

MEDICAL COMPUTER SYSTEMS: SECURITY AND SELF-AUDIT

PREAMBLE

The physician is responsible for the safe custody of information obtained in the course of patient care in order to fulfil the ethical precept:

"An ethical physician will keep in confidence information derived from the patient, or from a colleague, regarding a patient and divulge it only with the permission of the patient except when the law requires a physician to do so."

The following minimum guidelines are intended to assist the physician in applying this responsibility to the use of computerized records.

A. GENERAL

1. Databases should not be created without clearly stated objectives. Highly sensitive data and linkages should be identified and appropriate security measures described.
2. Staff (including outside service personnel such as transcription services and maintenance) should be committed by formal agreement to the principles of confidentiality and provided with relevant training.
3. No one should have access to electronic data who does not have access to traditional paper records. The guiding principle should be "Who needs to know?" before access is allowed.
4. A specific written policy should describe the measures in place or to be taken regarding the following aspects of security breach:
 - prevention
 - detection of inappropriate access
 - recovery
5. The system must have in place a monitoring system which creates an audit trail and which both alerts the physician to any inappropriate access and identifies how the system was accessed.
6. A specific written policy should define those procedures to be followed to ensure accuracy and timeliness.
eg. Proofreading lab data after entry.
7. Specific policies should be established for the retention and destruction of data including source documents and paper output. (also see Section C(5) of this statement)
eg. The policy statement that data concerning a patient will be archived if the patient is not seen for two years.

No. 104

B. SOFTWARE

1. Where different levels of access to data are indicated, then the software must ensure the following:
 - Each user is specifically identifiable as belonging to a designated level.
 - User identity is controlled by written policies covering such areas as employee termination or change of level.
 - The body of data to which each level can have access is defined.
 - Functional access, ie. alterations, deletions, data entry, etc., must be defined for each level of access and appropriately controlled by passwords.
2. All access must be entered onto a permanent file log. The software must be capable of identifying and recording where the access originated and by whom. Where alterations are made to the record, then it must be possible to identify by whom, what was altered, and when the alteration was made.
3. A test of the system's backup and recovery must be made on a regular basis.
4. The inventory of all data files must be regularly reviewed and updated.
5. The creation of backup and offsite storage must comply with written policies which are the responsibility of a specific individual. Daily backup and weekly offsite storage are suggested for active files.
6. Encryption or limited ability to link patients with data must be used where indicated by A.1.
7. The system must be capable of reproducing a paper record which contains all documented information that is stored within the electronic record including the dates that the information was entered and the identity of the author of the entry.

C. HARDWARE

1. Fire/heat, water damage and power surge protection is recommended.
2. Uninterruptable power supply is advisable.
3. The equipment and storage media should be secure from theft/vandalism.
4. An inventory control should be maintained for all equipment and media currently in use.
5. When physicians dispose of their office computer hardware, all patient information must first be eliminated. Programs are available which erase data to the level of 'military standards'.

Audit Protocol for Medical Computer Systems

GENERAL:	YES	NO
1. There are clear objectives for the purpose and use of the data base.		
2. Sensitive data and linkages are identified and appropriate security in place.		
3. Staff working with system signs formal agreement of confidentiality.		
4. Staff working with system are provided with pre-employment training relative to security.		
5. Specific written policies describe the measures to be taken regarding prevention of security breach.		
6. Specific written policies describe the measures to be taken regarding detection of security breach.		
7. Specific written policies describe the measures to be taken regarding recovery of security.		
8. A specific written policy defines procedures to be followed to ensure accuracy and timeliness.		
9. There are specific policies for the retention and destruction of data including source documents and paper output.		
10. At least one person in the organization is responsible for keeping up to date on current security issues, eg. viruses.		
11. The system has a comprehensive audit capability.		

No. 104

SOFTWARE:	YES	NO
1. Where different levels of access to data are indicated, answer the following: <ul style="list-style-type: none"> · each user is specifically identifiable as belonging to a designated level. · user identity is controlled by written policies covering such areas as employee termination or change of level. · the body of data to which each level can have access is defined. · functional access, ie. alterations, deletions, data entry, etc., is defined for each level of access and appropriately controlled by passwords. 		
2. All access is entered onto a permanent file log. The software is capable of identifying and recording where the access originated and by whom.		
3. It is possible to identify alterations, by whom they were made, what was altered, and when the alteration was made.		
4. A test of the system's backup and recovery is made on a regular basis.		
5. The inventory of all data files is regularly reviewed and updated.		
6. The creation of backup and offsite storage complies with written policies which are the responsibility of the specific individual.		
7. The electronic record can be reproduced on paper.		

HARDWARE:	YES	NO
1. Fire/heat, water damage, and power surge protection is in place.		
2. Uninterruptable power supply is in place.		
3. The equipment and storage media is secure from theft/vandalism.		
4. An inventory control is maintained for all equipment and media.		
5. When disposing of the computer hardware, all patient information must first be eliminated. Programs are available which erase data to the level of 'military standards'.		

REFERENCE

1. Security & Privacy Guidelines for Health Information Systems, COACH, *Canada's Health Informatics Association* 1995.

First Print PR/05-90
 Revision PR/05-98

**A statement is a formal position of the College with
 which members shall comply.**