Department of Health

Ministère de la Santé

Diagnostic Imaging Services
PO Box 6600
Charlottetown PE
Canada C1A 8T5

Services d'imagerie diagnostique
C.P. 6600
Charlottetown PE
Canada C1A 8T5

Diagnostic Imaging Procedure

DEPARTMENT	Diagnostic Imaging	**APPROVED BY**	PDIAC
UNIT		**MONITORING**	D.I. Quality Coordinator
TITLE	**Acceptable Use Procedure for Diagnostic Imaging Information Systems**	**EFFECTIVE DATE**	
NUMBER		**NEXT REVIEW**	
REFERENCE #	Acceptable Use Policy for Computer Systems ; IT Security Handbook; IHIS Network AccessPolicy, DIIS Security Policy	**REVISION DATES**	June 2008

Purpose:

Information within the Diagnostic Imaging Information Systems may only be accessed with proper authorization. Staff are entitled to have access to all patient/client information needed to perform his/her assigned work. Access to patient/client information is not permitted to satisfy staffs personal interest. It is not to be shared with other co-workers unless they specifically require the information for their own assigned tasks.

The patient/client must be assured that all electronic records will be accessed only by those individuals who have been given authority to do so.

Information technology security measures are implemented to ensure that the confidentiality and integrity of data are protected. Ensuring that unauthorized access to sensitive data or information, is the responsibility of all persons.

Department of Health
Ministère de la Santé

Diagnostic Imaging Services
PO Box 6600
Charlottetown PE
Canada C1A 8T5

Services d'imagerie diagnostique
C.P. 6600
Charlottetown PE
Canada C1A 8T5

Principles:

Diagnostic Imaging Information Systems (DIIS) contain patient/client and personal information whose confidentiality, integrity and availability must be preserved and protected at all times.

Access to these resources will be granted with the understanding that staff will observe the following:

1. The individual user is responsible and accountable for the use of their DIIS user ID and password. This password must be kept confidential, it is not to be shared with anyone.

2. The individual user is responsible and accountable to sign-off the DIIS system when leaving the workstation.

3. The logged in user is responsible for all functions performed under their username.

4. The individual user is responsible and accountable to use DIIS to access information that is pertinent for them to do their job. They are not permitted to view patient/client information within DIIS for personal use.

5. The logged in user will be held responsible for any violation to unauthorized access for personal use of patient/client information. Any violation of the spirit or intent of these principles may lead to loss of privileges, disciplinary action up to and including termination and/or legal action.

6. The individual user must sign a DIIS Request for Access form. This signed form will be kept on the staff's personnel file.

7. The individual user must have a signed Pledge of Confidentiality on their personnel file.

Any breeches in security or confidentiality must be reported to the individual's on-site supervisor and, if required, to the DIIS operational manager. The breech will be investigated promptly by management. Breeches may result in disciplinary action as per hospital policy.

Responsibilities:

Departmental Managers shall be responsible for :

Diagnostic Imaging Services
PO Box 6600
Charlottetown PE
Canada C1A 8T5

Services d'imagerie diagnostique
C.P. 6600
Charlottetown PE
Canada C1A 8T5

- Determining who needs access to the DIIS system for their staff to perform their job.
- Ensuring a pledge of Confidentiality is on the staff's personnel file.
- Ensuring that the staff has signed the DIIS Request for Access form.
- Contacting DI Manager when staff no longer need access to any of the DIIS systems.

Diagnostic Imaging Managers/ Supervisors shall be responsible for:

- Determining the appropriate DIIS access, needed for the requesting staff to perform their duties.
- Providing training on requested DIIS systems as needed.
- Reviewing user lists yearly to ensure staff on list still has appropriate access.

DIIS support staff will be responsible for:

- Setting up individual users in DIIS.
- Assigning each individual user a username and initial password.
- Providing training support as needed.
- Providing user list for DI manager to review.
- Run random audit reports to ensure patient/client confidentiality is maintained.