Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PC18-00074

Ministry of the Solicitor General

November 10, 2021

Summary: The complainant alleged that a staff member of the Ontario Provincial Police (the OPP) had inappropriately accessed and disclosed an OPP incident report that contained her personal information. The ministry responsible for the OPP admitted that the complainant's personal information had been accessed in violation of the *Freedom of Information and Protection of Privacy Act* (the *Act*).

In this report, I find that the complainant's incident report was accessed by an OPP sergeant without authorization on at least two occasions. In the absence of sufficient evidence, I do not find that the incident report was subsequently disclosed to the complainant's spouse, but I do conclude that the incident report number was disclosed by an unknown OPP employee contrary to the *Act*. I conclude that the ministry does not have reasonable measures in place to protect personal information in its database, as required by section 4(1) of Regulation 460. I recommend improvements to the privacy policies and procedures, privacy training, and auditing of accesses to personal information. I also recommend that the ministry disclose the disciplinary measures imposed on the sergeant as a result of the inappropriate accesses.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31, sections 2(1), 41(1), and 42(1); R.R.O. 1990, Regulation 460, section 4(1).

Orders and Investigation Reports Considered: Privacy Complaint Reports MC-060020-1, PC11-34, and PR16-40; *PHIPA* Order HO-010 and *PHIPA* Decision 110.

OVERVIEW:

[1] The Office of the Information and Privacy Commissioner of Ontario (the IPC) received a privacy complaint under the *Freedom of Information and Protection of Privacy Act* (the *Act*) from an individual (the complainant) concerning the Ontario Provincial Police (the OPP). The Ministry of the Solicitor General (the ministry) is the ministry responsible for the OPP.

[2] The complainant states that a sergeant (the sergeant) from the OPP provided the complainant's former spouse with her personal information. Specifically, the complainant states that her former spouse had noted the incident report number on some emails and court documents, leading her to believe that the sergeant had provided her former spouse with a copy of the incident report. The complainant knew the sergeant, who is a good friend of her former spouse.

[3] The complainant brought this complaint to the OPP. It was addressed by the OPP's Professional Standards Bureau (the PSB), which investigated the matter and issued an Investigation Report on October 16, 2018. This report confirmed that the sergeant had access to the Niche RMS database as part of her role at the OPP. However, when she used this database to view the complainant's incident report, she was not acting in the course of her duties. She did so twice in a six-month period, first on March 16, 2017 and again on August 9, 2017.

[4] According to the PSB Report, the sergeant admitted to looking at the report, stating that she "was curious", but denied providing the complainant's former spouse with a copy. The PSB Report confirmed that although the sergeant had accessed the incident report, she had not printed it at either viewing.

[5] In a November 8, 2018 letter to the complainant, the PSB Bureau Commander found sufficient evidence to reasonably believe that the sergeant viewed the incident report for personal reasons, but insufficient evidence to reasonably believe that she shared the incident report with the complainant's former spouse. The Bureau Commander determined that the matter was better addressed informally. He noted that this could include corrective actions, such as training or non-disciplinary corrective discussions with the sergeant, among other options.

[6] The complainant requested that the Office of the Independent Police Review Director (the OIPRD) review the PSB's decision. After doing so, the OIPRD determined that the PSB's investigation and conclusion were reasonable, and confirmed its findings. The OIPRD stated that no further action was required, and noted that discipline without a hearing had been imposed on the sergeant.

[7] During the IPC investigation, the ministry acknowledged that the sergeant should not have viewed the incident report, but stated that it had taken appropriate action to address the breach. When asked about audits of the sergeant's accesses to the

database, the ministry stated that it did not conduct additional audits as the PSB investigation did not find any additional inappropriate accesses of personal information.

[8] The ministry states that the OPP conducts training for new employees, that its Policy and Privacy Records Unit provides additional training upon invitation, and that the OPP has sent out reminders to staff regarding their privacy obligations. The ministry did not provide the IPC with information about the discipline imposed on the sergeant, despite repeated requests.

DISCUSSION:

Did the incident report contain "personal information" as defined in section 2(1) of the Act?

The Incident Report

[9] Personal information is defined in section 2(1) of the *Act*, which states:

> "personal information" means recorded information about an identifiable individual, including,
>
> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> (e) the personal opinions or views of the individual except where they relate to another individual,
>
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence

> (g) the views or opinions of another individual about the individual; and
>
> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

[10] This office has addressed incident reports, sometimes called occurrence reports, in the past, and acknowledged the sensitivity of the information that they contain. As stated in Privacy Complaint Report PC11-34:

> It is important to note that occurrence reports such as the one at issue here include highly sensitive and often detailed information about police incidents, as well as information about individuals such as the names of complainants, witnesses and victims, and other highly sensitive information about people, who may or may not have been charged with a crime.

[11] Past orders of this office have addressed the information contained in occurrence or incident reports. These have been described as containing personal information of parties whom the police speak to, including names, dates of birth, addresses, and statements that may include the interview subject's views and opinions about another person.[1]

[12] Although I have not reviewed it, the ministry does not dispute that the incident report identifies the complainant by name and contains her personal information. This is consistent with incident reports that this office has reviewed in the past.

[13] I hereby find that the incident report contains the complainant's personal information, as defined under subsections 2(1)(d) and 2(1)(g) of the *Act*.

Incident Report Number

[14] The complaint includes an allegation that the complainant's former spouse knew the incident report number, and that the OPP provided this to him. Before determining whether these allegations constitute an unauthorized disclosure under the *Act*, I first have to determine whether the incident report number itself is personal information.

[15] To do so, I must look at the context in which the incident number was communicated to the complainant's former spouse. The PSB Report provides details of this communication. It states that the spouse was aware of the incident report and

---

[1] See for example MO-3998 and PO-4024.

some of the details of the underlying incidents. He called the local OPP detachment to request the report and an unknown employee (who was not the sergeant) told him that he had the wrong incident number. The employee provided him with the correct incident number, as well as the name of the investigating officer. This corresponds with the narrative provided by the ministry in its submissions.

[16] In this context, the incident report number reveals, at a minimum, that there was a police investigation of some sort associated with the report number, and that it involved the complainant in some way. In my view, the way that it was communicated, when it was provided as confirmation of the complainant's involvement in a matter involving the police, made the incident report number information about the complainant.

[17] I find that the incident report number is recorded information about an identifiable individual and therefore, is the complainant's personal information, pursuant to section 2(1) of the *Act*.

Was the use of the "personal information" in accordance with section 41(1) of the *Act*?

[18] Section 41(1) of the *Act* states that an institution shall not use personal information in its custody or control unless the circumstances of the use fall within one of the exceptions set out in the *Act*.

[19] There is no evidence that the sergeant's viewings of the report were authorized under the *Act*, and the ministry has not made any claims that they were. In this case, the OPP's PSB investigated the accesses to the incident report, and found them to be inappropriate. The ministry acknowledges that the sergeant should not have viewed the report, that there was no reason for her to do so in the course of her duties, and that she did so for personal reasons. Accordingly, I find that these uses of the complainant's personal information were not in accordance with section 41(1) of the *Act*.

Was the disclosure of the "personal information" in accordance with section 42(1) of the *Act*?

[20] The complainant states that her former spouse had noted the number of an incident report and related details on documents having to do with their family law proceedings. The complainant states that her former spouse should not have known the details of that report.

[21] The ministry states that it determined through investigation that the sergeant did not disclose the incident report at issue. When asked for further details of how the ministry determined this, the ministry points to the PSB finding that the sergeant had not printed the report at either viewing.

[22] Without providing further details, I note that the PSB Report also included

statements from the complainant's former spouse, stating that he received information about the report from a source that was neither the OPP nor the sergeant.

[23] Considering all of the above, I do not have sufficient evidence before me to make a finding that the sergeant disclosed the incident report to the complainant's former spouse.

[24] This is not the case for the incident report number, as the ministry has confirmed that another OPP staff member communicated that number to the complainant's former spouse. The ministry states that, although there was disclosure, it did not consider this to be a breach of the *Act*, as "the only thing that was disclosed was an incident number, which the ex-husband was already in possession of, albeit incorrectly."

[25] The ministry's position appears to be that if an institution provides an individual with information already in their possession, that disclosure cannot be a breach of the *Act*. However, the ministry has not cited a section of the *Act* that corresponds with this position.

[26] The ministry was not able to provide any further details of the communication because it was unable to identify the staff member involved. The ministry conducted an audit of accesses to the incident report, and found that "many employees accessed the report, quite possibly as part of their regular employment (i.e. law enforcement) duties."

[27] Section 42(1) of the *Act* states that an institution shall not disclose personal information in its custody or under its control, except in the circumstances set out in subsections (a) through (o). Section 42 does not include any section stating that disclosure of personal information is permissible if the recipient was already aware of the information. As there is no subsection of s. 42(1) claimed, and none of which obviously apply, I cannot find that this disclosure was authorized under the disclosure provisions of the *Act*.

[28] I also disagree with the ministry's contention that no breach occurred, as the OPP staff member did not provide any new information, just a correction to existing information. The contents of the incident report do not need to be communicated for there to be a disclosure of personal information; confirmation of the existence of the report itself in the context in which it was given can constitute a disclosure.

[29] A comparison can be made to Privacy Complaint Report No. MC-060020-1. In that case, an individual had criminal charges brought against him, which were later withdrawn. The individual was asked for a police reference check for a volunteer opportunity. The Toronto Police Services Board indicated that in cases where it found no information on file, it informed the agency of that fact. However, if a match was found, it sent the agency a letter stating that the applicant had been sent "information on file." The police's position was that this was not a disclosure, because the individual

at issue, not the agency, was sent the information on file.

[30] This office did not accept that contention, stating as follows:

> In my view, revealing that a named individual has "information on file" with a police force is a very significant disclosure of sensitive personal information, even if no particulars are provided.

[31] Regardless of whether the complainant's former spouse had previously been told that there was an incident report involving the complainant, he did not have the ability to verify that this was actually the case. This verification was provided by the OPP when its staff member corrected the incident report number. I agree with the analysis in MC-060020-1, and do not see any reason why it would not also apply to police confirming that it has information regarding an individual – in this case, an incident report. I find that the disclosure of the incident report number, which communicated the complainant's involvement with the OPP in some capacity, is a disclosure of her personal information in contravention of section 42(1) of the *Act*.

Did the ministry have reasonable measures in place to prevent unauthorized access to the personal information of individuals, in accordance with section 4(1) of Regulation 460 of the *Act*?

[32] Even though the facts of this case are relatively straightforward (a sergeant with access to a database looked up records relating to an acquaintance for personal reasons unrelated to her job) and the ministry has agreed that this was in breach of the *Act*, its acknowledgment does not end the matter.

[33] The ministry is subject to section 4(1) of Ontario Regulation 460, made pursuant to the *Act*, which outlines the obligation of institutions to ensure they have reasonable measures in place to prevent unauthorized access to the records in the institution. Section 4(1) of Regulation 460 of the *Act* states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

[34] Investigator Lucy Costa, in Privacy Complaint Report PR16-40, addressed this requirement:

> From the way this section of the regulation is written, it is clear that it does not prescribe a "one-size-fits-all" approach to security. It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may

> not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.[2]

[35] The guidance set out in the IPC's "Privacy Breaches: Guidelines for Public Sector Organizations"[3] is useful in addressing the adequacy of the measures the ministry has in place to meet its Section 4(1) obligations. Specifically, the steps outlining how to investigate a breach and reduce the risk of future privacy breaches are instructive. These include reviewing the policies and practices in place protecting personal information, as well as the staff training, to determine whether changes are needed, and taking corrective action to prevent similar breaches from occurring in the future.

[36] In this case, I will address the policies and procedures in place, as well as the training provided to staff. I will also examine two additional areas that are key to remediation of the breach in this case: the auditing of accesses to personal information, and the communication of the discipline imposed on the offending employee.

Policies and Procedures

[37] I asked the ministry to provide me with any policies or other guidance documents that addressed unauthorized accesses to personal information. They provided sections of the OPP Orders addressing the Niche RMS database, and the Privacy Breach Protocol.

[38] The OPP Order relating to Niche RMS states that information from that database should not be disclosed without authorization, and that to do so could result in significant consequences. It does not contain a comparable statement prohibiting unauthorized access.

[39] The Privacy Breach Protocol Order sets out what the OPP considers to be breaches of an individual's privacy under the *Act*. This list includes unauthorized uses of personal information among those offences. It does not specifically address access as a distinct category of use.

[40] The OPP Orders provided by the ministry contain useful information, but do not adequately convey the extent of staff members' obligations to protect the privacy of individuals whose personal information is in OPP custody or control, and more particularly, in the Niche RMS database. This database contains sensitive personal information, making it key that the employees receive clear guidance on the limits on

---

[2] PR16-40 at paragraph 72.
[3] https://www.ipc.on.ca/wp-content/uploads/2019/09/privacy-breach-protocol-e.pdf.

the use of this information, including accesses to it.

[41] The ministry also provided a July 17, 2015 memo from the OPP Commissioner to all members regarding "Unauthorized Access to and/or Disclosure of Information." This memo notes the complaints that it had received regarding unauthorized access and disclosure since 2013 and states that oversight bodies "view the misuse of personal information held in the possession of the OPP as an increasingly serious misconduct issue." The OPP Commissioner in that memo states as follows:

> Utilizing OPP resources for any purpose that contravenes Ontario Public Service and OPP guidelines and policies could subject the member to disciplinary action under the Police Services Act, Public Service of Ontario Act, Freedom of Information and Protection of Privacy Act and/or as a result of a criminal investigation.
>
> All members are to be aware of the following:
>
> • The OPP is accountable to safeguard the overall integrity, confidentiality and security of information in its possession.
>
> • Personal information held in databases available to OPP members can only be accessed and used for specified and lawful purposes, and must not be used for personal interests.
>
> • Members must not access or use police databases when they have a personal interest in the matter, even if there is a police-related purpose, since doing so creates a conflict of interest.
>
> • Members are not to access, view, communicate, reproduce, display or show information obtained from a police database to others, unless allowed by law, policy, Memorandum of Agreement or other proper authority.

[42] This memo is clear and easy to understand. It demonstrates that the OPP views unauthorized access to and disclosure of personal information as serious matters. It communicates that privacy concerns are not limited to only disclosure, but include accesses made for personal reasons.

[43] Despite the excellent information in this memo, employees seeking guidance on these issues are more likely to turn to guidance documents, rather than dated memos or similar point in time communications. A memo can provide a valuable reminder of employees' privacy obligations, as this one does, but should not be the primary source of guidance.

[44] I recommend that the ministry enhance or revise its existing guidance documents, to more clearly communicate that staff are not permitted to use or access

personal information, including personal information in the Niche RMS database, for reasons unrelated to their work. These guidance documents should communicate that doing so is a breach of the *Act*, and set out the possible consequences to the employee for doing so.

Training in Privacy Obligations

[45] Policies and procedures can only achieve their goals if institutions provide employees with corresponding training. Given this, the obligations under section 4(1) of Regulation 460 also extend to providing adequate privacy training to protect personal information.

[46] Section 4(1) explicitly states that security obligations are to "[take] into account the nature of the records to be protected." In this case, the Niche RMS database contains sensitive personal information about those who have had interactions with the OPP, requiring even more robust training for those with access to that database.

[47] This is consistent with the analysis in Privacy Complaint Report PC11-34, which also addressed a breach of personal information from the Niche RMS database (in that case, a disclosure). The Report stated that:

> The requirement to put in place reasonable measures to protect information from unauthorized access pursuant to section 4(1) includes a requirement to ensure that staff are appropriately trained in the management of personal information. This means that staff and management who require access to personal information in order to perform their duties shall receive training to a level commensurate with the sensitivity of the information to which they have access.

[48] The ministry has stated that training is part of the orientation for all new employees. During this orientation, employees must complete two mandatory e-learning modules. One of these, called "Privacy and You" has been developed by the Ontario Public Service, while the other is OPP-specific, and references the Niche RMS confidentiality policy, as part of a module on OPP policies. The ministry tracks completion of the e-learning modules and any other courses required of employees, and supervisors may view this tracking information, as they are responsible for ensuring that employees meet all mandatory training requirements. During my investigation, I requested these documents, but the ministry did not provide them.

[49] The ministry also stated that under regulations to the *Police Services Act* all police officers are required to sign an Oath of Secrecy.

[50] I also asked the ministry about whether the OPP provides annual privacy training. The ministry questioned the necessity of the question, stating "there is no evidence to suggest that annual privacy training would have prevented the breach from occurring, or that it has anything substantive to do with the breach."

[51] I disagree with the ministry's position on this matter. The sergeant twice accessed the incident report for personal reasons, which the ministry agrees was inappropriate and a breach of the *Act*. She may have done so because she was unaware that this use of personal information was a breach. Alternatively, she may have known this was a breach of the *Act* but not been aware that it could have serious consequences. The ministry did not state whether the sergeant was asked if she knew that she had violated her privacy obligations under the *Act* by accessing this information.

[52] Training is a key tool to avert these types of accesses, by communicating to employees that accesses for non-work reasons are a breach of the *Act* that could result in serious consequences to the employee. While I take the ministry's point that unauthorized accesses may never be wholly prevented, and that annual training may not be possible in all cases, periodic training is one of the methods that can reduce unauthorized accesses.

[53] This is consistent with a recommendation in Privacy Complaint Report PC11-34, which was directed at this ministry for a breach involving the same database. PC11-34 recommended that the ministry put in place a training program where clerical staff handling sensitive personal information take part in privacy training at hiring, and that privacy training be repeated at regular intervals. It also recommended that this include training specific to the Niche RMS database. When I asked about the implementation of this recommendation, the ministry did not provide a response beyond questioning the necessity of my inquiry.

[54] While the ministry did not provide a copy of the "Privacy and You", I note that PC11-34 described what appears to be its precursor as "a reasonably good training tool." I further note that the ministry's response indicated that the current training materials address the Niche RMS, in that the OPP-specific online course includes the Niche RMS Confidentiality Policy.

[55] The ministry did not provide the document called "Niche RMS Confidentiality Policy", but it did provide a Niche RMS Order. This Order, as noted above, only addresses disclosures contrary to the *Act*, not accesses. Training specific to the Niche RMS would need to address unauthorized accesses in order to meet the ministry's obligations under section 4(1) of Regulation 460.

[56] Having not been provided with the training materials used, and not been assured of periodic training being provided, I am not satisfied that the ministry has satisfied its privacy obligations under section 4(1) of Regulation 460, especially as they relate to unauthorized accesses. I recommend that the ministry review its current training program to ensure that it provide adequate and specific privacy protection against unauthorized accesses to sensitive personal information in its databases, including Niche RMS, and that this training be repeated at regular intervals.

Auditing of Accesses

[57] As part of my inquiries, I asked the ministry what audits they had conducted on the sergeant's accesses to the Niche RMS. The ministry responded as follows:

> Please be advised that no additional audits of the employee's RMS accesses were conducted beyond what was relevant to this investigation. The complaint about the employee's access to information was specific to this incident and was investigated thoroughly by the Professional Standard's Bureau of the OPP. At no time was any evidence discovered of inappropriate accesses of information. If there was, it would have been thoroughly investigated. The OPP does not conduct "fishing expeditions" on the actions of its members without articulable cause.

[58] This complaint involved two accesses to the incident report; accordingly, my investigation of the uses of personal information at issue was limited to those instances. However, as with ensuring that adequate guidance and training are in place, the ministry's security obligations under section 4(1) extend beyond the particulars of this specific complaint. Its obligations include taking steps to ensure that the sergeant has not made similar unauthorized accesses, which did not come to the attention of the affected party as these ones did.

[59] Audits could uncover whether the sergeant made other unauthorized accesses to personal information. The ministry's objection to performing these audits is that there was no evidence discovered of inappropriate accesses of information. I do not agree with the ministry's reasoning. If the ministry limits its investigations only to the specific instances in this complaint, I fail to see how they could find evidence of any other inappropriate accesses, unless the sergeant herself confessed to them. Limiting investigations to the word of an employee who has already accessed personal information contrary to the *Act* does not satisfy the ministry's obligation to ensure the security of its records.

[60] The ministry's submissions to this office characterized audits as "fishing expeditions", when in fact they have become a common best practice. For example, one case of accesses to personal health information contrary to the *Personal Health Information Protection Act* (PHIPA Decision 110) involved a situation in which a random audit caught that a physician had made five accesses that may have been inappropriate. Further investigation, including further audits, found that this physician had likely inappropriately accessed the records of approximately fifty individuals.

[61] The same reasoning applies in the public sector, especially given the sensitivity of the information available in the Niche RMS database. Audits are a useful tool for determining if an employee has made additional inappropriate accesses, and therefore requires further investigation. Conversely, they can also confirm that an employee's breaches are indeed limited to the incidents initially raised to the attention of the

institution through the complaint at hand.

[62] The ministry has also stated that an audit would not be worthwhile in this case, given the time that has passed since the incidents in the complaint, and because the ministry contends that it would only reveal that the sergeant routinely accesses records as part of her employment duties. I acknowledge that conducting audits can be more complicated in cases such as the sergeant's, whose job requires that she access sensitive information regularly. However, it is especially important that institutions have the capability to monitor those with the most ready and far-reaching access to personal information through targeted auditing. If an institution says that it cannot monitor the database access of those employees, it is effectively telling those employees that unless there is a specific complaint, any unauthorized accesses will not be caught. While it is important for institutions to respond to the complaints of individuals, these should not be the only means by which unauthorized accesses are discovered.

[63] I want to be clear that I am not advocating for overbroad monitoring of all employees' accesses to personal information. However, in cases where there are substantiated allegations an employee has made unauthorized accesses to personal information, an institution should have both the willingness and capability to check to make sure there are not other similar instances. This is a reasonable measure to take in order to meet its obligations under section 4(1) of Regulation 460.

[64] While the ministry did not audit the sergeant's accesses to other records, it did conduct an audit of all accesses to the incident report. It did so in an effort to determine which unknown staff member spoke with the complainant's ex-spouse. The ministry was not able to determine the identity of this OPP employee, and provided the following reasons for why it was unsuccessful:

> The audit was limited in its usefulness by two important considerations: The first consideration is that no date was provided as to when the OPP detachment was contacted by the caller. If a date had been provided, the scope of the audit would have been narrowed, and this might have revealed which unknown employee spoke with the caller. The other consideration is that many employees unintentionally accessed the incident report. They could have done so, for example, while searching for information about other similar type offences. Moreover, these employees would not have kept notes of their search if they had been doing so for this or other legitimate reasons, and they therefore also likely would have had no independent recollection of accessing the report.

[65] The ministry did not state whether it attempted to narrow down the date of the call, either as part of the PSB investigation or otherwise. It also did not set out any other efforts it made to narrow the search results. For example, the PSB report indicates that the complainant's ex-spouse contacted a particular OPP location but the ministry did not state whether the search was limited to staff at that location. The

ministry also did not state whether they identified within the search results staff who may not normally query similar offences as part of their job duties. Examining the results with these types of parameters in mind may have aided the ministry in determining which accesses warranted further follow up.

[66] I acknowledge that there is no guarantee that the staff member would have been located if further efforts were made. I can only address the efforts themselves, which, based on the information before me, appear to have been a simple search of the accesses to the incident report, without further examination. Given this, I am not satisfied that the ministry made sufficient efforts to determine which staff member accessed the incident report and subsequently made the disclosure to the complainant's ex-spouse. The failure to do so means that the ministry lost a possible opportunity to take corrective measures vis a vis this staff member, which may have included reminding them of their privacy obligations, or providing them with further training.

[67] I recognize the time that has passed and accordingly, I will not recommend that the ministry conduct audits of the sergeant's accesses from the time period surrounding the incidents or look further into the accesses to the incident report. However, the ministry should put in place audit capability for any future similar instances, as a security measure to help deter unauthorized accesses, and to help ensure that any such unauthorized accesses are detected, so far as reasonably possible. As such, I recommend that the ministry develop the capability and implement a protocol for conducting audits of employees' accesses to personal information in cases where an employee has been shown to have made unauthorized accesses, or in cases where the ministry has reason to suspect the employee may have made unauthorized accesses to personal information.

Communication of Disciplinary Information

[68] The complainant has confirmed that she would like to know what discipline the sergeant faced due to her accessing personal information contrary to the *Act*. Neither the ministry nor the other bodies involved have provided this information to her. The PSB stated that the matter was being dealt with informally, while the OIPRD stated that discipline was imposed but provided no details.

[69] The ministry states that it will not provide information about the discipline the sergeant faced. Their position is that they are not obliged to do so, contending that disciplinary information is information related to an employee, and is therefore excluded from the scope of the *Act* pursuant to section 65(6). The ministry also cites a duty to protect employees' personal information and implications resulting from the collective agreement as further reasons not to disclose the sergeant's disciplinary information. The ministry disputes that this information is relevant to the privacy complaint, or would assist in preventing subsequent breaches.

[70] This is not a new position from the ministry. In the circumstances documented in

PC11-34, this ministry also refused to provide information regarding any disciplinary measures imposed; in that case, the breach was an OPP clerk disclosing an incident report.

[71] In PC11-34, this office drew from a previous order issued under the *Personal Health Information Protection Act*. Order HO-010 dealt with an inappropriate disclosure by a staff member, and provided guidance on how to address situations where there has been unauthorized access or disclosure of personal information. In that case, Commissioner Cavoukian stated:

> The complainant has a right to receive assurances that the incident has been appropriately addressed and that steps have been taken to prevent its re-occurrence. Critical to this assurance are details of the steps taken by the hospital, including the results of its investigation and the fact that disciplinary action was taken against the employee in question.

[72] Commissioner Cavoukian elaborated on this requirement in the post-script to Order HO-010:

> This level of transparency is important for several reasons. Accessing a patient's personal health information in an unauthorized manner is a serious violation of an individual's privacy and security of the person. In such a situation, the aggrieved individual has a right to a complete accounting of what has occurred. In many cases, the aggrieved parties will not find closure regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required.
>
> For other staff members of the hospital involved, knowing that all of the details of the disciplinary action imposed will be publicly disclosed, should serve as a strong deterrent. This is especially true if those details also become known to other employees, either through the actions of the aggrieved individual, the custodian, or both. Employees must understand that, given the seriousness of these types of breaches, their own privacy concerns will take a back seat to the legitimate needs of the victims involved to have a full accounting of the actions taken by the health information custodian. Our primary concern must lie with the aggrieved party, whose privacy was completely disregarded.

[73] The IPC found that this rationale also applied to the circumstances in PC11-34, in which an OPP clerk had disclosed an individual's personal information by providing an occurrence report to the individual's landlord, an acquaintance of the clerk. PC11-34 stressed the importance of providing assurances to the affected party that their personal information is secure, especially in cases where it had previously been

breached:

> This complainant is a resident of the community served by the OPP detachment where the privacy breach occurred. She is entitled to assurances that her personal information will not be the subject of any further inappropriate disclosures by staff at this detachment. She should also be entitled to assurances that if she requires the assistance of staff in this detachment at any time, including in relation to matters that may affect her own personal health and safety, she can provide her personal information to OPP staff knowing that it will be secure from inappropriate disclosures by clerical staff or members of the police force.[4]

[74] This office found that a policy of disclosing the details of a response to a privacy breach was a reasonable measure to take (barring exceptional circumstances), as it may deter staff from disclosing information when they do not have the authority to do so.

[75] I adopt and apply the reasoning in HO-010 and PC11-34. I see no reason why this rationale that applies in the case of disclosures of personal information should not equally apply to unauthorized accesses to that information. In both cases, the affected individual's right to privacy has been breached.

[76] The complainant in this case had her personal information twice accessed by someone she knew in her personal life, for what the ministry describes as personal reasons. The complainant was given only vague information about the type of discipline the sergeant faced for these violations. Providing fuller information about how the ministry addressed these breaches has a twofold purpose. It helps assure the complainant that her personal information will not be treated the same way in future. It also deters other employees from committing similar violations in future.

[77] The ministry disagrees that the IPC has authority to ask for information relating to matters of discipline, stating that such matters are excluded from the scope of the *Act.* They base this on section 65(6)(3) of the *Act*, which states that the *Act* does not apply to employment-related ministry records.

[78] The ministry raised this objection in PC11-34 as well, stating that there was an inconsistency between the IPC's interpretation of section 4(1) of Regulation 560, and this exclusion. In PC11-34, this office did not find any such irresolvable tension between the two, stating as follows:

---

[4] Privacy Complaint Report PC11-34 at page 10.

> I disagree with the ministry's view that there is any inconsistency in the recommendation to disclose the disciplinary action. I recognize that as a general rule, the *Act* does not apply to labour or employment related records and therefore, the access and privacy provisions of the *Act* do not apply to records of this nature. The exclusion in the *Act* for records of this nature does not however, limit the ministry's ability to provide victims of a privacy breach with information about the actions taken to respond to the breach, including the nature of the disciplinary action taken.

[79] Just as in PC11-34, I find that the obligation to provide information regarding the ministry's security measures extends to providing information about the disciplinary measures taken. Section 65(6)(3) does not limit this office's responsibility to ensure that an institution is taking reasonable measures to ensure that records are not being accessed contrary to the *Act*.

[80] I find that the ministry should have disclosed the disciplinary measures imposed on the sergeant as a result of the unauthorized accesses to the complainant's personal information and recommend that they do so now.

CONCLUSIONS:

1. The incident report contains "personal information" as defined by section 2(1) of the *Act*.

2. The incident report number is "personal information" as defined by section 2(1) of the *Act*.

3. The ministry's accesses to the personal information were not in accordance with section 41(1) of the *Act*.

4. The ministry's disclosure of the incident report number was not in accordance with section 42(1) of the *Act*.

5. The ministry does not have reasonable measures in place to prevent unauthorized accesses to personal information in accordance with section 4(1) of Regulation 460 under the *Act*.

RECOMMENDATIONS:

I recommend that the ministry:

1. Enhance guidance documents, or revise the existing documents, to more clearly communicate that staff are not permitted to access personal information,

including personal information in the Niche RMS database, for reasons unrelated to their work.

2. Review its current training program to ensure that it provide adequate and specific privacy protection against unauthorized accesses to sensitive personal information in its databases, including Niche RMS, and that this training be repeated at regular intervals.

3. Implement a protocol for conducting audits of employees' accesses to personal information in cases where an employee has been shown to have made unauthorized accesses, or in cases where the ministry has reason to suspect the employee may have made unauthorized accesses to personal information.

4. Advise the complainant what, if any, disciplinary actions were taken against the sergeant who was responsible for the breach of the complainant's privacy.

Within six months of receiving this Report, the ministry should provide this office with proof of compliance with the above recommendations.

Original Signed by: November 10, 2021

Jennifer Olijnyk
Investigator