OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

F08-06-MS **Laptop Theft Illustrates Need for Security Policy for Portable Storage Devices**

A laptop containing sensitive medical information was stolen from a public body's contracted agency. The personal information of 53 families on the laptop was neither encrypted nor password protected. The public body owning the laptop reported the theft to the police and sent reminders to staff about the physical security policies of the workplace and building.

On assessing the risk associated with the breach, the public body correctly determined that it needed to notify the affected parties and did so. It then notified our office as well. In addition to recommending improvements to future notification letters, we examined and commented on the public body's security policies.

The public body already had prevention strategies in place, including privacy breach guidelines. We recommended that it also incorporate the four key steps for responding to privacy breaches, posted on our website at http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf

We also recommended further prevention strategies to safeguard against future breaches, including

- conducting annual privacy audits;
- entering information and privacy management confidentiality agreements with contractors;
- conducting privacy, security and confidentiality training; and
- developing portable storage device security policies.

Security on portable storage devices is an important safeguard in the prevention of privacy breaches, and we recommend that all public bodies adopt the following standards to ensure compliance with the requirement under section 30 of the *Freedom of Information and Protection of Privacy Act* for reasonable security arrangements for the protection of personal information:

(1) Storage of personal information on local hard drives and portable storage devices should be generally prohibited. Staff should be

required to access personal information only through secure connections to a secure server.

(2) Storage on local hard drives and portable storage devices should only be permitted when absolutely necessary. If such storage does occur, policy should require that only the minimum amount of personal information needed be stored and only for the minimum amount of time necessary.

(3) Personal information must be immediately deleted after use or stored on a secure network drive as soon as possible.

(4) Personal information stored on a local hard drive or portable storage device must be encrypted; password protection is not sufficient.

(5) Laptops must be cable locked to desks during use and must be stored inside a locked cabinet or desk when not in use.

(6) While in transit, laptops must not be left unattended.