For example, the terminal in use at an inpatient nursing station allows access only to information about patients in that unit. The admissions terminal, on the other hand, displays the current census plus scheduled admissions but denies access to any clinical data.

In addition to the functional terminals which are located at work stations, there are other terminals which serve to screen the data according to user requirements. Thus, there is a Visitor Search Terminal which allows searching of the full data base, but all responses delete the patient identification and substitute an internal identification number. The Hopkins Search Terminal provides identification by name and hospital number but suppresses the display of patients in our outreach system of community hospitals. Outreach Search Terminal allows access to the full data base.

Each physical terminal is tied to a specific terminal function. Through use of a user ID and password, any terminal can perform any function. After a period of inactivity, each terminal times out to its original function. We illustrate this with some examples.

The terminal located in the 3 South inpatient area always displays the current census of that unit as shown in Exhibit I. To display the clinical summary abstract for patient number 2 (Basil Ball), the user would enter 2, A and the system would respond with the screen in Exhibit II. To continue with the abstract, one would use the return key to get the next page (Exhibit III). Alternately, we could select a specific page of the abstract (e.g., the History page) by entering a code given on the bottom line (in this case H) to produce the following result given in Exhibit IV).

Once a patient has been selected, the user need only identify the kind of output desired. For example, F will produce a menu for displaying a plot. For the standard peripheral white blood cell and platelet count plot is desired, a return will produce the plot illustrated in Exhibit V. As an entry of F, STFS would display the first page of the standard flow sheet (STFS) as shown in Exhibit VI.

In each of these steps, there has been no need to enter a password or learn very much about the system. Since instructions can be called by use of the question mark command, the unit terminal is essentially self instructing. It is, of course, limiting. Access is not available on this unit to data on patients scheduled for admission, patients recently discharged, or patients treated by a provider who is not in the given unit.

Access to such data is controlled by password. By entering the command "U" the user is shown the "Universal Terminal" (Exhibit VII) which provides access to all functional terminals. The user identifies the functional terminal desired and a request for his identifier and password is initiated. Once this has been entered it is used until the user logs off or there is no system activity for a reasonable period of time. Thus, the user never need log on more than once a session no matter how many functional terminals are used.

As noted previously, the search terminals are divided into three types. The first allows access only to Johns Hopkins patients, the second includes the outreach patients treated at other institutions, and the third - the "Visitor Search" - eliminates all personal identification. For example, the visitor search screen is shown in Exhibit VIII.

A search of the entire data base for multiple myeloma patients treated at the Oncology Center would produce a list given in Exhibit IX. By entering C, the next page of the list would be displayed; this process would continue until the list was exhausted. If one wished to see additional information on the second patient, one would enter 2 and the abstract with the identification would be shown. The first three pages of the abstract in the visitor search mode are shown in Exhibit X.

Conclusion

This paper addressed the question of privacy and security in a medical information system. The solution chosen for a specific institution and system was described. The underlying philosophy of this medical information system is:

(1) the automated security component is a part of a larger institutional privacy and security system; and

(2) the level of security implemented must be consistent with the institution needs, system philosophy, and potential for information misuse. It should be noted that no system is totally secure; nevertheless, the growing dependence upon automated systems requires that the development of automated systems for management of medical information take into careful consideration the privacy of patients and the security of institutional data from unauthorized access and use.

References

1. Griesser, G. (ed.) Realization of Data

References


### Exhibit I - Standard Inpatient Unit Terminal Screen

<table>
<thead>
<tr>
<th>Patient ID</th>
<th>Name</th>
<th>Age</th>
<th>Admit Date</th>
<th>Disch Date</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001000</td>
<td>ADAM, EVE</td>
<td>65</td>
<td>03/31/78</td>
<td>04/12/78</td>
<td>10</td>
</tr>
<tr>
<td>0001001</td>
<td>BALL, BASIL</td>
<td>57</td>
<td>04/12/78</td>
<td>04/17/78</td>
<td>12</td>
</tr>
<tr>
<td>0001002</td>
<td>CAIN, ABLE</td>
<td>49</td>
<td>04/17/78</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>0001003</td>
<td>DAY, DAWN</td>
<td>72</td>
<td>04/06/78</td>
<td>04/13/78</td>
<td>12</td>
</tr>
<tr>
<td>0001004</td>
<td>GOOD, MAY B.</td>
<td>36</td>
<td>04/17/78</td>
<td>04/15/78</td>
<td>10</td>
</tr>
<tr>
<td>0001005</td>
<td>HIGH, LO</td>
<td>65</td>
<td>04/15/78</td>
<td>04/15/78</td>
<td>15</td>
</tr>
<tr>
<td>0001006</td>
<td>KING, REK</td>
<td>45</td>
<td>04/17/78</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>0001007</td>
<td>LITTLE, MAX</td>
<td>67</td>
<td>04/13/78</td>
<td>04/17/78</td>
<td>15</td>
</tr>
<tr>
<td>0001009</td>
<td>PRINCE, ALBERT</td>
<td>85</td>
<td>04/17/78</td>
<td>04/17/78</td>
<td>15</td>
</tr>
<tr>
<td>0001010</td>
<td>QUEEN, VICTORIA</td>
<td>92</td>
<td>04/17/78</td>
<td>04/17/78</td>
<td>15</td>
</tr>
<tr>
<td>0001011</td>
<td>SMALL, MINNIE</td>
<td>63</td>
<td>04/17/78</td>
<td>04/17/78</td>
<td>15</td>
</tr>
<tr>
<td>0001011</td>
<td>VICTOR, R.C., ALBERT</td>
<td>72</td>
<td>04/17/78</td>
<td>04/17/78</td>
<td>15</td>
</tr>
</tbody>
</table>

**Phone:** 21205  
**Class:** JHH  
**Spouse:**  
**Birth Date:** 08/08/19  
**Pob:** 999  
**Admitted:** 02/12/78  
**Discharged:** 03/15/78  
**Sex:** M  
**Race:** Non-White  
**Status:** U  
**Eviden of Disease:**

---

### Exhibit II - Sample Abstract, Identification Screen

**Diagnosis Primary - 1**

<table>
<thead>
<tr>
<th>JHH Diagnosis</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>151.9 STOMACH, NOS</td>
<td>02/78</td>
</tr>
<tr>
<td>9481/33 MUCIN-PRODUCING ADENOCARCINOMA</td>
<td></td>
</tr>
<tr>
<td>GRADE: POORLY DIFFERENTIATED</td>
<td></td>
</tr>
<tr>
<td>EXTENT: REGIONAL, NODES ONLY</td>
<td></td>
</tr>
<tr>
<td>LATER: NOT A PAIRED ORGAN</td>
<td></td>
</tr>
<tr>
<td>BASIS OF DIAGNOSIS: PATHOLOGY, X-RAY</td>
<td></td>
</tr>
<tr>
<td>CARCINOMA OF STOMACH (UNRESECTABLE)</td>
<td></td>
</tr>
<tr>
<td>78-3301 - STOMACH BX.: INFILTRATING POORLY DIFFERENTIATED ADENOCARCINOMA OF STOMACH, 78-3641 - GASTROHEPATIC LIGAMENT: FOCI OF METASTATIC POORLY DIFFERENTIATED MUCIN PRODUCING ADENOCARCINOMA, MULTIPLE LIPOID GRANULOMATA</td>
<td></td>
</tr>
</tbody>
</table>

---

### Exhibit III - Sample Abstract, Diagnosis Screen

505
Exhibit VII - Universal Terminal Screen

Exhibit VIII - Visitor Search Terminal Screen

Exhibit IX - List of Entries Which Satisfy a Search
**NONAME** 0023236720
**NONAME** 0023236720

ADMITTED 09/05/76
SEX F
RACE WHITE
MAR. STATUS MARRIED
FOLLOW UP STATUS - 11/77
EVIDENCE OF DISEASE

**NONAME** 0023236720

**PRIMAR** I.d. Tx. Hx. Follow-up End results (RET) or Quit?

**NONAME** 0023236720

**DIAGNOSIS PRIMARY - 1**

<table>
<thead>
<tr>
<th>JHH DIAGNOSIS</th>
<th>09/76</th>
</tr>
</thead>
<tbody>
<tr>
<td>169.1 BONE MARROW</td>
<td></td>
</tr>
<tr>
<td>9730/39 PLASMA CELL MYELOMA (GRADE NOS)</td>
<td></td>
</tr>
<tr>
<td>GRADE: NOT DETERMINED</td>
<td></td>
</tr>
<tr>
<td>EXTENT: UNSTAGED OR NO DATA AVAILABLE</td>
<td></td>
</tr>
<tr>
<td>LATERAL: NOT A PAIRED ORGAN</td>
<td></td>
</tr>
<tr>
<td>BASIS OF DIAGNOSIS: PATHOLOGY</td>
<td></td>
</tr>
<tr>
<td>MULTIPLE MYELOMA</td>
<td></td>
</tr>
<tr>
<td>JT-14417 - RT. ILEUM: BONE &amp; SOFT TISSUE CONTAINING DIFFUSE</td>
<td>INFILTRATION OF MARKEDLY ATYPICAL PLASMA CELLS CONSISTENT WITH</td>
</tr>
<tr>
<td>MULTIPLE MYELOMA.</td>
<td></td>
</tr>
</tbody>
</table>

**NONAME** 0023236720

**TREATMENT PRIMARY - 1**

<table>
<thead>
<tr>
<th>FROM</th>
<th>TO</th>
<th>TYPE</th>
<th>PURP</th>
<th>LOC</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/07/76</td>
<td>9/DX</td>
<td>BIOP</td>
<td>JHH</td>
<td>RT. ILEUM</td>
<td></td>
</tr>
<tr>
<td>10/76</td>
<td>03/77</td>
<td>CHEM</td>
<td>PAL</td>
<td>JHH</td>
<td>NOTE 1</td>
</tr>
<tr>
<td>10/76</td>
<td>03/77</td>
<td>CHEM</td>
<td>PAL</td>
<td>JHH</td>
<td>ALKERAN &amp; PREDNISONE</td>
</tr>
<tr>
<td>06/21/77</td>
<td>07/31/77</td>
<td>CHEM</td>
<td>PAL</td>
<td>JHH</td>
<td>NOTE 2</td>
</tr>
<tr>
<td>11/18/77</td>
<td>10/DX</td>
<td>BIOP</td>
<td>JHH</td>
<td>NOTE 3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 3000R TO LOWER SPINE IN 8-10 TREATMENTS</td>
</tr>
<tr>
<td>2 (JHH 7715) 3 COURSES HIGH DOSE CYTOXAN</td>
</tr>
<tr>
<td>3 BONE MARROW EX. (ANNE ARUNDEL POS.)</td>
</tr>
</tbody>
</table>

**PRIMAR** I.d. Tx. Hx. Follow-up End results (RET) or Quit?

Exhibit X - Name Suppressed Abstract (First Three Screens Only)

508