Policy regarding breach of confidentiality and privacy

"**Material Breach**" includes, without limitation, (i) non-compliance by the Supplier with any provision of this Schedule relating to or resulting from the collection, use, disclosure, storage, disposal or destruction of any Personal Information or Records in contravention of FIPPA and/or this Schedule; and (ii) non-compliance by the Supplier with any other provision of this Schedule that is not cured to the satisfaction of HO, acting reasonably, within 20 days after written notice is given to the Supplier describing the breach in reasonable detail or otherwise within 20 days of the Supplier becoming aware the breach;

19. Notice of Breach and Corrective Action

a) The employee / subcontractor will provide Neo Code with prompt written notice of any actual or anticipated Material Breach, including full particulars of such breach.

b) The employee / subcontractor will co-operate fully with Neo Code in preventing the occurrence or recurrence of any breach of this Schedule, including, if requested to do so: (i) by preparing a written proposal to address or prevent further occurrences; (ii) complying with the reasonable directions of Neo Code; and (iii) taking all reasonable steps to recover or obtain any Records that have come into the custody or control of third parties contrary to FIPPA or this Schedule.

2.4 Breach of Confidentiality

Individuals will be held accountable for breaches of confidentiality.

Breaches of confidentiality include intentional and unauthorized access to, use and/or disclosure of, confidential information.

All Neo Code employees and sub-contractors have a responsibility to report breaches of confidentiality without fear of reprisal.

If it is established that a breach of confidentiality has occurred, those individuals deemed responsible may be subject to penalty or sanction up to and including termination of employment, cancellation of contract or services, termination of the relationship with Neo Code, withdrawal of privileges and/or legal action.

Examples of Breaches (What you should NOT do)
These are examples only. They do not include all possible breaches of confidentiality covered by the VIHA Confidential Information - Privacy Rights of Personal Information Policy and the Confidentiality agreement.

Source: http://www.viha.ca/NR/rdonlyres/A0E34A34-ABAC-4FBE-9F2E-55387851A292/0/policy_personal_information.pdf

Issuing Authority: Chief Executive Officer, VIHA
Date Issued: June 12, 2002
Date Last Reviewed (r)/ Revised (R): June 30, 2009 (R) , CA form added July 24, 2009
Policy Relationships: Corporate
General Administrative: Corporate
Effective Date: June 12, 2002
Section Number: 1.0
Sub-section Number: 1.5
Policy Number: 1.5.1

Accessing information that you do not need to know to do your job:
• Unauthorized reading of a patient's chart.
• Accessing information on yourself, children, family, friends or co-workers.
• Asking co-workers for information that you do not need to do your job.
• Showing, telling, copying, selling, changing, or disposing of confidential information that is not pertinent to your role or care activity.

Providing access to your sign-on code and password for computer systems:
• Telling a co-worker your password so that he or she can log in to a computer system.
• Telling an unauthorized person the access codes for employee files or patient information.
• Leaving your password in plain view so that others may know it.

Providing or gaining unauthorized access to physical locations (e.g. file cabinets) which contain confidential information
• Lending out your keys to someone else to access file cabinets, file storage areas or other areas where confidential information is stored, OR using another's keys for the same purpose
• Leaving file storage areas unlocked when they should be locked.

Leaving a password protected application unattended while signed on:

- Being away from your desk while you are logged into an application.
- Allowing a co-worker to use your application for which he/she does not have access after you have logged in.

Sharing, copying or changing information without proper authorization:
- Making unauthorized marks on a patient's chart.
- Making unauthorized changes to an employee file.
- Discussing confidential information in a public area such as a waiting room or elevator.

Using another person's sign-on code and password:
- Using a co-worker's password to log in to a VIHA computer system.
- Unauthorized use of a log-in code to access employee files or patient accounts.
- Using a co-worker's application for which you do not have rights after he/she is logged in.

Failing to report a breach of confidentiality
- Being aware of a breach of confidentiality, but not reporting the breach to your supervisor or other designated individual.
- Not reporting that your password to a computer system has been compromised or that you have lost keys to a storage location for confidential information.