Information Management - Security of informational assets

Type :	Policy
No :	
Adopted by :	Board of Directors
Issuer :	
Recipients :	Any person or entity whether employed by the Douglas or not who uses or accesses informational assets of a confidential nature or otherwise on behalf of the Douglas.
Date of adoption :	20 february 2013
Date effective :	12 march 2013

Older versions of this document are available in the 'Archives' section

Foreword

Along with all topics regarding information management, this present policy covers the safety of informational assets. Consequently, the general principles of information management must also be maintained in the application of this policy.

The evolution of the Health and Social Services network relies on the ability of establishments to exchange information in a quick and secure manner. Foreseeing an increased volume of information exchange, and in order to ensure that laws, regulations, and governmental standards regarding the safety of information are respected, the Ministry of Health and Social Services (MSSS) has developed a comprehensive informational assets safety framework.

The Douglas recognizes that information is essential to its current operations and, as such, that it must be subjected to evaluation, appropriate use and adequate security. The Institute acknowledges that it possesses personal information as well as information of a clinical, administrative, legal or financial nature.

Moreover, several laws and policies outline and govern the use of information. The Douglas is subject to and must respect these laws and policies.

Consequently, this present policy on the security of informational assets is set up by the organization in order to ensure the effective, coherent and uniform safety of its informational assets without losing any resources. The safety policy consists of this general policy, which explains the guidelines and the standards that support it.

The goals of the present policy are:

- To ensure that the confidentiality of individuals is respected, and in particular, that any information of a personal nature relating to the patients and employees of the Douglas is kept confidential;
- To ensure the safety of information with respect to the use of computer networks, the RTSS and the Internet;
- To ensure the safety of information with respect to the use of informational assets;
- To ensure the security of the organisation's electronic data;
- To ensure the respect of all legislation regarding the use and processing of information, more particularly personal information and information of a confidential nature that is transmitted or saved using the informational assets;
- To conform but not be limited to the safety measures as stipulated in the *Cadre global de gestion des actifs informationels appartenant aux organismes du réseau de la santé et des services*

sociaux – Volet sur la sécurité (Comprehensive framework for the management of informational assets for organizations in the Health and Social Services Network – Security). The Douglas reserves the right to set up additional safety measures in order to ensure the security of confidential information that it is entrusted with, including related informational assets

Definitions

With the aim of shortening the text, this document will employ the expressions, initials and abbreviations defined below:

Informational assets: Electronic data bank, information system, telecommunications network, telephony, information technology, portable storage, installation of or the whole of these elements. All specialized or ultra-specialized medical equipment can comprise components that belong to the informational assets, particularly when electronically linked to informational assets. Printed documents generated by information technologies are included as well. As an example, informational assets can be, but are not limited to, computers, software, applications, e-mail, the Internet and Intranet, photocopiers, smart phones, tablets, USB keys and any other stationary or mobile computer equipment used within the context of the Institute's mission.

COSAI: Committee on the Security of Informational Assets

DRFI: Financial and Informational Resources Directorate

Incident : Incident related to the safety and confidentiality of the informational assets

User: Any person or entity, regardless of whether employed by the Douglas, that uses or has access to informational assets , which may or may not be confidential, and not necessarily on behalf of the Douglas.

Statement

1.1 Scope of the policy

The present Policy applies to everything concerning the collection, confidentiality and communication of personal information, as well as access to confidential data and informational assets of an electronic nature, including documents produced by information systems.

1.2 Guidelines

The guidelines of the safety of information are based on five functions, forming the French acronym DICAI (Norme ISO 7498-2 : 1989). They are *Disponibilité (*Availability)*, Intégrité, Confidentialité, Authentification* and *Irrévocabilité*, and they are explained as follows:

- **A**vailability: guarantees that information be accessible and usable at the appropriate time and in the required manner by an authorized person;
- **I**ntegrity: guarantees that neither information nor information technology be modified, altered or destroyed without authorization;
- **C**onfidentiality : guarantees that information not be accessible to any unauthorized person
- **A**uthentication : the act of validating the identity of a person or device;
- **I**rrevocability: guarantees that an act is absolute and clearly assigned to the person who performed it, or to the device with which this act was accomplished.

1.3 Fundamentals

- In order to support the policy, certain elements that constitute the basis of the policy must be set up, and continually maintained:
- Directional plan for security
- Awareness and training program for all users;
- Classification of the informational assets;
- Risk analysis and contingency plan;
- Examination and audit of safety measures;
- Acquisition and development of information systems in compliance with the policy;

- Application of a “minimal access privilege” principle.

1.4 Implementation

The Douglas’ Board of Directors, with the recommendation of the Executive Director’s office, will appoint a person in charge of safety who must ensure the application of this policy, and who will be assisted by an informational assets security officer to set up the COSAI. The RSAI delegates the chairmanship of the COSAI to the officer. The roles and responsibilities of each of the parties concerned by the present policy are described in Appendix A and form an integral part of this policy.

This present policy is supported by a series of standards and procedures that must be observed as though they form an integral part of the policy in order to ensure that all objectives of this policy are maintained in the operation of information management. These standards and procedures can be accessed through the links mentioned further in this document.

The documents (policy, standards and procedures) are separated in order to allow for an easier consultation. Information is thus not repeated and documents are inter-related. In the event of a difference between two statements, the information in the document most strongly related to the subject must prevail. When in doubt, the most restrictive statement is to be applied. Appendix B contains links to the different policies, standards and procedures related to information management.

1.5 Standards regarding informational assets security

1.5.1 Standards regarding secure usage

In the security chain, the most important link is the human one. Every user contributes to security on a daily basis. The standard for using informational assets outlines the specific obligations of the user. This standard applies to everything concerning the collection, confidentiality and communication of personal information, as well as access to confidential data and informational assets of an electronic nature, including documents produced by information systems. This includes, but is not limited to, the use of a desktop or laptop computer, as well as several network services, systems or software provided by the Douglas. This standard is to be implemented while respecting confidentiality.

Commitment to confidentiality

Anyone practicing within the Douglas (employee, doctor, professional, trainee, volunteer, etc.) must respect the confidentiality of the information he or she receives directly or indirectly in the execution of his or her functions. A pledge to confidentiality is comprised of two complementary activities of equal importance:

- The manager reviews the confidentiality pledge with each new employee;
- The employee signs the pledge.

1.5.2 Standard of Access

The standard for accessing informational assets, which is an intrinsic part of the policy regarding the security of informational assets, strives to assure the consistent security of informational assets of the Douglas and does so by establishing a formal process for managing and controlling the access rights and codes accorded to users. This standard applies to all systems containing an internal mechanism that permits restriction of access. Precisely, the standard states:

- the conditions according to which a person can have access to informational assets;
- rules related to passwords required to access these assets

The following procedures have been implemented in order to make the standard operational:

a) Procedure for managing computer access

This procedure outlines the information needed and the steps to be followed for the management of access codes for informational assets.
A second procedure covers the specific case of certain employees on the recall list. By the nature of their

status, the employees on the recall list regularly have new positions for an unfixed period and the changes are made on short notice. It is therefore necessary for certain types of employment to adopt a specific procedure to manage access codes.

b) Procedure for requesting remote access

If a person's job requires it, it is possible to have access to certain parts of the network even when outside the telecommunications network of the *ministère de la Santé et des Services sociaux* (Health and Social Services Ministry). The manager responsible for the user must submit a request for remote access. The request must be submitted following the relevant procedure.

c) Procedures for reporting and managing an incident
Any incident related to the usage or security of informational assets must receive immediate attention. The procedure for reporting an incident indicates the steps to be taken when one has witnessed such an incident or has viable reason to believe that such an incident took place or will take place in the near future. Once reported, the incident is handled by the informational assets security officer.
The procedure for managing the incident indicates the actions required to assure the sound management of each incident reported.

1.5.3 Standards for security audit

The standard governing security audits aims to outline the measures required to efficiently protect informational resources. Audits, evaluations, analyses and tests are the means by which network security risks will be evaluated.

1.6 Related policies

The following are examples of policies which, despite the fact that they do not originate from the Financial and Informational Resources Directorate, are linked to information security:

- Policy regarding audio-visual recordings (consent)
- Policy regarding media relations
- Copyright policy – rights and obligations

1.7 Respecting the Policy

The Douglas must investigate any incident relating to information security and must apply the appropriate measures. The management procedure for incidents related to the security and confidentiality of informational assets must be applied in the event of non-compliance.

The Douglas reserves the right to alert the proper authorities of any illegal act, if required.

For preventative measures, the Douglas sets up monitoring network devices and can carry out an analysis of the use of informational assets, whenever required.

Attachment

Appendix_A.pdf

Related Links

Information management Policy – General principles
Information management – Use of informational assets and the Internet
Copyright – Rights and Obligations
Incident Management – usage and security – informational assets
Informational Assets Management Framework