Vancouver CoastalHealth
Promoting wellness. Ensuring care.

DATE: February 1, 2011

TO: All Researchers, Research Coordinators, Research Assistants, Summer Students & others using VCH Patients/Clients' Personal Information

FROM: Vancouver Coastal Health Authority's Information Privacy Office (IPO)
Vancouver Coastal Health Research Institute (VCHRI)

RE: BEST PRACTICES REGARDING PRIVACY & RESEARCHERS

As a public body under the BC *Freedom of Information and Protection of Privacy Act* (FIPPA), Vancouver Coastal Health Authority (VCH) is responsible for protecting the privacy of all personal information in its custody and/ or within its control. "**Personal Information**" means recorded information about an identifiable individual, including electronic and printed records, excluding business contact information.

As custodians of patient's/client's Personal information that may be used in research, researchers and research staff, including coordinators, research assistants, summer students, and anyone else involved with the research, need to take care in their handling and storing of such data. There are potential consequences whenever a privacy breach occurs that ranges from fines under FIPPA (up to $2000 per individual or up to $500,000 per corporation); or notification of all affected patients/clients about what happened to their Personal Information (depending on the specific facts and circumstances); or reporting to the Office of the Information and Privacy Commissioner's office (OIPC). If identity theft of the patients/client's Personal Information is a major possibility, VCH may need to provide the patients/clients with credit monitoring for a year. The costs of providing that service could escalate into the thousands of dollars depending on how many patients/clients were affected. Costs of this service may be attributed back to the researcher's department.

Best Practices for researchers and research staff from a privacy perspective:

- Use complex and strong passwords on your computers, laptops, or other information storage devices (eg. Upper Case, Lower Case, numbers and 8 or more characters).

- All information must be stored on a secure area of a network server where access is limited to only those staff that "need to know" and not on a C:drive.

- Only de-identified information should be transported, stored, etc but if this is not possible, then any Personal Information must be encrypted and/or if contained on a mobile device it must have encryption that is in compliance VCH IMIS security standards.

- Only the minimum amount of Personal Information should ever be collected.

- Any Personal Information that is no longer needed or required to be kept, should be deleted as soon as possible and not retained. Otherwise shred or destroy all research data containing Personal Information after the project is complete within the required data retention period established by the Research Ethics Board or VCH policy.

- Review VCH's current policies and procedures on handling and transporting Personal Information of patients/clients outside the office. These or similar UBC policies might also be reviewed as a reminder when handling and transporting Personal Information of patients/clients outside the office. Refer to UBC Policies #104 (Responsible Use of Information Technology Facilities and Services), #106 (Access to and Security of Administrative Information) and #117 (Records Management): http://universitycounsel.ubc.ca/policies/index/.

- Whenever there is a stolen or loss of a device or document that contains Personal Information, it must be reported **As Soon As Possible** to the supervisor/manager/privacy office as an immediate investigation needs to determine the risk of harm, containment, and possible notification if applicable and OIPC involvement. The concern is primarily identity theft/identity fraud where the patients/clients affected must be notified so they can take necessary precautions to protect their information (notifying their bank or financial institutions, flags on their PHN, etc).

- Researchers must abide by their projects protocols and security and compliance requirements as set forth via the Research Ethics Boards or other documentation about their project.

- Use study IDs in place of name or PHN or other personal identifiers if possible.

- A personally owned laptop should not be used for VCH research projects as it may not have proper security standards in place.

- Be careful when using email. It should only be an email account within the VCH firewall. No email should have Personal Information or personal identifiers listed in the body or attachment of an email unless it is ENCRYPTED. This encryption must be in accordance with VCH Security Services standards. No email attachment that contains Personal Information should be forwarded unless it is encrypted. Please edit your email dialogue messages and only send to those who “need to know” to do their job.

For additional questions related to information privacy: Contact the VCH Information Privacy Office (IPO) at **privacy@vch.ca** or **604-875-5568** or go to the IPO intranet site for privacy reminders and VCH Guidelines on Encryption at Information Privacy Office.