OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

Order F14-45

MINISTRY OF HEALTH

Elizabeth Barker
Adjudicator

November 4, 2014

Quicklaw Cite: [2014] B.C.I.P.C.D. No. 48
CanLII Cite: 2014 BCIPC 48

Summary: The applicant requested access to records related to data sharing and research agreements between the Ministry of Health and four individuals, including information about delays or impediments to accessing data for research purposes. The Ministry refused to disclose some information in the responsive records under ss. 13, 15(1)(a), 15(1)(l) and 22 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The Ministry established that disclosure of some of the information at issue could reasonably be expected to harm a computer system, so could be withheld under s. 15(1)(l). However, the Ministry did not prove that disclosure would be harmful to law enforcement, so it was not authorized to refuse to disclose information under s. 15(1)(a). Nor did the Ministry establish that it was authorized under s. 13 to withhold policy advice or recommendations because that information had already been disclosed elsewhere in the records. Finally, the adjudicator ordered disclosure of most of the information that was withheld under s. 22(1) because disclosure would not be an unreasonable invasion of third party personal privacy.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, ss. 13. 15(1)(a), 15(1)(l) and 22(1), 22(2)(a), 22(2)(h), 22(3)(d), 22(4)(e), 22(4)(f). *Financial Administration Act*, [RSBC 1996] Chapter 138.

Authorities Considered: B.C.: Order 36-1995, [1995] B.C.I.P.C.D. No. 8; Order 39-1995, [1995] B.C.I.P.C.D. No. 12; Order 50-1995, [1995] B.C.I.P.D. No. 23; Order 00-10, 2000 CanLII 11042 (BC IPC); Order 00-53, 2000 CanLII 14418 (BC IPC); Order 01-15, 2001 CanLII 21569 (BC IPC); Order 01-22, 2001 CanLII 21576 (BC IPC); Order 01-48, 2001 CanLII 21602 (BC IPC); Order 01-53, 2001 CanLII 21607 (BC IPC); Order 02-38, 2002 CanLII 42472 (BC IPC); Order 04-20, 2004 CanLII 45530 (BC IPC);

Order F06-16, 2006 CanLII 25576 (BC IPC); Order F07-15, 2007 CanLII 35476 (BC IPC); Order F08-03, 2008 CanLII 13321 (BC IPC); Order F10-15, 2010 BCIPC 24 (CanLII); Order F10-21, 2010 BCIPC 32 (CanLII); Order F11-13, 2011 BCIPC 3 (CanLII).

Cases Considered: *John Doe v. Ontario (Finance), 2014 SCC 36; British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner), 2012 BCSC 875.*

INTRODUCTION

[1] This inquiry is about a request by the BC Freedom of Information and Privacy Association ("applicant") to the Ministry of Health ("Ministry") for access to the following records for the time period January 1, 2011 to August 2, 2012:

- Data sharing and other agreements involving the Ministry and four named individuals;
- Correspondence between the Ministry and the four named individuals relating to the agreements, particularly correspondence about delays or impediments to accessing data for research purposes;
- E-mails, memos or other notices to staff from the Ministry's Assistant Deputy Minister of Information Management/Information Technology Division regarding delays or impediments to the release of data to researchers; and
- Any policy changes relating to release of data to researchers.

[2] The Ministry refused to disclose any information in the responsive records, citing ss. 14 (solicitor-client privilege), 15 (harm to law enforcement) and 22 (harm to third party personal privacy) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). The applicant requested that the Office of the Information and Privacy Commissioner ("OIPC") review the Ministry's decision.

[3] During the review, the Ministry reconsidered its response to the applicant's request. It decided to disclose some information, but withheld other information under ss. 13, 15(1)(a), 15(1)(f), 15(1)(l), 17 and 22. It also decided to withhold some records entirely under s. 3 (outside the scope of FIPPA). The issues in dispute were not resolved at mediation, and the applicant requested that they proceed to inquiry.

[4] In its initial inquiry submissions, the Ministry explained that it was no longer withholding records under s. 3 or refusing to disclose information under

ss. 15(1)(f) or 17.[1] The Ministry clarified that it was only relying on ss. 13, 15(1)(a), 15(1)(l) and 22 of FIPPA.

ISSUES

1. Is the Ministry authorized by s. 13 to refuse to disclose information because disclosure would reveal advice and recommendations developed by or for a public body or minister?
2. Is the Ministry authorized by s. 15(1)(a) of FIPPA to refuse to disclose information because disclosure could reasonably be expected to harm a law enforcement matter?
3. Is the Ministry authorized by s. 15(1)(l) of FIPPA to refuse to disclose information because disclosure could reasonably be expected to harm the security of any property or system, including a building, a vehicle, a computer system or a communication system?
4. Is the Ministry required to withhold information under s. 22 of FIPPA because disclosure would be an unreasonable invasion of third party personal privacy?

[5] The Ministry has the burden of proof, under s. 57(1) of FIPPA, to establish that s. 13 and 15 authorize it to refuse to disclose the requested information. However, s. 57(2) of FIPPA places the burden on the applicant to establish that disclosure of personal information contained in the requested records would not unreasonably invade third party personal privacy under s. 22 of FIPPA.

DISCUSSION

[6] **Background**—In 2012 the Ministry commenced an investigation of its Pharmaceutical Services Division regarding inappropriate data access, intellectual property infringement, standard of conduct violations, inappropriate procurement practices, contracting irregularities and suspected conflicts of interest. Around the same time, the Office of the Comptroller General ("OCG") also began an investigation into suspected financial improprieties in the procurement and contracting practices of the Pharmaceutical Services Division. At the time of this inquiry, the Ministry's investigation had concluded but the OCG investigation was still ongoing.

[7] **The Records**—The information at issue is contained in the following records, all of which are dated between January 1, 2011 and August 2, 2012:

[1] Ministry's initial submissions, paras. 3.01-3.02.

1. an *Information Sharing Agreement* between the Ministry and the University of Victoria ("UVic");[2]

2. an *Information Sharing Agreement*, a *Contribution Agreement* and an *Amended Transfer Under Agreement* between the Ministry and the University of British Columbia ("UBC");[3]

3. two *General Service Agreements* and an *Amendment Agreement #1* between the Ministry and a contractor;[4]

4. an *Undertaking of Confidentiality and Security* signed by the same contractor; [5] and

5. emails between Ministry employees and individuals at UBC and/or UVic.

[8] **Policy advice or recommendations**—Section 13(1) of FIPPA provides that the head of a public body may refuse to disclose information that would reveal advice or recommendations developed by or for a public body or minister. The Ministry withheld the body of only one email under s. 13(1).[6] I note that the Ministry has already disclosed all of this email to the applicant elsewhere in the records.[7]

[9] The Ministry does not explain why it chose to disclose information in one instance but not in another. Absent any logical explanation, in my view, it would be a perverse result to find that the Ministry may refuse disclosure of this information under s. 13(1). Therefore, I find that the Ministry is not authorized under s. 13(1) to refuse to disclose to the applicant the information in dispute in the email on pages 254-255.

[10] **Disclosure harmful to law enforcement** – The Ministry has relied extensively on ss. 15(1)(a) and (l) to withhold information from the responsive records. These sections read as follows:

> 15(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to
>
> (a) harm a law enforcement matter,
>
> ...
>
> (l) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

[2] Pages 1-59.
[3] Pages 145-166, 167-183 and 184-245, respectively.
[4] Pages 77-139 and 140, respectively.
[5] Pages 356-57.
[6] On pp.254-55. The email addresses and subject line have *not* been withheld.
[7] Pages 271-72.

[11] In order to prove that ss. 15(1)(a) and/or 15(1)(l) apply, the Ministry must establish that there is a clear and direct connection between the disclosure of the information in question and the harm that is alleged. Although there is no need to establish certainty of harm, it is not sufficient to rely on speculation.[8] In Order F07-15,[9] former Commissioner Loukidelis outlined the evidentiary requirements to establish a reasonable expectation of harm:

> …there must be a confident and objective evidentiary basis for concluding that disclosure of the information could reasonably be expected to result in harm… Referring to language used by the Supreme Court of Canada in an access to information case, I have said 'there must be a clear and direct connection between disclosure of specific information and the harm that is alleged'.

[12] Further, in *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner),*[10] Bracken, J. confirmed it is the release of the information itself that must give rise to a reasonable expectation of harm, and that the burden rests with the public body to establish that the disclosure of the information in question could reasonably be expected to result in the identified harm.

Law enforcement matter — s. 15(1)(a)

[13] The first step in determining whether s. 15(1)(a) applies is to determine whether the activity to which the information in question relates is a "law enforcement" matter.[11] Only if it does, is it then necessary to consider whether disclosure of the information could reasonably be expected to harm that law enforcement matter. Schedule 1 of FIPPA defines "law enforcement" as follows:

> "law enforcement" means
>
> (a) policing, including criminal intelligence operations,
>
> (b) investigations that lead or could lead to a penalty or sanction being imposed, or
>
> (c) proceedings that lead or could lead to a penalty or sanction being imposed;

[14] The Ministry submits that disclosure of the information withheld under s. 15(1)(a) could reasonably be expected to harm two ongoing law enforcement matters, namely an investigation by the OCG and an investigation by the

[8] Order 00-10, 2000 CanLII 11042 (BC IPC), at p. 10.
[9] Order F07-15, 2007 CanLII 35476 (BC IPC) at para. 17.
[10] 2012 BCSC 875, at para. 43.
[11] Order 01-48, 2001 CanLII 21602 (BC IPC).

RCMP.[12] The applicant submits that it is not clear that there is any activity currently underway or anticipated by any government or police body which would fall within the definition of law enforcement in FIPPA.[13]

OCG investigation

[15] The Ministry states that in 2012 the OCG commenced an investigation into alleged contraventions of government financial policy, conflicts of interest and misuse of public funds in the Ministry's Pharmaceutical Services Division, and that the OCG investigation is ongoing.[14] The OCG's senior investigator's evidence is that the records at issue in this inquiry are amongst those being considered in the OCG investigation.[15] Although I am satisfied that an OCG investigation exists, in order for s. 15(1)(a) to apply to the information at issue, I must first decide whether OCG's investigation constitutes "law enforcement".

[16] Previous orders have found that in order for a public body's investigation to meet the definition of law enforcement, the public body must have a specific statutory authority to conduct the investigation and to impose sanctions or penalties.[16] Other orders have expanded this requirement by adding that a public body's investigation can still meet the definition of law enforcement even if the public body is not itself empowered by statute to impose penalties or sanctions, as long as its investigation materials form part of the investigation of a second public body that does have that statutory authority.

[17] For example, in Order 36-1995, former Commissioner Flaherty found that the Ministry of Environment did not have statutory authority to conduct an investigation or impose penalties when, as allowed under the terms of their contract, it audited the Saturna Island Recycling Committee's financial statements. The Ministry had argued that the information in dispute might have resulted in a criminal prosecution, if the Ministry or the independent auditors had found irregularities and asked the Attorney General to become involved. That did not occur, however, as no irregularities were found. The Commissioner wrote:

> The definition of law enforcement in British Columbia requires, in my view, that a public body have a specific statutory authority to conduct the investigation and to impose sanctions or penalties.
> …

[12] Ministry's initial submission, para. 4.24 and Ministry investigator's affidavit, para. 10.
[13] Applicant's reply submission, paras. 16 and 29.
[14] Ministry's initial submissions, paras. 4.21-22.
[15] Ministry's initial submission, OCG's senior investigator affidavit, para 20.
[16] Order 36-1995, [1995] B.C.I.P.C.D. No. 8; Order 39-1995, [1995] B.C.I.P.C.D. No. 12; Order 01-22, 2001 CanLII 21576 (BC IPC); Order F08-03, 2008 CanLII 13321 (BC IPC); Order F11-13, 2011 BCIPC 3 (CanLII).

> Until such time as the information becomes part of such an investigation, the law enforcement exceptions do not apply to it.[17]

[18] As far as I can discern, the issue of whether an OCG investigation is a law enforcement matter has been considered only once before by the Commissioner, in Order 50-1995.[18] That case involved a forensic audit conducted by the OCG into alleged "double dipping" and conflict of interest. The records at issue were the handwritten answers to the auditor's questions. The OCG's audit materials were given to a special prosecutor appointed by the Attorney General to determine if there was sufficient evidence to lay criminal charges and prosecute. Due to that fact, the Commissioner found that OCG's audit process was a law enforcement matter because it could have led to a penalty or sanction being imposed.

[19] More recently, in Order F11-13,[19] former Adjudicator Fedorak examined the BC Corners Services reliance on s. 15 to withhold information from policy and procedures documents. The submissions included evidence that police departments rely on the BC Coroners Service investigations for information that is critical to criminal investigations and can lead to prosecutions and penalties and sanctions under the *Criminal Code*. He found that on their own coroners' investigations do not constitute law enforcement because coroners are not empowered to impose penalties or sanctions. However, in cases where a coroner's investigation actually forms part of a criminal investigation by police, it meets the definition of "law enforcement" under FIPPA.

[20] Turning back to the present case I have considered whether the OCG has the statutory authority to investigate and impose sanctions or penalties. The Ministry submits that s. 9(e) of the *Financial Administration Act*[20] provides the OCG with a statutory responsibility "to evaluate financial management throughout the government and recommend to the Treasury Board improvements considered necessary".[21] The OCG's senior investigator points out that, based on her previous experience, an OCG investigation has the potential to result in sanctions or penalties such as employee discipline (including dismissal) or charges under the *Criminal Code* for fraud or breach of trust.[22] However, the Ministry's materials, including the terms of reference for the OCG's involvement (submitted *in camera*), do not point to any statutory authority for the OCG to impose these, or any other, penalties or sanctions. I have also considered the *in camera* information regarding sanctions or penalties, which is in the OCG's senior investigator affidavit at paragraph 17.[23] Because it was

[17] Order 36-1995, supra at p. 14-15.
[18] Order 50-1995, [1995] B.C.I.P.D. No. 23.
[19] Order F11-13, supra.
[20] [RSBC 1996] Chapter 138.
[21] Ministry's initial submissions, para. 4.22 and OCG's senior investigator affidavit, paras. 11-12.
[22] OCG's senior investigator affidavit, para. 16.
[23] Ministry's initial submissions.

accepted *in camera* (it reveals legal advice to the Ministry), I may not discuss this information in any detail except to say that, in my view, the proceedings described are not a sanction or penalty. In summary, although the *Financial Administration Act* provides the OCG with the authority to examine, evaluate and report, it does not provide authority to impose penalties or sanctions.

[21] I have also considered if the information in dispute forms part of an investigation by another public body that does have the statutory authority to impose sanctions or penalties, as was the case in Orders 50-1995 and F11-13. Although the OCG's senior investigator states that the police often request access to records that the OCG has compiled during the course of OCG investigations,[24] there is no evidence that the actual records at issue here form part of a police investigation. In addition, I have carefully considered exhibit B of the OCG's senior investigator's affidavit, which was accepted into the inquiry *in camera*, so I may not describe it publicly.[25] However, I can say that, in my view, exhibit B indicates that the RCMP does not actually know what the records responsive to the applicant's access request are. Therefore, I am not persuaded that the information in dispute in this inquiry actually forms part of any RCMP investigation. As stated in previous orders, until such time as the information becomes part of an investigation by a public body with the statutory authority to conduct an investigation and impose sanctions or penalties, the information is not part of a law enforcement matter under FIPPA.

[22] Therefore, I find that the OCG investigation is not a "law enforcement matter" under s. 15(1)(a). Consequently, I do not need to address the second element of the s. 15(1)(a) exception, which is whether disclosure of the information in dispute could reasonably be expected to harm the OCG investigation.

RCMP investigation

[23] The Ministry submissions and supporting evidence satisfy me that an RCMP investigation into matters related in some way to the OCG's investigation was commenced and had not concluded at the time of inquiry submissions.[26] In my view, it is clear that an RCMP investigation would meet the definition of "law enforcement" because it is "policing, including criminal intelligence operations."

[24] I will now consider whether disclosure of the information in dispute could reasonably be expected to harm the RCMP investigation. Despite finding that

---

[24] OCG's senior investigator affidavit, at para. 18.

[25] The applicant explains in his reply submissions at para. 17, that the Ministry disclosed this email to him during the inquiry. It is evident from his submissions, that this is indeed the case.

[26] There was no evidence provided about the nature of that investigation or the identity of the individuals whose activities the Ministry submits are under scrutiny by the RCMP.

the OCG investigation is not a law enforcement matter, for the sake of completeness and because the Ministry's submissions regarding harm to the OCG and the RCMP investigations are intermingled, I will also consider whether disclosure of the information in dispute could reasonably be expected to harm the OCG investigation.

Reasonable expectation of harm

[25] The Ministry submits that disclosure of the information withheld under s. 15(1)(a) could reasonably be expected to result in potential witnesses or other individuals gaining access to the information, and this may result in them:

- "altering their responses to questions asked in interviews conducted for the purpose of the investigation";
- "destroying evidence, including emails, database data and hard copy records";
- "being less inclined to cooperate with an ongoing investigation";
- learning that they are the target of the investigation, "which could enable them to take steps to adversely affect or thwart the course of the ongoing investigation".
- being alerted to the fact that "they might be interviewed, thus resulting in the potential for those individuals to thwart the ongoing investigation". [27]

[26] The Ministry submits that if the above occurs, it "would hamper the ability of the investigators to get at the truth."[28]

[27] The applicant disagrees that disclosure of the information will result in the harm the Ministry alleges. Given that the OCG has been looking into the issues since May 2012, he submits that it is unlikely that potential witnesses or targets of the investigation are not already aware that their activities are of interest. He adds that in September 2012 the Minister of Health publicly revealed information about the investigations and the termination or suspension of a number of individuals and the cutting-off of data access to others, so if individuals were inclined to undermine the investigation by destroying evidence or altering their testimony, they would have done so by now.

[28] With one exception, the Ministry does not identify the individuals it believes might hamper the investigations.[29] The records contain references to multiple individuals, so it is not evident who the Ministry thinks might engage in

[27] Ministry investigator's affidavit, para. 12. In its submissions, the Ministry refers to these harms as Categories A, B, C, D and E, respectively.
[28] Ministry investigator's affidavit, para. 12.
[29] The exception is in the OCG's senior investigator's affidavit, paras. 25-27.

such behaviour. The Ministry does not explain the significance of the withheld information to any particular individual and why knowing that information might motivate that person to lie or attempt to thwart an investigation. In effect, I am required to guess in order to fill in the blanks. Even in the one instance where the Ministry does identify an individual, it provides no information that explains why it would be reasonable to expect that person to destroy evidence or be purposely deceitful and uncooperative.

[29] Further, there is no evidence suggesting that the records were treated as confidential when they were created. It is reasonable to conclude that their contents are already known to the multiple individuals engaged in the work associated with those records (for example, the multiple researchers named in the agreements and the individuals participating in the group emails). Finally, the records were created some time before the Ministry's, OCG's or RCMP's investigations commenced so they do not contain references to those investigations.

[30] In my view, the Ministry's submissions are based on speculation, and there is no objective evidentiary basis for concluding that the harms the Ministry fears will result from disclosure to the applicant. In conclusion, the Ministry has not proven that disclosure of the information in dispute could reasonably be expected to harm a law enforcement matter, so it may not withhold information under s. 15(1)(a).

Security of property—s. 15(1)(l)

[31] The Ministry also relies on s. 15(1)(l) to withhold some information from the records. The Ministry submits that the information withheld under s. 15(1)(l) is "security system documentation" and it is imperative, for security purposes, to maintain the confidentiality of such information. It submits that disclosure could reasonably be expected to harm computer systems owned and operated by the Province of British Columbia. Specifically, the information "would assist a potential hacker in attacking those systems."[30]

[32] The Ministry also submits that by refusing to disclose this information it is complying with its obligations under s. 30 of FIPPA to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.[31]

---

[30] Ministry's initial submission, paras. 4.40, 4.37 and affidavit of Director of Information Security and Audit for the Ministry's Health Sector IM/IT Division para. 3, respectively.

[31] The Ministry references Investigation Reports: F06-01, [2006] B.C.I.P.C.D. No. 7; F06-02, [2006] B.C.I.P.C.D. No. 17; F10-02, 2010 BCIPC 13; F11-01, 2011 BCIPC No. 6; F11-03, 2011 BCIPC No. 43, which addressed the obligations of public bodies to protect personal information contained in computer systems.

[33] The Director of Information Security and Audit for the Ministry's Health Sector IM/IT Division provided affidavit evidence about how an individual could use the withheld information to gain unauthorized access to the Ministry's computer systems. Based on his explanations and my review of the records, I am satisfied that access to some of the information withheld under s. 15(1)(l) would assist an individual in obtaining unauthorized access to the Ministry's computer systems. The information consists of the names of databases and systems, user IDs, passwords, identifiers associated with the level/role/access authorization for obtaining specific data, system URLs that reveal details about a database, user account names, and the identifiers or names for various database tables that would enable one to query the databases for specific types of data. I find that disclosure of that information could reasonably be expected to weaken, and thereby harm, the security of the Ministry's computer systems. Therefore, that information may be withheld under s. 15(1)(l).[32]

[34] However, there are several instances where I find that the Ministry does not demonstrate any link between disclosure of the information withheld under s. 15(1)(l) and the anticipated harm to its computer systems. For example, the Ministry withheld a reference to two types of personal information that are contained in its computer systems.[33] The Ministry does not explain how revealing the fact that such information exists in its computer systems could reasonably be expected to harm those systems, especially given the fact that it is obvious any health-related system would contain that type of personal information. There are also instances where the Ministry applied s. 15(1)(l) to information that it has disclosed multiple times elsewhere in the records, for example acronyms for the Alzheimer's Drug Therapy Initiative ("ADTI"), the PharmacoEpidemiology Group ("PEG"), and the Pharmaceutical Services Division ("PSD").[34] It has also applied s. 15(1)(l) to withhold information from emails about the purely administrative aspects of organizing data access for various individuals.[35] In my view, there is no clear and direct connection between disclosure of that information and the harm the Ministry fears will result to its computer systems. Therefore, I find that the Ministry is not authorized by s. 15(1)(l) to refuse to disclosed it.

[35] In summary, the Ministry has not established that it is authorized to refuse to disclose information under s. 15(1)(a). However, it has established that it is authorized to refuse to disclose some information under s. 15(1)(l).[36]

---

[32] Pages 60-68, 74-76, 312-313, 327, 329-33, 336, 338, 340-45.
[33] Page 341.
[34] Pages 66-71 of the records.
[35] For example, pp. 60, 72, 330,
[36] I have highlighted the information that may be withheld under s. 15(1)(l) in a copy of the relevant pages of the records that will be sent to the Ministry with this order.

[36] I will now consider the Ministry's refusal to disclose personal information under s. 22. However, I will not consider personal information that I have already found may be withheld under s. 15(1)(l), namely employee numbers, usernames and passwords that would allow identification of the individual they belong to.

[37] **Disclosure harmful to personal privacy**—Section 22 of FIPPA requires public bodies to refuse to disclose personal information where its disclosure would be an unreasonable invasion of a third party's personal privacy. The Ministry relied on s. 22 to withhold some information, which I will describe below in more detail. Further, I identified a few instances of personal information in addition to that which the Ministry withheld under s. 22 (it was originally withheld under other exceptions which I found do not apply). I will consider all of that personal information in this s. 22 analysis.

[38] Numerous orders have considered the application of s. 22.[37] First, one must determine if the information in dispute is personal information. If so, one must assess whether any of the criteria identified in s. 22(4) apply. If s. 22(4) applies, disclosure is not an unreasonable invasion of third party personal privacy and s. 22 does not require that the public body refuse disclosure. However, if s. 22(4) does not apply, then one must determine whether disclosure is presumed to be an unreasonable invasion of third party privacy under s. 22(3). Finally, one must consider all relevant circumstances, including those listed in s. 22(2), in deciding whether disclosure of the information in dispute would be an unreasonable invasion of third party privacy. I have applied those principles here.

[39] The sections of s. 22 that play a role in this case are as follows:

> **22**(1) The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.
>
> (2) In determining under subsection (1) or (3) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether
>
> (a) the disclosure is desirable for the purpose of subjecting the activities of the government of British Columbia or a public body to public scrutiny,
>
> ...
>
> (h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant, and
>
> ...

[37] See for example, Order 01-53, 2001 CanLII 21607 (BC IPC) at p. 7.

(3) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if

...

(d) the personal information relates to employment, occupational or educational history,

...

(4) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if

...

(e) the information is about the third party's position, functions or remuneration as an officer, employee or member of a public body or as a member of a minister's staff,

(f) the disclosure reveals financial and other details of a contract to supply goods or services to a public body,

...

(i) the disclosure, in respect of

(i) a licence, a permit or any other similar discretionary benefit, or

(ii) a degree, a diploma or a certificate,

...

The following two definitions in Schedule 1 of FIPPA are also relevant:

"employee"**,** in relation to a public body, includes

...

(b) a service provider;

"service provider" means a person retained under a contract to perform services for a public body;

Personal information

[40] The first step in any s. 22 analysis is to determine if the information is personal information. Personal information is defined as **"**recorded information about an identifiable individual other than contact information". Contact information is defined as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual".[38]

[38] See Schedule 1 of FIPPA for these definitions.

[41] With only two exceptions, I find that the information withheld under s. 22 is personal information, and I will describe it in more detail below.[39] The exceptions are information which meets the definition of "contact information" so is not personal information. The first is a UBC project coordinator's work contact information on a data access request form.[40] The second is a contractor's mailing address and fax number in two *General Services Agreements* and in an *Amendment Agreement #1*.[41] The Ministry submits that the latter is the contractor's home contact information.[42] However, given the context in which it appears, it is clearly also his business contact information for the purposes of the contracts. Therefore, I find that it too is contact information, so it is not personal information. The Ministry may not withhold the contact information under s. 22.

Section 22(4) factors

[42] The next step in the s. 22 analysis is to determine if any of the circumstances listed in s. 22(4) apply because if they do, disclosure of the personal information is not an unreasonable invasion of personal privacy. The Ministry makes no submissions regarding s. 22(4). The applicant submits that s. 22(4)(f) and (i) apply.

[43] It is not apparent how s. 22(4)(i), which deals with licences, permits, discretionary benefits, degrees, diplomas or certificates, applies (and the applicant does not explain). Therefore, I find that s. 22(4)(i) does not apply. However, I find that s. 22(4)(e) and (f) both apply to some of the personal information in dispute.

[44] In my view, s. 22(4)(e) applies to much of the personal information the Ministry withheld because it is about the named individuals' positions and/or assigned functions as officers, employees or members of a public body (i.e., the Ministry, UBC and UVic).[43] For example, the Ministry withheld third parties' names, job titles and assigned roles from the various agreements between the Ministry, UVic, UBC and contractors. In several agreements and forms, the Ministry also withheld the name of the Ministry division, university, health institute or research agency where a third party works. The Ministry also withheld third parties' names from emails in which the third parties' functions regarding specific tasks and agreements are identified (i.e., the individual who will edit an

[39] The Ministry withheld a personal email address on p. 297. The applicant says in his reply submission he does not want access to personal email addresses. Therefore, the Ministry may refuse to disclose it under s. 22 (not s.15).
[40] Page 361.
[41] Pages 81, 109, 116, 140.
[42] I understand the Ministry's submission to be that this is the contractor's home information – despite the fact that the Ministry actually calls it the contractor's "home email addresses" (para. 4.50, initial submissions). There are no email addresses on these pages, so I assume that the Ministry meant to say "home address and fax".
[43] Pages 27, 28, 29, 31, 33, 34, 35, 36, 39, 248-50, 263, 354, 356-57, 361, 362, 380, 384, 385.

agreement, the individuals who will provide more information about an agreement, the individual who has signing authority, etc.). The Ministry also withheld the names of individuals who are identified in emails as requiring access to provincial health data because of their roles in the research and data sharing agreements.[44] I also note that there are multiple instances where the names of individuals are withheld in one instance but disclosed elsewhere in the records.[45] The reasons for doing so have not been explained, and from my review of the context where this occurs, I cannot see why the Ministry chose to treat the names differently throughout the records.

[45] The context in which personal information appears plays a significant role in determining whether s. 22(4)(e) applies. In Order 01-53,[46] former Commissioner Loukidelis found that a third party's name and other identifying information would, when appearing in the normal course of work activities, fall under s. 22(4)(e), but that s. 22(3)(d) would apply if the personal information appeared in the context of a workplace investigation or disciplinary matter. This is the same approach taken in many other orders, where it was held that s. 22(4)(e) covers personal information that is about the third party's job duties in the normal course of work-related activities, namely objective, factual statements about what the third party did or said in the normal course of discharging his or her job duties but not qualitative assessments or evaluations of such actions.[47]

[46] The Ministry's submission is that much of the personal information relates to the employment history of the third parties because it was amassed for the purpose of an internal investigation, so s. 22(3)(d) applies.[48] The applicant disagrees that s. 22(3)(d) applies because, he argues, the personal information was not created for the investigation and it already existed in files and was only "accumulated" during the investigation.[49]

[47] I find that s. 22(3)(d) presumption does not apply to the above mentioned personal information. When this information is viewed within the context of the records where it is located, it is evident that it is not about a workplace investigation or disciplinary matter. It is information about the role and function of named individuals, and it does not even hint at wrongdoing or an investigation. The records existed before any such investigation, and the personal information was clearly recorded in the normal course and as part of the Ministry's efforts to work out the protocol and practical details for data sharing and research. While at a later date some or all of the records may have been gathered together for

[44] Pages 65-67, 75.
[45] Pages 2, 18, 23, 37, 60, 62, 312, 361, to name just a few examples.
[46] Paragraph 40, Order 01-53, supra.
[47] Order 01-53, supra at para. 40. See also Order 00-53, 2000 CanLII 14418 (BC IPC), p.7; Order 01-15, supra, para. 35; Order 04-20, 2004 CanLII 45530 (BC IPC) at para. 18; Order F10-21, 2010 BCIPC 32 (CanLII).
[48] Ministry's initial submissions, para. 4.52.
[49] Applicant's reply submission, paras. 46-47.

investigation purposes, the records and the personal information they contain are not about an investigation into anyone's workplace actions or behaviour. The records do not contain witness or complainant evidence or statements about an individual's workplace behaviour or actions. Nor do they reveal an investigator's observations, findings or other work product.

[48] As I find that s. 22(4)(e) applies to the personal information described above, and its disclosure would not be an unreasonable invasion of personal privacy, the Ministry may not refuse to disclose it under s. 22.

[49] There is also a small amount of personal information that I find falls under s. 22(4)(f), which states that a disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if the disclosure reveals financial and other details of a contract to supply goods or services to a public body. The Ministry relied on s. 22 to withhold the contents of "Schedule A - Services" to a *General Services Agreement*.[50] I find that this information falls squarely within s. 22(4)(f) because it outlines the services the contractor will supply under the contract with the Ministry. Therefore, its disclosure would not be an unreasonable invasion of personal privacy and Ministry may not refuse to disclose it under s. 22.

[50] I do not need to consider the personal information to which ss. 22(4)(e) and (f) apply any further. However, there is also a small amount of personal information in emails which differs from that discussed above because none of the factors in s. 22(4) apply. It consists of the following:

1. Details about the personal lives of identifiable individuals (e.g., that someone is checking emails while on vacation, that someone else is boarding a flight, and that certain individuals will no longer handle tasks because they have changed jobs or will be on maternity leave).[51]
2. An opinion about a work unit and its processes (the identity of the opinion-giver has already been disclosed to the applicant).[52]
3. Details about how an individual performed at work and the comments and judgements of others about the same.[53]

For ease of reference, I will refer to this as the "remaining" personal information.

---

[50] Pages 93-94 of the records.
[51] In emails on pp. 247, 312, 325, 332.
[52] Page 313. I found that the Ministry could not refuse to disclose this opinion under s. 15. However, I recognize that an individual's opinions are his/her personal information.
[53] Pages 289-90 and 297-98.

Section 22(3) presumptions

[51] I will now proceed to the third step in the s. 22 analysis, which is to consider if any of the presumptions in s. 22(3) apply to the remaining personal information.

[52] I find that s. 22(3)(d) presumption, which states that disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if the personal information relates to employment, occupational or educational history, applies to #3 in the list of remaining personal information above. It is about how an individual performed at work and the judgements and comments of others about the same. This is personal information that relates to the individual's employment history and its disclosure is presumed to be an unreasonable invasion of the individual's personal privacy. There are no other presumptions that apply to the personal information in the records.

Relevant circumstances—Section 22(2)

[53] The final step in the s. 22 analysis is to consider the impact of disclosure of the remaining personal information in light of all relevant circumstances, including those in s. 22(2).

[54] The Ministry says that it considered s. 22(2)(a) (i.e., whether disclosure is desirable for the purpose of subjecting the activities of the Ministry to public scrutiny), but was unable to conclude that disclosure of the personal information would enhance public understanding to the extent that it would warrant invading the personal privacy of third parties.[54] The Ministry also explains that it considered s. 22(2)(h) and whether disclosure of the personal information may unfairly damage the reputation of third parties. The Ministry says that it withheld the names of individuals about whom serious concerns were raised during the course of investigation,[55] but it does not elaborate further regarding these individuals and how disclosure of their identities in the context of the records could harm their reputations. The Ministry also submits that it withheld the names of the researchers and medical investigators about whom no concerns were raised because they might be assumed to be guilty by virtue of being mentioned in records the Ministry reviewed during its investigation. This, the Ministry submits, could unfairly damage their reputations.[56]

[55] The applicant submits that the Ministry's contention that s. 22(2)(h) applies to the identity of third parties who were not targets of the investigations is "overbroad". He submits that a failure to disclose the personal information in dispute could undermine the reputation of anyone who is associated with the

[54] Ministry's initial submission, paras. 4.53-55.
[55] Ministry's initial submissions, para. 4.56.
[56] Ministry's initial submissions, para. 4.57.

Ministry and its research programs because there has been much speculation and very little information released since the Ministry publicly announced its investigation. The applicant also submits that due to this speculation, s. 22(2)(a) weighs in favour of disclosure because it would subject the Ministry to public scrutiny.[57]

[56] I note that the Ministry's s. 22(2) submissions are about the personal information whose disclosure I have already found is not an unreasonable invasion of third party personal privacy because it falls under s. 22(4)(e). However, for the sake of completeness, I have considered the Ministry's submissions about damage to reputations that it believes would result from disclosure of this s. 22(4)(e) personal information. As previously mentioned, most of the personal information falls under s. 22(4)(e) because it is simply about the nature of the third parties' professional roles and what they did in the usual course of discharging their duties. I disagree that negative inferences could reasonably be drawn about an individual's culpability merely because he or she is identified as a researcher in an information sharing agreement or in emails arranging for data access – even if those records were later considered during an investigation. With the sole exception of the information to which I found s. 22(3)(d) applied and which I will discuss next, there is nothing of a critical nature about the individuals named in the records. In short, I do not think that disclosure of any of the s. 22(4)(e) personal information would unfairly harm third party reputations.

[57] However, I do find that disclosure of the personal information about the manner in which a particular individual performed at work and the opinions of others about the same would unfairly harm third party reputations. This is the information to which the s. 22(3)(d) presumption applies.[58] In my view, disclosure of this information, some of which is critical, without the opportunity for the individuals involved to respond or clarify what is expressed, may unfairly damage the reputations of all those involved. I do not believe that the goal of subjecting the activities of the Ministry to public scrutiny outweighs the damage to reputations that might occur from such disclosure in this context. Therefore, the presumption that disclosure of these details would be an unreasonable invasion of personal privacy has not been rebutted, so this personal information must not be disclosed.

[58] Regarding the remaining personal information about the third parties' personal lives, I can see no harm to their reputations from disclosure.[59] The information is not sensitive and it does not appear to have been supplied in confidence. In each instance, the information was included in a work email sent to several work colleagues and forwarded along to others as part of chains of

[57] Applicant's reply submission, para. 48-49.
[58] This is #3 in the list of remaining personal information at para. 50, above.
[59] This is #1 in the list of remaining personal information at para. 50, above.

emails. It is the type of innocuous information that most people would not object to anyone else knowing, especially more than two years after the fact. Therefore, I find that its disclosure would not be an unreasonable invasion of third party personal privacy.

[59] I have also considered whether disclosure of the remaining personal information that consists of an opinion about a work unit and its processes would unfairly harm any third party's reputation.[60] The opinion was included in an email sent by a Ministry employee to four individuals, some of whom were external to the Ministry, and there is nothing to suggest that it was said in confidence. The opinion-giver passes judgement on a work unit and its processes but does not refer to, or criticize, any individuals. I find that disclosure of this opinion would not unfairly harm any third party reputations. I have also considered the fact that this opinion relates to the subject matter of the applicant's access request, namely information about the delays or impediments to accessing data for research purposes. It would shed light on the activities of the Ministry in that regard. Therefore, I find that its disclosure would not be an unreasonable invasion of third party personal privacy.

[60] In conclusion, I find that the only personal information whose disclosure would be an unreasonable invasion of third party personal privacy is the information about how an individual performed at work and the comments and judgements of others about the same. Under s. 22(1), that personal information, which is on pages 289-90 and 297-98, must not be disclosed. For clarity, I have highlighted this information in a copy of the records that will be sent to the Ministry along with this order.

CONCLUSION

[61] For the reasons given above, I make the following orders under s. 58 of the Act:

1. The Ministry is not authorized by s. 13 of FIPPA to refuse to disclose the contents of the email on pages 254-255.

2. Subject to paragraph #3 below, the Ministry is not authorized to withhold information under s. 15(1)(a) or s. 15(1)(l).

3. The Ministry is authorized to refused to disclose, under s. 15(1)(l) of FIPPA, the information that has been highlighted in pink on pages 60-68, 74-76, 312-313, 327, 329-33, 336, 338, 340-45 of the records, which accompany the Ministry's copy of this order.

[60] This is #2 in the list of remaining personal information at para. 50, above.

4. In accordance with s. 22(1) of FIPPA, the Ministry is required to refuse access to the information that has been highlighted in green on pages 289-90 and 297-98 of the records, which accompany the Ministry's copy of this order.

5. The Ministry must comply with the terms of this order by December 11, 2014 and concurrently send the OIPC Registrar of Inquiries a copy of the cover letter and records it sends to the applicant.

November 4, 2014

ORIGINAL SIGNED BY

Elizabeth Barker, Adjudicator

OIPC File No.: F12-50727