Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

News Release

For Immediate Release
Sept. 30, 2015

More attention needed by Health Authorities to avoid future privacy breaches

VICTORIA—Elizabeth Denham, British Columbia's Information and Privacy Commissioner is calling for immediate action to address gaps in the privacy breach management practices of B.C.'s health authorities following the release of today's report, *Examination of British Columbia Health Authority Privacy Breach Management*.

Breaches of citizens' personal information occur when there is unauthorized access, use, loss, disclosure or disposal of that information. The growing reliance on electronic records has made privacy breaches more prevalent, affecting citizens in greater numbers.

"Health authorities collect our most sensitive personal information. Strong policies, compliance monitoring and training of health care providers and staff are essential to protect the privacy rights of the citizens of B.C.," said Commissioner Denham.

"Serious breaches – those involving a large number of people or those involving the compromise of one's sensitive health or financial information – can cause significant damage and uncertainty. However, when sound management practices are followed most breaches of personal data can be avoided."

The Office of the Information and Privacy Commissioner launched this examination to help health authorities reduce the incidence of health sector data breaches. The review follows the release of a previous report in January 2015 that examined privacy breach management within the B.C. government.

The most common types of breaches within health authorities include lost or stolen records, misdirected communications, unsecured or unencrypted data, inappropriate access (including "snooping" in electronic health records) and deliberate social media disclosures.

Findings in the report highlight a need in many health authorities for:

- increased compliance monitoring and risk assessment in order to identify gaps in privacy management programs and proactively resolve issues before breaches occur;

- greater awareness by all staff, through regular mandatory training, regarding their duties and responsibilities for ensuring privacy and security of personal information;
- stronger governance and leadership in creating a culture of privacy; and
- a review of resources to ensure that privacy officers are equipped with the staff and tools needed to build and maintain adequate privacy management programs.

“I have made 13 recommendations for immediate preventative action which will protect personal information and build trust with citizens,” said Denham.

Many jurisdictions around the world are building explicit accountability requirements into their legislation and policies, including mandatory breach reporting for the public sector.

“I believe it is time for all public bodies and private sector organizations in B.C. to move from simply reacting to events like breaches to undertaking a strong proactive approach. Health authorities need to implement or strengthen the management processes outlined in this report, along with the provisions in the OIPC’s guidance document *Accountable Privacy Management in BC’s Public Sector*, in order to meet their legislative obligations.”

Examination of British Columbia Health Authority Privacy Breach Management is available for download at https://www.oipc.bc.ca/report/audit-compliance

Media Contact:
Jane Zatylny
Communications Officer
250-415-3283
jzatylny@oipc.bc.ca

BACKGROUNDER

What is this report about?

Examination of British Columbia Health Authority Privacy Breach Management is the second project under the Office of the Information and Privacy Commissioner ("OIPC") Audit and Compliance Program.

This report addresses the degree to which health authorities effectively manage privacy breaches.

Who did the OIPC examine?

The OIPC examined eight B.C. health authorities: Fraser Health, Interior Health, Island Health, Northern Health, Vancouver Coastal Health, Provincial Health Services Authority, Providence Health Care and First Nations Health Authority.

Why did the OIPC choose to review breach management within health authorities?

We chose health authorities because they collect and store the most sensitive personal information from British Columbians. Whether it's an HIV test, mammogram or routine blood-work results, citizens of this province rely on their health authorities to protect their privacy and safeguard their personal data.

When did this review take place, and what did it involve?

The review was announced on April 10, 2015, and data and information were collected between April and June 2015. We reviewed written policies and statistical information and interviewed key health authority staff.

What were the gaps that concerned you in this examination?

Although the gaps are not consistent across all health authorities, examples of gaps identified through this examination include:

- minimal analysis of the causes of breaches within some of the health authorities;
- lack of follow-up in some health authorities regarding whether preventative measures are implemented after a breach occurs;
- few health authorities ensure the timely reporting of breaches to the head of the health authorities, as required by the *Freedom of Information and Protection of Privacy Act* ("FIPPA");
- there is no threshold or trigger for when health authorities report breaches to the OIPC or affected individuals;
- some health authorities fail to track participation in privacy training; in others the participation is relatively low;

- proactive physical on-site audits of safeguards do not happen regularly;
- electronic tracking systems for managing breaches lack utility for proactively analyzing patterns or trends; and
- no common coding system across the health authorities to track and compare types of breaches.

What are your recommendations?

We made 13 recommendations to help the health authorities improve their breach management programs, including:

- more work needs to be done to analyze the causes of breaches and to ensure that preventative measures are in place;
- health authorities need to regularly audit privacy and security safeguards;
- breaches should be reported to the OIPC if they can be expected to cause harm or if they involve a large number of individuals;
- timely information about breaches must be communicated to the heads of the health authorities, as required by FIPPA; and
- everyone who accesses personal health information must participate in regular refresher training.

What else should health authorities do to improve?

Executives need to do more to provide their privacy offices with the resources and tools to implement these recommendations. This is not a job that should be left solely to privacy officers. Leadership needs to take a stronger role in cultivating and promoting rigorous data security and privacy controls.

Are health authorities obligated to report privacy breaches to the Commissioner or the public?

No. While many Canadian provinces or territories have mandatory breach reporting requirements in the health sector, it is not a legislated requirement in B.C. In the absence of a legislative amendment, the Commissioner has recommended that health authorities promptly and directly notify affected individuals and report all suspected breaches to this Office if they involve personal information, can be expected to cause harm, and/or involve a large number of individuals.

Media Contact:
Jane Zatylny
Communications Officer
250-415-3283
jzatylny@oipc.bc.ca