ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2022-54

November 7, 2022

CITY OF CALGARY

Case File Number 005896

Office URL: www.oipc.ab.ca

Summary: The Complainant made a complaint to this Office regarding the City of Calgary (the Public Body). The Complainant, who is an emergency medical technician (EMT) with Alberta Health Services, was concerned that employees of the Public Body's 911 Centre had accessed her schedule information for their own purposes, without authority. In order to obtain records to substantiate this concern, the Complainant made an access request to the Public Body for emails and messages sent by particular employees about her. The Public Body asked each of these employees to search through their emails and messages for the Complainant's personal information. The Complainant raised concerns that her identity as a FOIP applicant was inappropriately disclosed.

The Commissioner authorized a review of the complaint. Following that review, the Complainant requested an inquiry. In her request for inquiry, the Complainant raised a concern about the security measures taken by the Public Body to ensure that unauthorized access of scheduling information did not continue.

The Adjudicator found that the Public Body made reasonable security arrangements to protect the Complainant's personal information as required by section 38 of the FOIP Act.

The Adjudicator found that the Public Body had authority to use and/or disclose the Complainant's personal information as it did.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 1, 38, 39, 40, 41, 72

Authorities Cited: AB: Orders F2008-029, F2009-041, F2013-06, F2014-19, F2014-23, F2015-10, P2012-02

I. BACKGROUND

[para 1] The Complainant made a complaint to this Office regarding the City of Calgary (the Public Body). The Complainant, who is an emergency medical technician (EMT) with Alberta Health Services (AHS), was concerned that employees of the Public Body's 911 Centre had accessed her schedule information for their own purposes, without authority. In order to obtain records to substantiate this concern, the Complainant made an access request to the Public Body for emails and messages sent by particular employees about her. The Public Body asked each of these employees to search through their emails and messages for the Complainant's personal information.

[para 2] The Complainant made the following complaint to the Commissioner:

> I am contacting your office to inform you that I reasonably believe that my personal information has been looked up without lawful reason on City of Calgary, and Alberta Health Services databases, as well as my information was disseminated unlawfully by both City of Calgary employees, and employees of Alberta Health Services.
>
> I am currently employed as an Emergency Medical Technician with Alberta Health Services Emergency Medical Services. I recently became aware that certain staff at the City of Calgary 911 Centre (who are contracted by Alberta Health Services to provide dispatching services for EMS) were asking other City of Calgary staff, as well as Alberta Health Services staff to look up information on my scheduling which was a part of some staff activity engaging in bullying and harassment against myself. I was made aware that staff in both entities had been discussing various acts of violence against myself, and that scheduling rosters were being routinely access to identify when and where I was working.
>
> As a part of information gathering for the purpose of bringing my concerns forward to my superiors and Human Resources department I filed a FOIP request with the City of Calgary, and was issued file #2017-p-0161 in response to my request. In my FOIP request with the City of Calgary I specified that I would like information relating to City of Calgary emails, as well as computer aided dispatch (CAD) messages which make up a part of the EMS dispatch system. On May 24th , 2017 I was contacted by [M] with the City of Calgary FOIP office who indicated that searching all of the Calgary 911 staff email accounts would take a significant amount of time, and that this time could be reduced if I was to provide her with a list of specific individuals at the 911 Center [from whom they could gather my information]. As I did not wish for my FOIP request to be seen as targeting, harassing, or bullying any of the staff at the 911 Center I made sure to ensure with [M] that me providing a specific list of staff would not be construed as harassment or bullying, and that my information would remain private. [M] advised me that this FOIP request would not be construed that way, and that my request would be completely confidential. I compiled a list of staff at the 911 Center and provided it to [M] via email for the purposes of having my FOIP request completed.

> During the process of the City of Calgary conducting the FOIP Investigation I was provided with information that the Deputy Commander of Operations at the Calgary 911 Center ([G]) was assisting the FOIP Investigation. She would call individual staff members into an office and would ask them if they knew me, ask if they were aware of why I had filed a FOIP request, and were then asked to their computer and search my name in their email and print off and provide to her any emails that had my name in them. Some of the staff members at the 911 Center were provided information that 15 staff members were specifically named in the FOIP request, and were provided some of the names on the list. I was further advised that [G] made known that 15 people were on the list of the FOIP request and that the result of the email searches had turned up no information so a blank document would be issued as a result of my FOIP request.

[para 3] The Commissioner authorized a senior information and privacy manager (the Manager) to investigate and attempt to settle the complaint. Following this process, the Complainant requested an inquiry. In her request for inquiry, the Complainant raised a concern about the security measures taken by the Public Body to ensure that unauthorized access of scheduling information did not continue.

[para 4] The Complainant and Public Body both made comprehensive submissions on the matters set out for inquiry.

II. ISSUES

[para 5] The issues as set out in the Notice of Inquiry dated February 5, 2020, issued by the adjudicator previously assigned to this file, are as follows:

1. Did the Public Body make reasonable security arrangements to protect the Complainant's personal information in relation to her work schedule against such risks as unauthorized access, collection, use, or disclosure, as required by section 38 of the FOIP Act?

This issue relates to the Complainant's allegation that employees of the Public Body were looking up the Complainant's work schedule in contravention of the FOIP Act.

2. Did the Public Body use the Complainant's personal information? If yes, did it do so in compliance with or in contravention of sections 39(1) and 39(4) of the Act?

This issue relates to the Complainant's complaint regarding the processing of her access request by the Public Body.

If the Public Body is relying on section 39(1)(a), the parties should also make submissions as to whether the requirements of section 41 are met.

3. Did the Public Body disclose the Complainant's personal information? If yes, did it have authority to do so under sections 40(1) and 40(4) of the Act?

This issue also relates to the Complainant's complaint regarding the processing of her access request by the Public Body.

III. DISCUSSION OF ISSUES

1. Did the Public Body make reasonable security arrangements to protect the Complainant's personal information in relation to her work schedule against such risks as unauthorized access, collection, use, or disclosure, as required by section 38 of the FOIP Act?

[para 6] The Notice of Inquiry sets out the scope of this issue as follows:

This issue relates to the Complainant's allegation that employees of the Public Body were looking up the Complainant's work schedule in contravention of the FOIP Act.

[para 7] Section 38 of the Act states:

> *38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.*

[para 8] In Order F2009-041, the adjudicator provided a useful overview of the burden of proof with respect to an alleged unauthorized disclosure of personal information under Part 2 of the FOIP Act (at paras. 25-29). She concluded that the complainant bears an initial evidential burden of establishing a basis for the complaint. I believe this conclusion applies equally with respect to a complaint of a failure to meet the duty under section 38. The authors of *The Law of Evidence* 2nd Edition describe the evidential burden as follows:

> The term "evidential burden" means that a party has the responsibility to insure that there is sufficient evidence of the existence or non-existence of a fact or of an issue on the record to pass the threshold test for that particular fact or issue.

[para 9] A public body's obligation under section 38 is explained in Order F2014-19 as follows (at paras. 26-27):

> Section 38 addresses whether a public body has made reasonable security arrangements to safeguard personal information; it does not directly address situations in which a breach is alleged but the safeguards were reasonable. In other words, it is possible for a public body to have made reasonable security arrangements and yet personal information can be accessed, used, disclosed or destroyed in an unauthorized manner. For example, a "rogue" employee who is appropriately authorized to access information may access the information for unauthorized purposes. This is essentially the situation alleged by the Complainant. In such a case, it is not clear that section 38 is contravened.
>
> That said, the fact of a breach may undermine what would otherwise appear to be reasonable security arrangements; therefore I will consider the Complainant's allegations regarding unauthorized alteration of her performance contract.

[para 10] The Complainant and Public Body have each provided a comprehensive explanation of how the EMS system works. Below is my understanding of the relevant details.

[para 11] Various terminology has been used by the parties in discussing EMS personnel. As the Complainant is an Emergency Medical Technician (EMT), I will be using that term. EMTs are employed by Alberta Health Services (AHS), whereas dispatchers and other Emergency Communications Officers (ECOs) are employed by the Public Body.

[para 12] The Public Body and EMTs use a Computerized Aided Dispatch (CAD) system. EMS personnel, who are employed by AHS, have unique identifier numbers – which the parties refer to as a registration number – that they use to sign in via a computer in their assigned ambulance.

[para 13] Work schedule information of EMTs is contained in the CAD system. When EMTs log onto the CAD system in an ambulance, their registration number is visible in CAD as being assigned to that ambulance. CAD system users can also access the name associated with the registration number.

[para 14] ECOs take calls from the public and dispatch EMS units (dispatchers). ECOs use the CAD system for dispatching units. Dispatchers cannot access the entire work schedule of EMTs; they can access only whether the EMT is currently logged onto a unit and available to be assigned to respond. Dispatchers can also search the history of a unit and view which EMTs were assigned to that unit on previous days. This is the only way for ECOs to search for an EMT's work history. Future work schedules of EMTs are not viewable by ECOs.

[para 15] The Public Body states that dispatchers require real-time access to EMTs' current availability as part of their job duties.

[para 16] The Complainant argues that ECOs do not have a bona fide reason to access EMT's work schedules. She further states (initial submission, at page 9):

> In the alternative, if there is a determination that this information is required by ECO's to execute their duties, the Public Body has not taken reasonable security arrangements to ensure that this information is accessed only for lawful purposes. The most basic arrangements of electronically logging of which ECO has accessed this information, and their purpose for accessing this information, has not been implemented.

[para 17] With its initial submission, the Public Body provided an affidavit sworn by an Access and Privacy Analyst, who participated in the Public Body's investigation of the Complainant's complaint. The affiant states that following the earlier review by this Office, the Public Body accepted most of the recommendations made by the Manager conducting the review, but it did not accept the recommendation to audit a particular

module of the EMS CAD system (the "CAD Resource Log") as this system does not have the functionality to audit that module (affidavit, at para. 9).

[para 18] The affiant states that during the previous review by this office, they spoke with the Calgary 911 Deputy Commander of Technical and Business Services (M), who has knowledge of the EMS CAD system. M informed the affiant that the Public Body has an agreement with AHS to provide integrated emergency dispatch services. The affiant also states that M informed them that the CAD system is owned by AHS, not the Public Body. The system allows for different permissions to be assigned to different users depending on their job functions.

[para 19] Regarding audit functions, affiant states that M informed them that the unit work history information is contained in the CAD system "resource log" and that the system does not have the functionality to audit "view only" access to this resource log. In contrast, the "real time" availability information of EMTs is accessible via the CAD system "event log". The CAD system has the functionality to audit "view only" accesses. The Public Body states that this function was enabled in response to the review by this office.

[para 20] The Complainant did not disagree with the above facts in her detailed rebuttal submission.

[para 21] The Public Body argues that the Complainant's work schedule is not sensitive information that requires additional safeguards. It notes that personal information of public body employees that relates only to the employees' job duties is not personal information to which section 17(1) applies when responding to an access request, citing Orders F2015-10 and F2014-23. The Complainant argues that this analysis doesn't apply in this case as the disclosures at issue were not in records responding to an access request.

[para 22] The Public Body states that the administrative safeguards in place to protect personal information in the CAD system consist of two policies that apply to Public Body 911 employees. The Public Body provided me with copies of these policies. Some of the information regarding the Public Body's security policies relate to security of the 911 system more broadly. I will discuss only the policies that relate to the CAD system and the Complainant's concerns about that system.

[para 23] One policy is entitled "Policy - Admin – Security of Calgary 9-1-1". This policy relates to the security of the Calgary 911 system more generally, but includes information specific to the CAD system. For example, it sets out that an ECO requires a Level III security clearance, which appears to be the highest clearance level. This level requires a CPIC check, a Calgary Police Service Security Clearance Declaration, that fingerprints be submitted, and that a polygraph be administered. The policy addresses the handling and storage of data, including CAD-generated documentation, destruction of hardcopy data, visitor permissions and expectations of confidentiality.

[para 24] This policy is 12 pages long. The only information in this policy directly relevant to the Complainant's concerns is the following:

> **Personal Handheld Devices**
> Includes but not limited to PDAs, cellular telephones, other personal electronic devices capable of conveying, disclosing, storing, transmitting, texting or sending messages, data or information.
>
> Since these private devices cannot be universally secured (encrypted) and supported to the satisfaction of the C911 or its partners, the practice of utilizing personal devices to transmit C911 or C911 partner information, data or messages is prohibited.
> …
>
> **Confidentiality**
> C911 employees have access to confidential databases (e.g. Sentry, CAD, CPIC) to support partner emergency communication services and objectives. Security and confidentiality relating to the access and disclosure of information seen, heard or spoken via these strictly confidential databases or through the critical operations of the C911 is a shared responsibility between C911 personnel and their partners.
>
> Although appropriate and responsible information sharing is encouraged, the responsibility for safeguarding information lies with the person accessing, possessing, storing and controlling the information.
>
> Actual or perceived breaches of CPIC confidentiality or security expectations will be investigated by the Calgary Police Service. An employee involved in an allegation may be removed from the C911 Operations Centre immediately pending the outcome of the investigation. The disposition of the investigation may result in discipline up to and including termination of employment.

[para 25] The other policy is entitled "Policy – Admin – CAD Access Levels". This policy is very short. It states that access levels for the CAD system will be determined based on job functions, in order to protect the system and data from unauthorized users. It delineates who can provide or authorize access, what happens when the employment of an authorized user is terminated, and sets out an audit schedule to validate current users.

[para 26] The Public Body states that it also has physical safeguards in place, such as requiring escorts for any visitors, and requiring all documents generated by the CAD system to remain in secured areas.

[para 27] The technical safeguards described by the Public Body include limiting access to the CAD to what is necessary for each employee's job duties, as well as the auditing functions described above.

[para 28] The Complainant cites Order F2013-06, in support of her argument that the Public Body's safeguards are not sufficient. That Order relates to an unauthorized disclosure of personal information from the Motor Vehicle registries database (MOVES database) by a registry employee. The MOVES database was maintained by Service

Alberta and the information contained in that database is information in the custody or control of Service Alberta. In Order F2013-06, the adjudicator considered whether Service Alberta made reasonable security arrangements to protect personal information in the MOVES database from unauthorized disclosures, as required under section 38 of the Act.

[para 29] The adjudicator cited Order P2012-02, which addressed a similar provision under the *Personal Information Protection Act* (PIPA), which noted that the sensitivity of the personal information at issue will affect what security arrangements are reasonable. The adjudicator in Order F2013-06 said (at para. 30):

> Like section 34 of PIPA, section 38 imposes a duty on a public body to make reasonable security arrangements to protect personal information. In my view, a public body will have met the duty under section 38 if it demonstrates that deliberate, prudent, and functional measures have been adopted to guard against, or mitigate, a foreseeable risk. The extent to which security measures are necessary will depend on the sensitivity of the information, as discussed above.

[para 30] In that case, Service Alberta acknowledged that the information contained in the MOVES database was highly sensitive and confidential. The adjudicator noted that the registry employee disclosed the personal information in that case to an individual who sought the address of the complainant to confront them at their home. The adjudicator also noted that the information in the MOVES database is sufficient to create false identifications and expose registry clients to identity theft.

[para 31] The adjudicator summarized the existing safeguards as follows (at para. 38):

> From the foregoing, I conclude that Service Alberta has developed policies and procedures that prohibit gaining access to and disclosing personal information from the MOVES database without legal authority. It conducts audits (which I will discuss below) to ensure that its policies are understood and its procedures are being followed. It also requires registry agents to conduct criminal record checks for their employees. It publishes disciplinary measures such as termination and suspension of registry employees as a deterrent and to ensure that disciplined employees are not hired at another registry. There are mechanisms to track employees' use of the MOVES database (I will discuss these mechanisms below). Investigators are on staff to investigate complaints of unauthorized disclosure or violations of policy.

[para 32] The adjudicator concluded that these safeguards were reasonable but insufficient. She states (at para. 47):

> If a public body does not create a mechanism to ensure compliance with its policies or procedures, such as regularly monitoring and auditing how employees access personal information, then it is essentially relying on an "honour system" to protect personal information. Establishing that an employee understands policies and procedures does not necessarily mean that the employee will follow them.

[para 33] She further states (at paras. 49-51):

> It appears that Service Alberta does not proactively investigate the possibility of unauthorized access to the MOVES database, in that it does not regularly monitor employees' access. Service Alberta's audit process, as it has been described to me, does not address or investigate employees' actual usage of the MOVES database, but rather, poses questions regarding knowledge of policies and procedures. Moreover, audits take place every three years and are scheduled, which may not be sufficiently frequent or random to act as a deterrent. The audit process essentially tests knowledge; however, employees may choose not to follow policies and procedures despite having adequate knowledge of them. Consequently, it may be that the prospect of an investigation by Service Alberta is sufficiently remote so as not to amount to a deterrent to an employee who may choose not to follow Service Alberta's policies regarding unauthorized access.
>
> I also find that the fact that the employment of the employee who disclosed the Complainant's personal information without authority was terminated will not necessarily operate as an effective deterrent against unauthorized disclosure by other employees. If a rogue employee is satisfied that unauthorized access and disclosure will go undetected, that employee may access and disclose personal information despite the threat of termination.
>
> Given the sensitivity of the personal information in the MOVES database, and given that it is a requirement for Albertans to submit their personal information to this database in order to obtain identification or a driver's license, it may be necessary for Service Alberta to adopt more extensive proactive measures to protect the personal information of the Complainant, and that of other Albertans, from unauthorized disclosure by registry employees, such as regularly monitoring use of the MOVES database, even in the absence of a complaint.

[para 34] The adjudicator concludes (at paras. 54-55):

> The submissions of Service Alberta indicate that it is committed to ensuring the safety of personal information contained in the MOVES database, and I accept that this is so. However, I cannot ignore that there appear to be insufficient measures in place to monitor and ensure Sentinel Registry employees' compliance with legislative requirements when they access personal data, with the result that the personal information of the Complainant, and other Albertans, is subject to the risk of unauthorized access and disclosure. As the Complainant's personal information has already been improperly disclosed to an individual to whom he did not want this information to be disclosed, ordering Service Alberta to take steps to ensure that this does not happen again to his information may appear to be the equivalent of ordering it to close the stable doors. However, there is some benefit to ordering Service Alberta to take proactive measures to monitor the manner in which Sentinel Registry employees gain access to personal information from the MOVES database, as doing so will contribute to increased security against unauthorized access not only in relation to the Complainant's personal information, but also that of other Albertans whose information is stored in the database.
>
> I note that many of the findings I have made regarding the measures Service Alberta takes to protect information from unauthorized disclosure may apply equally to registries other than Sentinel Registry. However, the scope of this inquiry is limited to

> consideration of the circumstances giving rise to the disclosure of the Complainant's personal information by an employee of Sentinel Registry and the submissions of the parties reflect this. Therefore, the issue of whether Service Alberta takes adequate measures to protect personal information in the MOVES database from unauthorized access and disclosure by registry employees, other than Sentinel Registry employees, must be left for another day.

[para 35] The Complainant argues that the same finding should be made here (rebuttal submission):

> 18. Similar to [para 44] in F2013-06, the Public Body would not have been aware of this disclosure if the Complainant had not brought this matter to the Public Body. ln this same Order para. 45-50 appear analogous to this matter. The Public Body appears to be taking the position that their policies are sufficient to prevent the unauthorized access or disclosure of personal information despite this Order quite clearly stating that this "honour system" is insufficient, as is the threat of disciplinary action in the unlikely event they are caught.
>
> 19. The Public Body has not provided information to indicate that they have, or will, proactively investigate unauthorized access to private information. In fact, the Public Body goes a step further and states they will not do so with some information as "The EMS CAD system does not have the technical capacity to audit "view only" access to the "Resource Log" where Work Schedule Information is retained."
>
> 20. The submission from the Public Body, and the Affidavit of [EG] confirm that the City of Calgary operates the CAD system under a contract with Alberta Health Services. Publicly available information shows the City of Calgary employs some 13327 employees. Alberta Health Services directly employs some 102700 people. Despite these vast resources, the Public Body makes an assertion that they lack the technical capacity and as such are unable to audit this information. This position by the Public Body is grossly irrational, inflammatory, and lacks an air of reality

[para 36] In her complaint to this office, the Complainant states that "scheduling rosters were being routinely accessed to identify when and where I was working." In her rebuttal submission, the Complainant argues (at paras. 23-24):

> 23. The Complainant has provided information to the Public Body that demonstrates the level of animus displayed towards the Complainant by an employee of the Public Body that includes reputation destruction, mentions of physical violence, and reference to the possibility of workplace "accidents" where the Complainant could suffer physical harm. In accordance with Order P2012-02 this information would likely function as a contributing factor towards a determination of sensitivity. I take the position that a reasonable person provided with this information would more likely than not come to the conclusion that the sensitivity of the information disclosed is higher due to the potential of the Complainant suffering harm.
>
> 24. The Public Body asserts that there is no requirement for excessive measures to protect this information. Putting aside the differences in the Parties positions to whether the information is sensitive, I take the position that the Public Body has not met the lower

> threshold requirement within the Act to provide reasonable safeguards for personal information as I detail in para. 14-20 of this rebuttal.

[para 37] The Complainant concludes:

> 34. Further the Public Body has failed to implement reasonable safeguards against unauthorized access of personal information, and has provided no evidence that it proactively investigates, conducts audits, or routinely monitors how their employees access personal information. The Public Body can provide extensive information on its policies and procedures; however these policies and procedures provide no actual safeguards as the Public Body does not employ a mechanism to ensure compliance with its policies or procedures.

[para 38] The Public Body argues that the personal information at issue in Order F2013-06 is substantially different from the information at issue in this case, such that the outcome of Order F2013-06 ought not to be applied here. It states (rebuttal submission at para. 4):

> As stated in the Public Body's Initial Submission, the extent of security measures that will be considered to be "reasonable" depends on the sensitivity of the information at risk (see Initial Submission, para 20). In other words, the Act does not require Public Bodies to implement the same security measures for all systems containing personal information. The Public Body submits that given the broader scope and sensitivity of the personal information contained in the MOVES database as compared to the EMS CAD System, the Act does not require the Public Body to implement the same security measures in the EMS CAD System as would be required for MOVES. The Public Body further submits that it has implemented reasonable safeguards to protect the Complainant's personal information as described in its Initial Submission.

[para 39] In her rebuttal submission cited above, the Complainant has said that she provided information to the Public Body showing that information in the CAD system was used to harass her. I do not know what information the Complainant provided to the Public Body that mentions or threatens workplace violence or "accidents" involving the Complainant. Such information has not been provided to me.

[para 40] The Complainant has provided printouts of what she states are text message conversations from a Public Body ECO's phone. There are four conversations from this ECO, who I will refer to as AB; the Applicant states that two conversations are with other ECOs, one is with an AHS supervisor and one is between AB and their significant other.

[para 41] The Public Body argues that the copies of the text messages "do not indicate the names of the individuals involved nor has the Complainant provided sworn evidence to support her allegation of which individuals were involved with sending the text messages" (initial submission at para. 51).

[para 42] In her rebuttal submission the Complainant acknowledges that sworn evidence is usually given more weight than unsworn evidence; however, she states that she does not have access to legal advisors and "I believe a reasonable person would more

likely than not expect the evidence provided to the Commissioner by the Complainant may not be to quite the same standard as the submissions of the Public Body…".

[para 43] It is true that sworn evidence is often given more weight than unsworn evidence. I understand the Complainant's point about having access to legal or other resources and this is one reason that administrative decision-making bodies are not bound by formal rules of evidence. However, it is also true that the Complainant has not provided any information about the text messages, except to state who was involved. The Complainant has left visible the phone numbers involved, but there are no names associated with the phone numbers. The Complainant has blacked out "export details" relating to each conversation, which might have corroborated the Complainant's statements as to the source of the texts (i.e. that these texts are from AB's phone).

[para 44] Presumably, since all conversations involve AB, the texts are most likely from AB's phone. It is not clear how the Complainant came to be in possession of printouts of the text conversations. The Complainant's name appears only once in the text messages so it is not evident from the texts that they are even about the Complainant. Assuming that the conversations do relate to the Complainant as she asserts, they are rather unfavourable. All of the participants in the text conversations appear to have disliked the Complainant. This raises obvious questions about how the Complainant came to have copies of these messages when the apparent source of the messages (AB) does not seem to have the sort of relationship with the Complainant such that the individual would have provided the printouts to her. These questions raise doubts about the reliability of the texts as evidence.

[para 45] Even if the Complainant was unable to provide sworn evidence regarding the source and content of the text messages, she could have provided additional unsworn information in response to the concerns raised by the Public Body that may have mitigated my concerns about their reliability.

[para 46] For the reasons discussed below, I do not need to rely on the text messages or their content to make a finding regarding the Public Body's obligation under section 38. To the extent that the text messages are offered as support that the Public Body used or disclosed the Complainant's personal information without authority, I will discuss the weight to be given to the text messages in the relevant sections of this Order.

Analysis

[para 47] While the information relates to the Complainant's work duties, her work history and whether she is currently at work is information about her (i.e. her personal information). That said, I agree with the Public Body that the Complainant's work schedule information contained in the CAD system is not particularly sensitive information in this case. This is due, in part, to the fact that the work schedule information that is accessible to Public Body employees is of past shifts that were worked by EMTs, and who is currently signed in. Future work schedules are not at issue.

[para 48] I cannot see how information about the Complainant's past work shifts would be used to harass the Complainant or otherwise be used to her detriment. Nothing in the submissions before me indicates that past work shifts have been searched by Public Body employees.

[para 49] In my view, the Public Body's safeguards, described above, are sufficient to protect the minimal personal information available in the CAD system regarding past assignment to particular EMS units.

[para 50] Current information about whether an EMT is working at a given time could presumably be used to locate that individual. This is true of most employees who work pre-determined hours at a permanent location but many organizations, including the Government of Alberta, publish the business contact information (including work addresses) for many employees. In my view, this is not sensitive information that obliges significant safeguards such as those discussed with respect to the MOVES database in Order F2013-06. It is also not information that obliges the Public Body to proactively investigate or routinely monitor how its employees access personal information, as argued by the Complainant.

[para 51] I find that the safeguards currently in place, including the newly enabled auditing system, are sufficient to fulfill the Public Body's obligations under section 38.

2. Did the Public Body use the Complainant's personal information? If yes, did it do so in compliance with or in contravention of section 39(1) and 39(4) of the Act?

[para 52] The Notice of Inquiry sets out the scope of this issue as follows:

> *This issue relates to the Complainant's complaint regarding the processing of her access request by the Public Body.*
>
> *If the Public Body is relying on section 39(1)(a), the parties should also make submissions as to whether the requirements of section 41 are met.*

[para 53] Personal information is defined in section 1(n) of the Act as follows:

> *1(n) "personal information" means recorded information about an identifiable individual, including*
>
> > *(i) the individual's name, home or business address or home or business telephone number,*
> >
> > *(ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,*
> >
> > *(iii) the individual's age, sex, marital status or family status,*

(iv) an identifying number, symbol or other particular assigned to the individual,

(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,

(vi) information about the individual's health and health care history, including information about a physical or mental disability,

(vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,

(viii) anyone else's opinions about the individual, and

(ix) the individual's personal views or opinions, except if they are about someone else;

[para 54] A public body's use of personal information is governed by section 39 of the Act. The relevant portions of section 39 of the Act state:

39(1) A public body may use personal information only

(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or

(c) for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43.

...

(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.

[para 55] Section 41 defines what constitutes a "consistent purpose" under section 39(1):

41 For the purposes of sections 39(1)(a) and 40(1)(c), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure

(a) has a reasonable and direct connection to that purpose, and

(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

[para 56] In this case, the Complainant's name was provided to several Public Body employees for the purpose of searching for responsive records.

[para 57] In the affidavit provided with the Public Body's initial submission, the Access and Privacy Analyst set out the Public Body's process for responding to access requests generally. They state that an access and privacy analyst determines which business unit(s) with the Public Body is likely to have responsive records, and a records request form is sent to those units. Each business unit has a FOIP Program Administrator who either conducts or directs the search for responsive records within that unit. The applicant is not identified on the records request form sent to the business units. If the applicant has requested their own personal information, the applicant is identified to the business units as a "subject" of the access request (rather than as the applicant). The "subject" name is provided to the business units verbally.

[para 58] The affiant states that an Access & Privacy Administrator was assigned respond to the Complainant's access request. The affiant states that the Administrator informed the affiant that the Administrator followed the process described above: the Administrator verbally clarified the Complainant's request; the Administrator advised the Complainant that her identity as the applicant would not be disclosed but that she would be identified as the subject of the search for responsive records; and the Administrator verbally identified the Complainant as the subject of the search for records to the FOIP Program Administrator for the Calgary 911 unit.

[para 59] The Public Body argues that it was authorized to use the Complainant's personal information under section 39(1)(a). The Public Body states that it collected the Complainant's name in her access request, in order to process the request. It states that it used the Complainant's personal information for the same purpose.

[para 60] I agree that the Public Body was authorized under section 39(1)(a) to use the Complainant's name to process the access request where the Complainant's name was the subject of the search. From my understanding of the Complainant's argument, she is not objecting to the use of her name to process the request in general. Rather, the Complainant is concerned that the 15 employees identified in her access request should not have been involved in searching for records, and that Deputy Commander G identified the Complainant as the applicant (rather than just the subject of the request) to the 15 employees. These concerns relate to the extent of the Public Body's use of the Complainant's name, under section 39(4).

[para 61] Section 39(4), cited above, limits a public body's use of personal information to the extent necessary to enable the public body to carry out its purpose.

[para 62] Order F2008-029 states that "necessary" in section 42(b) does not mean "indispensable". The Director of Adjudication states in that Order (at para. 51):

> In the context of section 41(b), I find that "necessary" does not mean "indispensable" – in other words it does not mean that the CPS could not possibly perform its duties without

> disclosing the information. Rather, it is sufficient to meet the test that the disclosure permits the CPS a means by which they may achieve their objectives of preserving the peace and enforcing the law that would be unavailable without it. If the CPS was unable to convey this information, the caseworkers would be less effective in taking measures that would help to bring about the desired goals. Because such disclosures enable the caseworkers to achieve the same goals as the CPS has under its statutory mandate, the disclosure of the information by the CPS also meets the first part of the test under section 41(b).

[para 63] I will first discuss whether the Public Body used the Complainant's personal information beyond what was necessary when it asked the 15 employees identified in the request to conduct a search for records.

[para 64] The Complainant states that after she submitted her access request to the Public Body, a Public Body employee asked her if her request could be narrowed to specific 911 Centre employees, rather than conducting a search of all 911 staff email accounts. The Complainant states that she was concerned that narrowing the request could be construed as harassing or bullying the specified employees. She states that she was assured her request would be confidential. She further states that she was told that the 15 employees ultimately named in the request would not be made aware of the request or searches being conducted.

[para 65] The Analyst who swore the affidavit states that they reviewed an email from the business unit Administrator responsible for conducting the search for records in the Calgary 911 area, which indicates that the Administrator informed the 911 Commander and two Deputy Commanders of the access request. The team lead for the of the 911 Operational Effectiveness Team was advised of the request, in order for them to conduct a search of the CAD system for records. The Analyst further states that Deputy Commander G told them that they (G) spoke with each of the 15 employees named in the Complainant's request and instructed them to conduct a search of their email account for responsive records.

[para 66] The Analyst further states (affidavit, at para. 32):

> As part of the search for Responsive Records, I requested that [K], the FOIP Program Administrator for Corporate Security, conduct a search on the Outlook system of employees named in the Request. I provided her with the subject's name over the phone. This search did not locate any Responsive Records.

[para 67] The Complainant cites the above paragraph as support for her argument that it was unnecessary for the 15 employees named in her request to conduct their own searches for responsive records. The Complainant states that this shows that the search for records could have been done by one person alone.

[para 68] By letter dated October 5, 2022, I asked the Public Body the following questions about K's role in searching for responsive emails:

> Can the Public Body please provide further information regarding the Outlook searches conducted in the course of responding to the Complainant's access request? Specifically, the Complainant's concern seems to assume that [K's] search replicated the searches conducted by the individual employees; is this the case? If so, why was it necessary to also ask each employee to conduct a search of their Outlook accounts? Please address how this affects the analysis of whether the Public Body used the Complainant's personal information only to the extent necessary under section 39(4).

[para 69] The Public Body explained that K's additional search for responsive emails did not replicate the searches conducted by the 15 named employees. The 15 employees conducted a search of their email accounts. K conducted an additional search that could not be undertaken by the 15 employees. The Public Body states that this additional search was undertaken when no responsive emails were located and the Complainant communicated an expectation that several records ought to exist.

[para 70] The Public Body provided an affidavit sworn by K. In that affidavit, K explains that at the time of the Complainant's request, any emails in the Public Body's email system that had not been interacted with for 30 days were archived. The search tools routinely available to employees would locate responsive records that had been archived only if the keywords were located in the 'to', 'from', 'cc', 'bcc' or 'subject' lines. The only way for most employees to search the body of archived emails would be to open and review each one. As part of the role that K had with the Public Body at the relevant time, K had access to additional tools that allowed them to undertake a more comprehensive search of archived emails, including conducting a keyword search that would encompass the body of archived emails. K explained the process as follows:

> To conduct the search of the archived emails I collected 22 Gigabytes of archived PST files of the employees named in the access request. These were indexed overnight on June 5, 2017. I completed my search the next day.

[para 71] The Public Body argues that when a request includes emails of named employees, it is reasonable to have those employees conduct a search of their email accounts, including any emails that may have been printed and filed in hardcopy format.

[para 72] I agree with the Public Body. There are practical reasons for having an employee identified in an access request search their own files, whether it be an email account, a network drive assigned to them, or their own hardcopy records. Even if someone in K's position could search the email accounts of all 15 employees, K would not be aware of any emails that may have been printed and maintained in hardcopy format, if the electronic email no longer existed at the time of the search. K would also not have known whether any of the 15 employees was likely to have saved any emails in another location (e.g. a network drive) before deleting them from their email account. Having the named employees conduct their own search ensures that the search is sufficiently comprehensive to fulfill the Public Body's obligations under section 10 of the Act (duty to assist applicants).

[para 73] I find that the Public Body did not use the Complainant's personal information beyond what was necessary when the 15 employees identified in the Complainant's access request were instructed to conduct a search for responsive records, and that accordingly it complied with section 39(4) of the Act.

[para 74] To the extent that the Complainant was led to believe that the employees identified in her request would not be involved in the search for responsive records, this does not negate the Public Body's authority to use her personal information to process her request as it did here. That said, the Public Body should take care to be clear with applicants on this point should a similar situation arise in the future.

[para 75] The other concern raised by the Complainant is that Deputy Commander G revealed to the 15 employees named in the Complainant's request that the Complainant made the access request, and discussed the outcome of the search for records with them (specifically that no responsive records were located). The printouts of text messages were provided as support for this allegation.

[para 76] The text messages provided with the Complainant's initial submission appear to indicate that Deputy Commander G revealed to someone that the Complainant made the access request. However, as I have discussed above, the Complainant's name appears in only one text and I cannot be certain that she is the individual discussed in the other texts. Further, I have discussed the fact that I do not know from where (or whom) the Complainant obtained copies of these texts. Without knowing how the Complainant obtained these texts, and because I cannot verify that the participants are those identified by the Complainant or that the Complainant is the subject of the various texts, is it difficult to accept them as evidence that supports the Complainant's arguments. In other words, the texts are not reliable evidence that the Public Body employees identified by the Complainant used or disclosed her personal information as she asserts.

[para 77] Further, to the extent that the text are meant to support the claim that Deputy Commander G told other employees that the Complainant made the access request, none of the texts purport to be from Deputy Commander G, so they are not first-hand evidence that Deputy Commander G disclosed this information to someone. One text states what was purportedly said to the author of the text by Deputy Commander G. In another text, the author is informing the recipient of what Deputy Commander G apparently said to a different individual, and not the author directly.

[para 78] Some of the Public Body's affidavit evidence is similarly flawed. For example, the Access and Privacy Analyst explained what was told to them by Deputy Commander G about whether G discussed the Complainant's access request with Public Body employees (affidavit, at para. 30):

> I am advised by Deputy Commander [G] and do verily believe that she did not discuss the responsive records or results of the Request with anyone, but may have inadvertently wondered as to who the "subject" was to an individual named in the Request because the subject's name was not familiar to her.

[para 79] The affiant is merely relaying what was said by Deputy Commander G. A sworn statement from Deputy Commander G would be more reliable and carry more weight.

[para 80] The Access and Privacy Analyst also states that the Complainant's access request was processed by another Administrator, and explains what this Administrator told them about how the request was processed. This is evidence of what the Administrator said to the Analyst, but not evidence of what the Administrator actually did.

[para 81] That said, I accept the Analyst's affidavit evidence of the Public Body's usual process for processing access requests, including that the applicant's name is not shared with other areas conducting the search. If the Public Body followed its usual approach, Deputy Commander G could not have disclosed the Complainant's identity as the applicant, for the reason that Deputy Commander G would have known only that the Complainant was the subject of the request.

[para 82] Even if I were to give weight to the text messages provided by the Complainant, it is quite possible that Deputy Commander G and the 15 Public Body employees who were asked to search their email accounts for records assumed that the Complainant was not only the subject of the request but also the applicant, without being told as much. Such an assumption may be understandable given that the Complainant was identified as the subject of the request, and the hostile relationships the Complainant described as having with at least some of her coworkers. It seems to me that the only way to avoid such an assumption is by not involving the employees named in the request in the search for records. However, as explained above, informing the 15 named employees was necessary to assure that an adequate search for records was undertaken.

[para 83] On the basis of the above, I find that on a balance of probabilities, the Public Body did not reveal to the 15 employees named in the Complainant's request that the Complainant was the applicant who made the request. Therefore, the Public Body did not use the Complainant's personal information in that manner.

3. Did the Public Body disclose the Complainant's personal information? If yes, did it have authority to do so under sections 40(1) and 40(4) of the Act?

[para 84] The Notice of Inquiry sets out the scope of this issue as follows:

> *This issue also relates to the Complainant's complaint regarding the processing of her access request by the Public Body.*

[para 85] A public body's disclosure of personal information is governed by section 40 of the Act. The relevant portions of section 40 of the Act state:

> *40(1) A public body may disclose personal information only*
>
> ...

> *(c) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,*
>
> *...*
>
> *(4) A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in subsections (1), (2) and (3) in a reasonable manner.*

[para 86] The Public Body argues that it did not disclose the Applicant's personal information, stating that "[r]elaying the Complainant's Request within a business unit is not a "disclosure" of information, as the information [did not leave] the Public Body" (initial submission at para. 50).

[para 87] I agree that the sharing of information in processing the Complainant's access request is better characterized as a use of information rather than a disclosure. If that is not correct, the Public Body would have been authorized to disclose the personal information under section 40(1)(c), which mirrors section 39(1)(a). The Public Body would have also met its obligation under section 40(4) to disclose the personal information only to the extent necessary, for the same reasons I have found that section 39(4) was met.

IV. ORDER

[para 88] I make this Order under section 72 of the Act.

[para 89] I find that the Public Body made reasonable security arrangements to protect the Complainant's personal information as required by section 38 of the FOIP Act.

[para 90] I find that the Public Body had authority to use and/or disclose the Complainant's personal information as it did.

_____

Amanda Swanek
Adjudicator