RISK NOTE

Subject: Confidentiality and Contracted Data Services

When entering into a contractual arrangement with a third party for data services, especially with a private corporation, Health Care Agencies (HCAs) must pay particular attention to their legal obligations to ensure all patient care information in their custody remains confidential. HCAs must take all necessary precautions to comply with the *Freedom of Information and Protection of Privacy Act* ("FOIPPA"). The Information and Privacy Commissioner for B.C. ("Commissioner") has issued "Guidelines for Data Services Contracts OIPC 01-02" dated May 8, 2003 ("Guidelines") for use by public bodies (including HCA's) that contract out the processing or storage of information including: personal information; the operation or management of computerized systems containing personal information; or services involving the collection, use or disclosure of personal information. These Guidelines can be found on the Commissioner's website at: http://www.oipc.bc.ca/advice/Guidelines-Data_services.pdf.

The Commissioner has stressed the importance of maintaining public confidence in the handling of personal information by public bodies. Issues raised include use or disclosure of personal information by unauthorized personnel, compromised integrity of personal information, accidental disclosure of personal information, improper use or disclosure of personal information and improper retention or secondary use of personal information. The Guidelines state that contracts between public bodies and service providers must contain provisions requiring compliance with FOIPPA. The HCA may include any further requirements for compliance in any internal privacy policies. The public body is also expected to monitor performance of the service provider, for example, by conducting periodic audits of its records and practices.

While the Guidelines are not mandatory, they will be considered if an HCA is ever investigated for compliance with FOIPPA. Therefore, we recommend that HCAs follow the Guidelines.

The HCA should involve its own privacy staff in the contract process. The contract should clearly spell out FOIPPA requirements, as well as any additional privacy duties and obligations the contractors will need to meet (including, but not limited to, keeping data stored within Canada to protect it from foreign legislation such as the *Patriot Act* in the USA: http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foippa/usa_patriot_briefing.pdf.

The Health Care Protection Program (HCPP) recommends that HCAs consult their legal counsel in establishing standard form privacy provisions. The complexities of individual contracts must be considered when determining the appropriate privacy provisions in any data service contract. Refer to the Guidelines which set out a recommended list of important contractual provisions.

One of the Commissioner's recommendations within the Guidelines is that public bodies contracting out personal information services should carry out a Privacy Impact Assessment ("PIA") before making a final decision to contract out personal information services. A model PIA tool can be found at http://www.oipc.bc.ca/index.php?option=com_content&view=article&catid=16%3Aresources-for-public-bodies&id=80%3Apublic-sector-g-privacy-impact-assessment-pia&Itemid=76.

The Commissioner also recommends that public bodies review the information management and information technology privacy and legislation available through the Ministry of Labour, Citizens' Services and Open Government website at:. http://www.cio.gov.bc.ca/cio/kis/infomgmt/index.page. The website contains links to a Privacy Protection Schedule (PPS) designed for use by public bodies http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foippa/pbpps.doc . The PPS is a document which can form part of any contract and addresses privacy issues in detail.

We recommend addressing the following additional issues in contracts:[1]

1. Establish a process by which the public body has control over the employees of the contractor (or sub-contractor) to the extent that the public body has the right to approve any such employees or have them removed from its premises for certain reasons such as breach of security provisions, etc.

2. Require the contractor to have their employees sign a confidentiality agreement which ensures they adhere to the provisions of FOIPPA.

3. Restrict the disclosure of personal information by the contractor (or sub-contractor) to its employees to that which is necessary for the performance of the duties of the employee.

4. Restrict the disclosure of personal information by the contractor (or sub-contractor) to third parties. Disclosure to third parties should only be allowed subject to the public body's prior written consent. The third parties must agree to be bound by the provisions of FOIPPA as if they were the HCA.

---

[1] Washington, Penny, *"Recent Developments in Freedom of Information & Protection of Privacy Law"*, Bull, Housser & Tupper Health Care Newsletter, March 2002, pp. 1 and 5. http://hcpp.org/content/pdfstorage/16996473592920092234 5PM95775.pdf . We caution that this should not be considered legal advice and we recommend each public body consult its own legal counsel when entering such contracts.

5. Set out clear rights of the public body in the event the contractor, a sub-contractor or a third party does not comply with the terms of the contract (and in particular, with the terms of FOIPPA). Examples include the right to seek injunctive relief, to terminate the contract and to demand the return of all personal information in the possession of the offender, etc...

HCA Sensitive Information

In addition to protecting personal information under the *Freedom of Information and Protection of Privacy Act*, there may be circumstances where HCA contracted services are considered highly "sensitive" in nature. Sensitive information means personal information as defined under FOIPPA and other information considered confidential or sensitive to the HCA. This may include, but is not limited to: budget information, proprietary information, records related to Treasury Board Submissions, records whose release may cause financial hardship or harm to the HCA, the public interest or a third party, or where the release of the information may be expected to compromise the anticipated delivery of services posing a high risk to the HCA.

For contracts involving sensitive information we recommend utilizing Schedule G Security which forms part of the government General Service Agreement (GSA) located on the Procurement and Supply Services website at: http://pss.gov.bc.ca/psb/gsa/gsa_index.html. Security screening of the contractor may also be required when dealing with sensitive information. Schedule G – Procedures, Appendix G1 and Appendix G6 can assist the HCA with screening of contractors. Schedule G is not recommended for low risk services that do not have particular security concerns.

Personal Information Leaving the HCA

HCPP recommends that any time an HCA releases private information that is anticipated to leave their premises, the data should be encrypted. The service provider must be required to maintain at least an equivalent level of confidentiality as would the HCA itself in the terms of the contract. Information on laptops, blackberries and other portable devices should be subject to similar protection. At a minimum all information and all hardware devices should be password protected.

Sample Insurance and Indemnity Language

To assist the HCA, the GSA link above (under Information Technology & Management Consulting Professional Services) also provides the most recent insurance (Schedule D) and indemnity (Schedule F – including allowable limitations of liability) language used in government IT contracts. These schedules, which are intended to be used together, were negotiated between the province (Risk Management Branch) and the four largest IT companies.

More Information

We have included a link to an investigation report completed by the Privacy Commissioner relating to improperly securing personal information for your review. The document provides valuable information to assist any HCA in the protection/mitigation of personal information in both contracted and non-contracted data services: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-02.pdf

January 2010
Links updated: December 2011

Published by the Health Care Protection Program