Minimum Requirements for the Security of Computerized Records of Health and Social Services Network Clients

April 1992

Mr. Benoît Elie and Mrs. Alice Labrèque wrote this document and carried out an extensive series of consultations on it.

Mr. Elie and Mrs. Labrèque wish to acknowledge the significant contribution of Mr. Claude Francoeur to the preliminary draft policy released in August 1991.

TABLE OF CONTENTS

THE COMMISSION'S ORIENTATIONS

INTRODUCTION

This document embodies the new "Issue-oriented Approach" of the Commission d'accès à l'information.

Since the implementation of this approach, the Commission has studied and made decisions on all aspects of the protection of personal information and access to information. It develops orientations, recommendations and guidelines on the issue under consideration. This is a preventive approach aimed at agencies concerned by the issue in question.

This document deals with the computerization of records of clients of the health and social services network. In the fall of 1991, extensive consultations on this document were held. The measures it proposes are therefore realistic and can be applied by network agencies.

The Commission reminds agencies of the fundamental rights of persons with reduced physical, psychological and social autonomy, and more specifically their right to privacy. This right belongs to every citizen, but it is all the more important that it be protected when a person, in a situation of dependency, must provide personal information.

The Commission therefore encourages agencies of the health and social services network to be vigilant and prudent when developing and implementing computer systems. This guide will help them to comply with the *Act respecting Access to documents held by public bodies and the Protection of personal information* and avoid possible actions under the *Charter of Human Rights and Freedoms*, the *Act respecting health services and social services*, and the *Act respecting Access*. The Commission's staff is also available to provide assistance.

THE ISSUE

For some years now, computers have become increasingly important in maintaining the records of health and social services clients. The largest projects, involving many hospitals, were the first to attract the attention of the public and the Commission d'accès à l'information.

At present, in 1992, computerization of records is very uneven. In some hospitals, it is relatively advanced and used on a daily basis by most departments, while in nursing homes, for instance, it is still at an early stage. The Commission will not comment on the pros and cons of computerization of client records since the process is irreversible and will soon be standard throughout the health and social services network.

In accordance with the authority vested in it by the *Act respecting Access to documents held by public bodies and the Protection of personal information*, the Commission seeks to ensure that the confidentiality of client records will continue to be guaranteed. Experts agree that the risk of a breach of confidentiality of computerized records is high enough for the security of these records to be a major concern. The possibilities for processing, linking, and matching data are virtually unlimited, and that is where the main threat to confidentiality lies. Now, unlike ever before, hundreds, even thousands of items of data can be processed very rapidly by increasingly user-friendly computer systems, i.e. systems that are more and more accessible to the lay person. In addition, it is relatively easy to link systems, and such links can give rise to personal information "requirements" for uses other than those contemplated when the information was gathered.

OBJECTIVE OF THE DOCUMENT

First, the Commission's experience concerning client records on paper should be recalled. The risk of breach of confidentiality in this case is also real and must not be minimized. The Commission had to investigate many cases, and concluded that unauthorized persons had access to client records. Agencies must therefore be constantly on guard to ensure that records, on whatever medium, remain confidential.

The Commission's objective in publishing this document is to instruct, advise and help agencies of the health and social services network. The Commission's aim is to ensure that computerization complies with the principles entrenched in the *Act respecting Access to documents held by public bodies and the Protection of personal information*. It offers assistance both to those responsible for agencies and to managers and designers who want to implement computer systems.

This document lists and describes what the Commission considers the minimum in terms of security measures required to guarantee the confidentiality of computerized records.

These measures are based on the *Charter of Human Rights and Freedoms*, which enshrines the right to privacy, and on the principles of the *Act respecting Access*.

THE MAIN PRINCIPLES OF THE *ACT RESPECTING ACCESS*

These principles hinge on the collection, confidentiality and access to personal information.

1. Collection of personal information

Section 64 of the Act respecting Access states the rules for collecting personal information:

> 64. No person may, on behalf of a public body, collect nominative information if it is not necessary for the carrying out of the attributions of the body or the implementation of a program under its management.

The ministère de la Santé et des Services sociaux, the Régie de l'assurance-maladie, regional boards[1], and health and social services network establishments must therefore ask themselves whether an item of nominative information is truly necessary before obtaining it from the person concerned. The installation of a computerized client record system provides agency managers with an opportunity to do so. It will no longer be possible to incorporate certain information unless the agency cannot deliver its services without it. For instance, some hospitals ask patients for their religion on being admitted. Is this information necessary, or simply desirable? If necessary, the hospital can certainly incorporate it. It is worth noting that the Commission has already interpreted the notion of "necessary information" and given it the meaning of "indispensable".

2. Confidentiality and transmission of nominative information

Clients' records are kept strictly confidential. Section 53 of the *Act respecting Access* and section 19 of the *Act respecting health services and social services* state that no information can be taken from an individual's record without his or her consent.

---

[1] The new legislation respecting health services and social services (1991, Chapter 42) will soon enter into force. That is why the Commission frequently refers to it

The Commission's preference is that the person concerned give his or her free and informed consent in writing. It is worth noting that the information requested often does not concern the entire record. For instance, the Commission de la santé et de la sécurité du travail du Québec only requires, with the person's written consent, information concerning the work-related injury. Therefore, the hospital must not forward the worker's entire record.

Section 19 of the *Act respecting health services and social services* also allows for exceptions to the principle of consent. In very specific - and exceptional - cases, the information can be transferred, provided confidentiality is maintained.

3. Access to nominative data

Under section 83 of the *Act respecting Access* and section 17 of the *Act respecting health services and social services*, the client is entitled to see his or her record and obtain a copy of it. Computer systems must provide for this possibility. Patients have the same access rights as when files were maintained on paper. Hospitals must take these rights into consideration if terminals are installed in patients' rooms.

However, access to nominative information on clients by the staff of health and social services agencies raises problems. Each system must allow for different access rights according to employee categories. Employees working in an agency's financial department clearly should not have the same access rights as clinical staff. This is an extreme example, but it illustrates the need to segment access according to employee duties. Similarly, opportunities for consulting, entering, altering and destroying socio-health information must also be differentiated for staff in admissions, the dietetic department, the occupational health and safety department, and the adoption department.

---

in this document.

MINIMUM SECURITY MEASURES

PURPOSE

This section specifies the security measures a health and social services agency must take to maintain the confidentiality and integrity of the computerized personal socio-health data it holds.

AGENCIES COVERED

Health and social services agencies subject to the *Act respecting Access* are required to implement the measures described in this document. These agencies are: the ministère de la Santé et des Services sociaux, the Régie de l'assurance-maladie, regional boards and network establishments.

SCOPE

The personal socio-health information covered by the measures described in this document consists of any information a health and social services agency stores in its main computer, in the computer of its supplier of computer services, or in its microcomputers. This covers any computer hardware that stores, transmits, or processes information, and any support medium: magnetic tape, diskettes, computer output lists and microfilms, etc.

NOMINATIVE DATA

The security measures described in this document concern nominative information in the health and social services sector. But what is nominative information? Sections 54 and 56 of the *Act respecting Access to documents held by public bodies and the Protection of personal information* define its characteristics:

> **54.** In any document, information concerning a natural person which allows the person to be identified is nominative information.
>
> **56.** The name of a natural person is not nominative information, except where it

> appears in conjunction with other information concerning him or where the mere mention of his name would disclose nominative information concerning him.

These sections indicate that, within the scope of this policy, almost all information held is nominative. Agencies must be very cautious in deciding whether or not a piece of information is nominative. A single item of information may not be enough to identify a particular person. However, when combined with another item, it becomes easier to identify the individual. A record number alone is not enough to localize a person, but when the name of the establishment is added, identification becomes much more likely. Taken together, these two items of information must be considered nominative.

Regardless of the medium an agency uses to store socio-health data, the data can be disclosed and altered, accidentally or voluntarily, under a variety of circumstances: flooding, earthquakes, fire, vandalism, sabotage, hardware failure, data entry, transmission or processing errors, fraud, falsification, alteration, addition to, destruction or theft of socio-health data or hardware, etc.

We discuss below the minimum security measures or systems that will enable agencies to comply with the main principles of the *Act respecting Access* and thwart such occurrences (some agencies could be required to implement other, more secure measures to provide better protection for their socio-health data). Like most of the agencies we consulted, the Commission is convinced that these security measures will be effective if staff is made aware of them regularly. The most sophisticated security measures will prove effective only if the individuals who apply them are convinced of their merits.

As a result, to decide which security measures are most appropriate to its particular case, an agency will have to assess its risk factors. This assessment is commonly called: risk analysis.

STEPS AGENCIES MUST TAKE

To implement and enforce security measures, agencies must develop policies and procedures and keep them up to date. To do so, a person must be appointed to assume this responsibility, and this person must have senior management's unequivocal support.

The Commission considers a person is already in a position to assume this role: the person responsible for the protection of personal data whose role, as defined in the *Act respecting Access*, is to maintain the confidentiality of socio-health data.

This person should set up and preside over a socio-health data security committee to help in carrying out his or her duties and when justified by the agency's activities. This committee would have the following responsibilities:

- develop a staff awareness and training program for socio-health data security and protection;

- coordinate activities related to the protection of socio-health data and computer security (implementation of appropriate mechanisms, such as access profiles, access verification, management of identification codes and bar cards, etc.);

- periodically checking compliance with the socio-health data protection and security program (this task should be carried out by the internal or external auditor, or at least by a person who is independent of the various security groups);

- submit an annual report (follow-up and control) on the application of the security program to the most senior person in the agency.

Since the situation varies from agency to agency, the Commission does not intend to indicate who should be on the committee. It is up to the agency's management to make those choices.

SECURITY MEASURES

To protect computerized socio-health data from disclosure or alteration, security measures or systems must at least cover the following aspects: user[2] identification and authentication for purposes of access to socio-health data, access profiles, data collection or entry, back-up copies,

---

[2] In this document, "user" means any person with a recognized right to access. For instance, employees or agents.

terminals, the main computer, access logs, telecommunications, any mandate granted by an agency to a person or other agency (for computer or office services, for instance), sharing of common data bases or a common processing centre, an awareness and hiring program, transmission of socio-health data, microcomputers, and printing of socio-health data.

1. User identification and authentication for purposes of access to socio-health data

- Users must first identify themselves before gaining access to the computerized socio-health data for which they are authorized. Various identification mechanisms are available: the user can enter his or her identification code at the keyboard, using a bar code card, a smart card or magnetic key, for instance.

- A unique identification code should be assigned to each user. If a user must have access to more than one work station at the same time, he or she is entitled to several identification codes. However, two users should never share the same identification code.

- Identification codes that have not been used during a given period of time should be deactivated or destroyed after being checked.

- Each establishment should develop policies and administrative procedures for assigning identification codes.

- The identification code must be supplemented by user authentication. The user can be authenticated by entering a password, or by biometric means: hand print, voice registration, retinal image, etc.

- Passwords can consist of letters or digits and must be between five and eight characters long.

- User passwords must not be posted on screens.

- Users must change passwords periodically, at least once every three months if

the identification code is entered using the keyboard, once every six months if the identification code is entered any other way (bar code card, smart card, magnetic key, etc.). An agency can also decide how often to change a password by considering the number of times a user has accessed the system during a given period.

- A user must be refused access after a maximum of five errors in entering his or her password.

- Anyone receiving an identification code and a means of authentication to gain access to socio-health data must agree not to disclose or lend them and, if applicable, assume responsibility for them.

- The immediate superior or other specially authorized person must revoke or suspend a user's identification code and means of authentication:

  . if the user resigns from the agency or is fired;

  . when he or she has completed his or her contract;

  . when he or she changes jobs within the agency and his or her new duties do not require access to socio-health data;

  . if there is abuse or an indication of abusive use;

  . if the user must be absent for a period determined by the agency.

2. Access profiles

- Users must have access only to the socio-health records necessary to carry out their duties. Agencies must therefore define an "access profile" for each user that will determine what he or she has access to (administration, medical, social) and the type of access (writing, reading, etc.). Provision must be made for every possible type of necessary

access because of emergency situations.

- Establishments must have different access profiles for their employees depending on whether or not client records are active or inactive. The records administrator, or a person appointed to fill that role, must have access to inactive records to make them active if need be.

- The systems development staff must not have access to real nominative socio-health data and production systems. They should have access to real socio-health data only if the data have been de-nominalized. Systems support staff should have access to the production systems if necessary (in the event of a system breakdown, for instance).

- Agencies must use fictitious or de-nominalized socio-health data for training and presentation purposes. Trainees working with clients, though they are being trained, can use real socio-health data if that is necessary for their training.

- Access to socio-health data or to laboratory results is allowed from the client's residence when he or she is being treated at home, or from the residence or clinic of a physician or specialized professional provided the record or laboratory results concern the client treated by such physician or specialized professional.

- Subject to the *Archives Act*, authorization to destroy socio-health data must be limited to a few staff members under very specific conditions.

- Socio-health data must be destroyed in such a way that their confidential nature is maintained.

- Each agency must adopt administrative procedures and policies for assigning access profiles to its staff.

3. Data collection (entry)

- Only persons authorized by the agency can collect, enter or cause clinical data to be entered into a client's computerized record.

- An agency must be able to identify any person who enters an item of socio-health data into a client's record. This authenticates the clinical data that is entered. To prevent the authenticity of this computerized information from being contested, the software used must be designed in such a way that data previously entered cannot be erased. However, since it is possible to make corrective entries, such entries must include a notation indicating the author and the time the change is made.

- An agency must only collect socio-health data that is relevant, accurate and necessary for client services and public health, as well as for monitoring operations, management, and planning services.

4. Back-up copies

- Back-up copies of socio-health data, programs and software must be made periodically.

- Only a restricted number of persons is to be authorized to make these copies.

- Each agency must decide who will be responsible for making back-up copies.

- Back-up copies must be stored in a different room from the computer and, if possible, in another building.

- Circulation of these copies must be monitored.

5. Terminals

- Terminals must be installed in restricted access rooms (work zones) or rooms that can be locked. If they cannot be located in such rooms (for instance, terminals at a

patient's bedside), they must be equipped with a lock or a magnetic card reader.

- When nominative data appear on the screen, an agency must terminate a user's work session if, after a given period of time, he or she has not made any transaction at the terminal. This period of time must be as short as possible, varying from terminal to terminal depending on the user's duties, and will be determined by the establishment.

- When nominative data appear on the screen, steps must be taken so that unauthorized persons cannot see what is on the screen (appropriate disposition of screens or suitable carrels will help).

6. Site security

Agencies must provide adequate protection for rooms where their computers and communications lines are installed, and restrict access to authorized persons only.

7. Access log

Every access to nominative information must be logged. The log must include:

1- the user's identification code;
2- the name of the file accessed;
3- the number of the record concerned;
4- type of access (record creation, retrieval, modification or destruction);
5- the transaction code or program name (show the more specific of the two);
6- date of access (year, month, day);
7- time of access (hour, minute, second).

This information can be stored in the client records or in a separate file.

- Unauthorized accesses must be checked.

- For printing jobs involving the nominative data of all records in a file, it is not necessary to log the record numbers concerned. However, the other items mentioned above must be logged.

- Printing jobs involving de-nominalized or statistical data exclusively need not be logged.

- Logs must be kept for two years. However, in the event of an investigation or legal proceedings, they must be kept as long as the case has not been settled.

- Using access logs, computerization of client records makes it easy to identify an employee who has seen a client's record without a valid reason, and apply the appropriate sanctions.

8. Telecommunications

- Periodic controls of user passwords and access privileges must be carried out to detect anomalies or fraudulent use of telecommunications.

- Telecommunications must be structured in such a way that any nominative data transmitted cannot be intercepted or introduced from an unauthorized terminal. If the telecommunications environment is not secure enough to guarantee confidentiality, the nominative socio-health data transmitted must be encrypted before transmission and de-encrypted only upon reception (coding).

9. Mandate from an agency to a person or other agency

Any mandate an agency grants to a person or other agency must be in writing. In addition, the mandate must:

- clearly specify in the text of the agreement the mandate's objectives and ultimate purpose, the procedures for communication, etc.;

- include a confidentiality clause to be signed by the mandatary;

- require mandataries to guarantee the protection of socio-health data they receive, not to use them for their own purposes, to train and make their staff aware of the issue;

- hold mandataries responsible for breaches of the *Act respecting Access* by their staff;

- include a contract or service termination clause if the mandatary breaches the requirements of the agreement or the *Act respecting Access*;

- stipulate that a supplier of services who receives a mandate ensure that other suppliers he deals with also comply with the requirements of the mandate;

- stipulate that the mandatary return or destroy the information obtained once his mandate has been completed or cancelled, regardless of the reason.

10. Sharing common data bases or a common processing centre

If many agencies have to share the same data bases or the same computer centre to process socio-health data, they must take the measures necessary to ensure that none of the other agencies has access to their respective data without the client's consent.

11. Awareness and hiring program

- Judgment is necessary in selecting which staff members will have access to clients' nominative data.

- Agencies must require staff with access to socio-health data to sign a confidentiality clause (this rule applies to any person outside the agency who has access to this type of data).

- Agencies must train their staff and make them aware of the need to protect the confidential nature of socio-health data (by periodically displaying messages on the protection of socio-health data on the screens of users, by posting non-disclosure notices, etc.).

- Agencies must educate users to close their work session when they leave their work station.

- Agencies must stipulate disciplinary measures (up to and including dismissal) for any breach of the integrity of socio-health data and for their disclosure.

12. Transmission of socio-health data

The consent of the person concerned is necessary, or the conditions stipulated in the *Act respecting health services and social services* must be satisfied, before socio-health data can be transmitted.

- The recipient's security measures must be adequate.

- Only necessary data should be transmitted.

- In the event data is transmitted for study, research or statistical purposes, agencies must verify whether or not nominative data must be transmitted. If they are not required, the data must be de-nominalized before being transmitted to the researcher. In addition, the researcher must agree in writing to treat the data as confidential and destroy them after they have been used.

13. Microcomputers

- Use a microcomputer communications program such as "Sesame" (a Québec product).

- Certain measures must be taken to prevent computer viruses:

  . never use programs or software of dubious or external origin;

  . make users aware of the dangers of computer viruses;

  . implement automatic software control and computer audit procedures;

  . use virus protection programs and security functions (control logical access to work stations, encrypt data, etc.).

- Deactivate the "Print Screen" key when nominative data are displayed on the screen to prevent records from being printed without authorization.

14. Printing socio-health data

- Senior management must approve a policy on the user's right to print socio-health data. The policy should also make provision for procedures to dispose of print-outs after they have been used.

- These documents must be printed by users and in authorized premises.

15. Implementation period

- The Commission d'accès à l'information allows agencies three years to adapt their systems to these minimum requirements.

- The Commission asks that systems under development comply with these minimum requirements as soon as they are installed.

16. Breach of certain standards

It may happen that, because of the multiplicity of computer hardware and software in use in the health and social services network, a standard described in this document is technically inapplicable. In such a case, the Commission asks that the agency concerned include the resources required in its master plan to change its hardware or to develop support programs.

CONCLUSION

We have described the minimum security measures that must be applied to computer systems to manage the records of health and social services network clients.

These security measures must be stated in the administrative procedures written by each establishment.

A public agency is of course free to apply additional or more stringent security measures to protect the confidential information entrusted to its care.

GLOSSARY

Telecommunications:

remote communications systems (the telephone, for instance).

Client:

person receiving health and social services from a network agency.

User:

person entitled to access to the computer system.

This text reproduces the gist of a round table discussion on some practical problems encountered in protecting personal information as part of client record computerization projects.

It was conducted by Mr. Germain Lacasse for the Commission d'accès à l'information.

The following took part in the round table: Dr. Michel Brazeau and Mr. Normand Lambert, of the Laboratoire de santé publique, Mrs. Françoise Martin and Mr. Jacques Monette, of the Centre hospitalier de l'Université de Sherbrooke, Mrs. France Nicole and Mr. Claude Lévesque, of the Centre hospitalier de Gatineau, for the SIDOCI project.

***

Left to right: Mr. Normand Lambert, Mrs. Françoise Martin, Mr. Jacques Monette, Mrs. France Nicole, Mr. Claude Lévesque, Dr. Michel Brazeau and Mr. Germain Lacasse.

The locksmith in the hospital

Germain Lacasse

Recently, the Laboratoire de santé publique du Québec had to dismiss a computer programmer who had exceeded his mandate by devising a way to access confidential records for which he was not authorized. The individual felt he had been dismissed unfairly and appealed to an arbitration board. The arbitrator found in favour of the Laboratoire, stating the individual's actions had violated the *Act respecting Access to documents held by public bodies and the Protection of personal information*. This decision was made public and constituted a precedent. The Act had been interpreted vaguely in so far as protection of socio-health records was concerned. That weakness has now been corrected with the publication of the Commission's minimum requirements in this regard. This document covers these requirements.

These rules are timely, noted Dr. Michel Brazeau, scientific director of the Laboratoire de santé publique. They'll clarify the meaning of the Act and the measures needed to apply it. They'll help make computer system users more aware of the importance of always being careful to protect information. At the Laboratoire, we receive data on tens of thousands of people. You can imagine the harm that would be done by, for instance, disclosing information on people with AIDS, or other notifiable diseases on which we gather information.

The programming team, because they were vigilant and aware, noticed the activities of this over-curious or over-zealous employee. However, if we had not already had strict measures in place limiting access to data, he could have had access. We eventually caught on to him because of his persistence in trying to break the rules. Thank goodness for them!"

This becomes clearer when Normand Robert, engineer and assistant systems manager, explains that the Laboratoire is connected to 34 community health departments that send and receive information using telecommunications. The information's structure provides an initial measure of security. It is divided into three files: nominal, anonymous and depersonalized. The first can be accessed only by the CHD concerned. The second is open to all CHDs, but contains only anonymous data that can't be altered. The last is open to other users and contains only numerical

data.

The number three occurs frequently in the Laboratoire's security formula. To restrict access, three different computers are used: one to enter and process data, the second for communication with community health departments, and the third to control the quality of microbiology laboratory data. In each file, the user can access only the information concerning his task. Even there, we make a distinction between right and need, adds Mr. Lambert, and need is as far as the user can go. In other words, he cannot see everything he has a right to see, but rather only what he needs to see. I use the following metaphor to explain this: a locksmith has the right to make keys, but that does not authorize him to open any door he wants. The user must enter an access code, and menus then restrict his movements to the parts of the record that concern him.

Unlike what many people feared, computers have not made it more difficult to protect these data, Dr. Brazeau says. On the contrary, it provides many protection alternatives not available for paper records. But it also offers other benefits. Information can be standardized and made more accessible to those who need it. It is now possible to compile information on communities very quickly, for instance to know health conditions by region or city. This information is very valuable. With computers, it can be stored, analyzed and quickly forwarded to those who need it. This helps improve public health.

The Centre hospitalier universitaire de Sherbrooke (CHUS), where a computer system named Ariane (Ariadne) manages almost all information, has also discovered this benefit. Ariane is the heroine of Greek myth who gave Theseus a thread and so allowed him to escape the labyrinth where he slew the Minotaur. With computerization, the number of such threads has increased phenomenally.

"This system protects the patient's record," agrees Jacques Monette, human resources manager at the CHUS and the person responsible for enforcement of the *Act respecting Access*. "Each user at our establishment must have an access card and a password, and his access to the computer is restricted by menus to the levels of information that concern him."

Ariane also enables the patient to exercise his rights under the *Act respecting Access*, i.e. to truly

see his record if he so wishes. Previously, that was difficult to do in practical terms. He could obtain the record, but would he be able to understand it? Paper records are full of handwritten notes, corrections, additions by the physician or the nurse, often hastily scribbled and hard to make out. The computerized record is standardized, everything is typed, comprehensible, corrections do not erase previous comments, and the development of the patient's condition can be followed and understood.

"And, if a patient wants, his entire record can be easily printed. More and more people are asking to see their records. The reason isn't clear, but it's up substantially. Now, they'll have a file that's adequately maintained and presented. Ariane is also useful in following the user's trail. We also log everything; no transaction takes place without leaving a mark."

Françoise Martin, the CHUS's data base coordinator for the implementation of Ariane, says there are now over five hundred computer terminals in the hospital, in every department and at the bedside of many patients. Patients viewed the machines with some reservation. They had the impression they were being watched, and feared anyone could find out everything about them by pressing a few keys. Many employees had similar fears. It was fairly easy to demonstrate that such is not the case. The screen immediately shows that Ariane has mixed up its threads so that it cannot be trailed. It has sectioned off the labyrinth and put double locks on the door of each section. Anyone who can get around that is pretty clever.

"At first, it was difficult to enforce the rules because the system monitors patients who move from place to place in the hospital," Jacques Monette notes. "Information has to circulate a great deal, as much if not more than the patient, and that's what makes it more difficult to control. To avoid problems, we compensated by tightening access policies even more. We formed a committee that determines access profiles, which must then be approved by the Ariane implementation committee. There's a whole series of security measures, including logs, in addition to disciplinary measures, up to and including dismissal, that are strictly enforced."

Unlike the Laboratoire de santé publique, it has not been necessary to invoke this measure at the CHUS. Some people have tried to overstep their authorization and the sanctions called for have been applied. However, the reaction has focused on raising the staff's awareness of

confidentiality which includes advising them of disciplinary measures. Messages to that effect were displayed on computer screens. Françoise Martin says that the demonstration of deterrent measures was very effective in inculcating discipline and reforming "delinquents".

To overcome patients' fears, their curiosity was whetted by informing them of the role of the computer and the services it provides. "That means more work for the staff," says Jacques Monette, "but the results are worth it. You see it in outpatient clinics, where patients return on a regular basis, some each week. At first, the machines caused them some anxiety. The staff answered their questions, and encouraged them to ask more. Now, patients aren't even aware of the computer, it's part of the landscape."

The approach is slightly different at the Centre hospitalier Gatineau. It is one of five establishments involved in developing the SIDOCI project. This is designed mainly as a clinical record management system that will interact with existing medical and administrative systems. In addition to the security measures of these systems, similar to the ones previously mentioned, SIDOCI will include its own specific measures. Access profiles will be limited in various ways, for instance, by work shift (day, evening, night) and by section of the building (5th floor north). There will also be a menu-driven access profile, so that the user will only be able to access a single part of the record, radiology for instance. Allowance is made for necessary exceptions, such as emergencies, where an "unauthorized access" section has been built in. In this case, security measures are more draconian.

"There are three levels of confidentiality," explains Claude Lévesque, SIDOCI project manager at Gatineau. "A record can be taken from the general level and placed in the "highly confidential" level. That can also be done with parts of the record, or treatment episodes, such as a teenager's therapeutic abortion. Everything concerning this procedure can be withdrawn from her record and transferred to a file accessible only to her attending physician."

There will also be various levels for forwarding a record to a patient: public and private modes. In public mode, a patient could be shown his file with his spouse in attendance, and some information would be withheld, such as information supplied by a third person. In private mode, the patient would have access to the entire file, except information from third persons. Here

again, entry codes and authorizations limit access. Technicians coming from outside to provide technical services will need two codes. Nominative data are encrypted, so they cannot be accessed by external technicians.

Even supplier reports will be logged. Computer rooms will be locked, accessible to a limited and controlled number of people. All the software includes passwords and can be accessed only by cards with bar codes. "When IST's involvement in the SIDOCI became known," Claude Lévesque recalls, "many people expressed apprehension because IST was owned by Industrielle-Alliance insurance company. We didn't share those fears at the hospital because we know how well the system is protected."

"We've even integrated a time lapse into the access function," adds France Nicole, principal consultant with Groupe DMR which collaborated in developing SIDOCI. "If a patient changes unit, users of the previous unit no longer have access to the record after a set period of time. This time lapse can vary with the user's function, physician or nurse." Mrs. Nicole once acted as a guinea pig to demonstrate the security of the computerized system compared to paper records. Without informing his colleagues, Claude Lévesque supplied her with a smock and identity badge. Thus "disguised", she moved about in the hospital, retrieved patient records in a department, and brought them to the office of one of the hospital's executives. "That would have been impossible with a computerized system," Mr. Lévesque concluded. "She wouldn't even have had access to a terminal once the security measures are implemented."

However, before those measures were in place, the Gatineau hospital went through a telling experience. An unauthorized employee showed that he had succeeded in retrieving information to the screen. "Fortunately, the system still wasn't functional at that point, we were still being trained," Claude Lévesque notes. "But it showed us that very strict measures have to be taken."

Professionals at the CHUS expressed other concerns. "Can a stretcher bearer access a patient's records?", some people wanted to know. It was easy to show that was impossible due to access codes and menus. Other demonstrations are more delicate. It was explained that a physician's access to the system could be more restricted than a nurse's. A nurse might be responsible for all the patients in a ward, while the physician is treating only two patients in the same department.

Consequently, the physician would only have access to those patients' records. This is a case where hierarchical habits and human relations have to change, rather than the actual mechanics. The CHUS even called in a psychologist specializing in these issues to deal with people's fears and demystify the changes caused by the arrival of the computer.

"These problems can be overcome fairly easily," Michel Brazeau believes. "You develop the rules and apply them using the tools provided by the computer itself. On the other hand, some problems can only be resolved through education. Regardless of how good the rules and structures are, vigilance is necessary. But vigilance can decline through habit. For instance, an employee may have a problem with the system and turn to his spouse, who is a professional programmer, to step in for the accredited programmer when he is not available. He thinks he is bending the rule for a good reason, but he is giving an unauthorized person access to our data banks, with potentially disastrous results. We must always be on our guard."

Will doctors' offices eventually communicate with hospitals and have to submit to the same rules concerning record access and confidentiality? You might expect physicians to be apprehensive about these rules being extended to their offices but, according to Claude Lévesque, hospitals are the most reticent. He believes the criteria will have to be very strict before they would be willing to send records or parts of records to physicians. Dr. Brazeau replies that in any event, communication does take place, for laboratory examinations among other things, and services will improve when it becomes more general.

Can small hospitals that are unable to afford sophisticated computer systems apply the minimum protection measures? Jacques Monette saw a machine, in a small establishment, locked only with a key that remained on the machine when operator was absent. Anyone could have used it. Many people say it is better not to have a system than one that is not secure.

Everyone agrees that the computer is a fantastic tool and provides ways to control its content. However, the best mechanisms and the best rules cannot be separated from a sense of ethics and individual responsibility. To deal with access to and protection of medical records means constantly educating health professionals to respect their patients as persons.