Schedule B

Drug Information System Privacy and Security Guidelines for Best Practices

---

1. Purpose

1.1. The purpose of this guideline document is to provide users of the Drug Information System (DIS) with recommended practices to help maintain the confidentiality, integrity, and availability of information collected, used, disclosed, and retained by the DIS.

2. Recommended Security Safeguards

User ID and Passwords

2.1. Pharmacy Software User ID's should be uniquely identifiable.

2.2. Passwords should be at least 8 characters long.

2.3. Passwords should contain characters from at least two of the following classes:

- English upper case letters A, B, C, ...Z
- English lower case letters a, b, c, ...z
- Westernized Arabic numerals 0, 1, 2, ... 9
- Non-alphanumeric characters {} [],.º;:"'?/\`~!#$%^&*()_-+=

2.4. Passwords should not be constructed using only the following:

- Username or User ID
- Any of the user's names
- Names of family, pets, friends
- Email addresses or part thereof
- Words found in a dictionary
- Birthday, address, phone numbers
- Cities
- Company name and derivatives
- Letter patterns like QWERTY, ZXCVBN
- Computer terms
- Any of the above preceded or followed by a digit (e.g., 1Halifax or Halifax1)

2.5. User accounts should be locked-out after 3-10 logon attempts. The lock-out can be permanent or temporary. Temporary lock-outs should be at least one hour.

2.6. Users should change their password at least every 120 days.

2.7. Users should use a different password each time the password is changed. Pharmacy software systems should remember at least the previous 5 passwords and prevent the user from re-using them.

2.8. System and application default passwords should be replaced with strong passwords using the elements described in clauses 2.2 thru 2.4.

2.9. Administrator accounts should require strong passwords.

2.10. Guest accounts should be disabled.

2.11. Access to password files should be restricted.

2.12. Users should be reminded of the following regarding their passwords:

- Don't reveal your password to anyone. This includes your boss, secretary, administrative assistant, family members, helpdesk staff, and co-workers while on vacation.
- Don't use the same passwords for work and personal use (e.g. Facebook, Hotmail).
- Don't talk about your password in front of anyone.
- Don't reveal your password over the phone to anyone.
- Don't reveal your password in an email message.
- Don't hint at the format of your password.
- Don't write your password down.
- Don't store your password in your office, near your computer or on your computer or phone.
- Don't reveal your password on questionnaires or security forms.
- Don't use the "remember password" feature that your browser or some other applications have.

Workstation Controls

2.13. Users should take reasonable precautions to ensure that, if confidential information is displayed on a computer screen, the information is not visible to any person not authorized to view the information.

2.14. Where practical, users should not leave computers unattended when personal health information is accessible. Computers should be configured to enable screen locking when the system is idle or unattended. This screen lock should require a password to reactivate the screen.

2.15. Users should be restricted from saving, copying, or moving any files containing personal health information to their computer hard drive or other medium, e.g. a CD/DVD or USB key.

2.16. Operating system security patches should be applied to all computers in a timely fashion.

2.17. Virus protection software should be installed on all computers in the pharmacy and should be configured to receive automatic updates of virus definition files.

2.18. Host based firewalls (e.g. Windows firewall) should be enabled on workstations and only applications that are necessary for business should be allowed.

2.19. Portable computers such as laptops/notebooks should be fitted with physical lockdown devices. These devices are similar to bicycle locks for portable computers.

2.20. Personal use of the Internet should be discouraged from workstations which connect to the DIS.

User Roles

2.21. User accounts in the Pharmacy Software systems should be role-based.

2.22. User Roles should be mapped to authorized levels of access to personal health information.

Access Logs

2.23. All access to personal health information stored in the DIS is logged and all users of the DIS should be made aware of this.

2.24. Access logs should be reviewed regularly to ensure reasonable access to data by authorized users only and to review login and logout attempts including failed attempts. This review function may be automated using tools that search log files and report defined suspicious activity on an ongoing basis.

Audit

2.25. Privacy and security audits of pharmacy software systems should be carried out annually or more frequently.

2.26. Audits should include the analysis of privacy and security controls and the access to and use of pharmacy software systems.

Networking

2.27. A firewall should be implemented to protect the network within the User Organization.

2.28. An analysis should be conducted to identify any weaknesses and vulnerabilities related to any wireless networks used by the User Organization and mitigations should be identified and implemented where necessary.

2.29. The User Organization should take all reasonable and practicable steps to ensure that all devices connected to the nshealth.ca network use the most up-to-date firewall and anti-virus software and that virus definition patterns are kept current.

2.30. User Organizations should work with their Internet Service Provider to ensure internet connections are of sufficient bandwidth to support efficient access to the DIS and any other internet access requirements they may have.

3. Recommended Privacy Safeguards

Confidentiality Agreements

3.1. User Organizations and Pharmacy Software Vendors should maintain copies of confidentiality agreements signed by staff who require access to the DIS.

Patient Consent

3.2. Dispensing staff should ensure that personal health information obtained from the DIS is not disclosed outside the patient's circle of care without consent of the patient or the patient's substitute decision-maker.

New Patients

3.3. Dispensing staff should obtain the Health Card Number (HCN) or equivalent whenever possible from the patient for encounters that result in queries to the DIS. Searching for a patient by HCN (or equivalent) is the most effective way to locate the patient in the Client Registry.

3.4. Only add an individual to the Client Registry (CR) if an individual cannot be located.

Service Desk

3.5. Calls to a service desk and resulting service desk tickets should not include personal health information.

3.6. Where necessary, personal health information should be sent to support staff via secure methods only (e.g. secure email, secure file transfer).

Privacy Breaches

3.7. In addition to audit logs, a record should be maintained of every privacy and security breach that may have occurred in the DIS and this record should include details of all corrective procedures taken to diminish the likelihood of future privacy and security breaches.

Printed Information

3.8. If it is necessary to print reports and listings of data from the DIS that may include personal health information these should only be printed, displayed, stored, and reviewed in restricted, secured locations to which only authorized users have access.