Information Security and Confidentiality

Quick Reference Tips

When dealing with computerized health care records, specific confidentiality and security issues must be followed to protect the patient. Also, there are increasing regulations that dictate how these records are handled. There are provincial policies specific to confidentiality protection of security and privacy.

- Your username will keep a foot print of where you are in the system. Therefore you should only access information that is pertinent to your job.
- The system keeps an audit trail, or record, of who enters each chart and when. It records who read the chart and who recorded each piece of information in the chart.
- Do not leave the computer while still signed on.
- Do not access any charts that do not apply to your current job and caseload.
- When selecting a password, don't choose anything obvious, such as your birth date, or spouse and children's names.
- Do not share your password with anyone.
- Your password is your signature.
- Do not write your password down or place under your keyboard.
- Your password is case sensitive and has to be 8 or more characters and should contain one special character.
- If you forget your password you can call the ITSS Help Desk (902-620-3600)
- The system requires you to change your password at regular intervals (every 90 days).
- When you open a chart you will be asked to identify your relationship to the patient, for example RN, consulting physician, etc. if applicable.
- Every employee will not be allowed to see or perform every activity on the computer. For example, a lab technician will be able to see and do more in the lab application than a nurse will.

Confidentiality

Confidentiality is the expectation of privacy of information.

There are three levels of confidentiality:

- None - information that is considered public knowledge, and as such, would not cause any harm to government or any individual should the information be released.
- Normal - information that could cause harm to government or any individual should the information be released.
- High - information that could cause significant hardship or harm to government or to an individual should the information be released.

Access to Information

- You are entitled to have access to all information needed to perform your assigned work.
- Access to information is not permitted to satisfy your personal interests.
- Beware of any attempt by non-authorized personnel to gain access to sensitive information. Report to your manager/supervisor all such attempts.
- For more information refer to the Health PEI Policy.

Computer Use and Access

- Access to the Clinical Information System is restricted to personnel have received training in the system.
- Access to the information personnel view is directly linked their scope of practice.
- All users are uniquely identified by user ID and verified by password before being granted access to any sensitive information.
- Access will be monitored. Each time a chart is accessed a footprint is left in the chart.
- When leaving your computer you must log out or lock the device.

Passwords – Your First Line of Defense

Effective passwords protect your computer and other devices, such as personal digital assistants (PDAs) or Blackberries from being used or abused by others. To check your current computer security, ask yourself the following questions:

- Do I use passwords that someone could easily guess such as my birthday or my child's name?
- Do I use common words found in the dictionary?
- Do I routinely allow my computer to remember this password so I don't have to type it in every time?
- Do I use the same password elsewhere?

If you answered ***yes*** to any of these questions, the information on your computer could be at risk. When selecting a password, your goal is to make it as difficult as possible for someone to guess. This is a small yet critical step in protecting the confidentiality, integrity and availability of information within your workplace.
Create a password that is at least six characters long and is a combination of mixed-case letters and digits, for example **AbGrl4498**. Consider choosing a line or two from a song or poem and use the first letter of each word. For example, "I'm Bud the spud, from the bright red mud" becomes **IBtSftbrm**. Then take a random number and insert it so it becomes **IBtS65ftbrm**.
Examples of effective passwords include: **We2raed?** (Who eats two red apples every day?) **Gt%Real2dY!** (Get real today!). Intentionally misspelling a word is even better, such as: **Git@Rele2dY**

Examples of weak passwords include: **Bbrown123** (user name and simple number) **Scuba41** (hobby with user's age)

- All users are to be uniquely identified by user ID and verified by password before being granted access to any sensitive information stored or processed on departmental computer systems.
- Passwords are to be selected by the user, must contain at least one special character, and should be difficult to guess. Family names, dates, telephone numbers, or words found in dictionaries should not be used as passwords.
- Passwords should be memorized (not written down) and not shared.
- If you are trying to access the CIS Network and have forgotten your password. You must then contact the help desk (902-620-3600) to have this reset.
- Your access will be denied after 6 unsuccessful log in attempts. You must then contact the help desk (902-620-3600) to have this reset.
- Passwords are to be changed at least every 90 days. Passwords should be changed immediately if compromise is suspected.
- The system will remember your previous 8 passwords and will not allow you to repeat one.

Security Incidents

A security incident

- Is any occurrence which did or could compromise the security of information.
- Includes the unauthorized access or attempts of access to sensitive information.

When a security incident has been identified:

- Contact your department manager or supervisor.
- Security and Confidentiality Policy dictates that the department will apply sanctions when a security violation occurs as a result of negligence or misconduct by an employee.
- Such circumstances could lead to administrative, disciplinary or statutory actions.
- For more information contact your manager/supervisor.