Office of the
Saskatchewan Information
and Privacy Commissioner

REVIEW REPORT 039-2021

eHealth Saskatchewan

March 2, 2022

Summary: eHealth Saskatchewan (eHealth) received an access to information request from the Applicant. eHealth responded to the Applicant denying access to the record pursuant to sections 15(1)(c), (e), (m), 17(1)(a), 21 and 22(a) of *The Freedom of Information and Protection of Privacy Act* (FOIP). The Applicant requested a review from the Commissioner of eHealth's application of these exemptions. The Commissioner found that eHealth did not appropriately apply sections 21 and 22(a) of FOIP to the record. However, the Commissioner found that eHealth appropriately applied sections 17(1)(a) and 15(1)(m) of FOIP to parts of the record and recommended that eHealth continue to withhold those parts and release the remaining parts of the record to the Applicant. The Commissioner also recommended that eHealth review its polices and procedures to ensure that it is consistent with its obligations pursuant to section 8 of FOIP.

I BACKGROUND

[1] On January 14, 2021, eHealth Saskatchewan (eHealth) received an access to information request from the Applicant, requesting the following information:

> A 840-page Data Forensics Analysis Report (DFA report) prepared by SaskTel on eHealth's system and security. I understand that someone else has already sent in a request for this document and would like to receive it whenever it has been redacted and prepared for release. Time period January 1, 2020 and December 31, 2020.

[2] On February 2, 2021, eHealth responded to the Applicant denying access to the requested record in full pursuant to sections 15(1)(c), (e), (m), 17(1)(a), 21 and 22(a) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

[3] On February 26, 2021, my office received a request for review from the Applicant. The Applicant requested that my office review the exemptions cited by eHealth for denying access to the requested record.

[4] On March 3, 2021, my office provided notification to the Applicant and eHealth of my office's intent to undertake a review. Both parties were invited to provide submissions to my office. My office also requested a copy of the record from eHealth.

[5] On April 5, 2021, eHealth provided its submission to my office. The Applicant did not provide any submission.

II RECORDS AT ISSUE

[6] The record at issue is an 870 page report titled, *Data Forensics Analysis Report* (DFA Report), completed by Saskatchewan Telecommunications (SaskTel) for eHealth to assist with its investigation into a ransomware attack that eHealth had proactively reported to my office on January 10, 2020. Further information regarding this ransomware attack can be found in my Investigation Report 009-2020, 053-2020, 224-2020.

[7] eHealth denied access to the entire record requested by the Applicant, pursuant to sections 15(1)(c), (e), (m), 17(1)(a), 21 and 22(a) of FOIP.

III DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[8] eHealth qualifies as a "government institution" pursuant to section 2(1)(d)(ii) of FOIP and section 3 and Part I of the Appendix of *The Freedom of Information and Protection of Privacy Regulations* (FOIP Regulations). Therefore, I have jurisdiction to conduct this review.

2. Did eHealth properly apply section 17(1)(a) of FOIP?

[9] eHealth applied section 17(1)(a) of FOIP to pages 20 to 48, 49 to 51 and 52 to 290 of the DFA Report. It withheld the information on these pages in full.

[10] Section 17(1)(a) of FOIP provides:

> **17**(1) Subject to subsection (2), a head may refuse to give access to a record that could reasonably be expected to disclose:
>
> (a) advice, proposals, recommendations, analyses or policy options developed by or for a government institution or a member of the Executive Council;
> …

[11] My office's *Guide to FOIP*, Chapter 4: "Exemptions from the Right of Access", updated on April 30, 2021, pp. 123-131 (*Guide to FOIP*, Ch. 4), explains that section 17(1)(a) of FOIP is a discretionary class-based exemption. It permits refusal of access in situations where release of a record could reasonably be expected to disclose advice, proposals, recommendations, analyses or policy options developed by or for a government institution or a member of the Executive Council.

[12] The following two-part test can be applied:

1. Does the information qualify as advice, proposals, recommendations, analyses or policy options?

2. Was the advice, proposals, recommendations, analyses and/ or policy options developed by or for a government institution or a member of the Executive Council?

(*Guide to FOIP*, Ch. 4, pp. 123-131)

1. Does the information qualify as advice, proposals, recommendations, analyses or policy options?

[13] In its submission to my office, eHealth asserted the withheld information constituted advice, recommendations and analysis and stated:

Significant portions of the DFA Report constitute advice, recommendations and analysis. For example:

a. Pages 20 through 48 of the DFA Report contain advice as the information therein relates to the expert opinions of SaskTel as to matters of fact (e.g., the extent of the Ransomware Attack, the existence of malware, extraction of personal information, etc.) of which eHealth must make a decision for future action such as how to respond to the Ransomware Attack or how to prevent future attacks;

b. Pages 49 through 51 contain recommendations regarding cyber-security maturity, governance, security organization and incident response;

c. Pages 52 through 290 contain analysis of data, including live response analysis, volatile data analysis, cyber-triage analysis, forensic analysis and malware analysis; and

d. Any further material included in the DFA Report provides further information supporting or summarizing the advice, recommendations and analysis contained in the DFA Report.

[14] "Advice" is guidance offered by one person to another. It can include the analysis of a situation or issue that may require action and the presentation of options for future action, but not the presentation of facts. Advice encompasses material that permits the drawing of inferences with respect to a suggested course of action, but which does not itself make a specific recommendation. It can be an implied recommendation. The "pros and cons" of various options also qualify as advice. It should not be given a restricted meaning. Rather, it should be interpreted to include an opinion that involves exercising judgement and skill in weighing the significance of fact. It includes expert opinion on matters of fact on which a government institution must make a decision for future action (*Guide to FOIP*, Ch. 4, p. 124).

[15] Advice includes the views or opinions of a public servant as to the range of policy options to be considered by the decision maker even if they do not include a specific recommendation on which option to take. Advice has a broader meaning than recommendations. The legislative intention was for advice to have a distinct meaning from recommendations. Otherwise, it would be redundant. While "recommendation" is an express suggestion, "advice" is simply an implied recommendation (*Guide to FOIP*, Ch. 4, p. 124).

[16] A "recommendation" is a specific piece of advice about what to do, especially when given officially; it is a suggestion that someone should choose a particular thing or person that one thinks particularly good or meritorious. Recommendations relate to a suggested course of action more explicitly and pointedly than "advice". It can include material that relates to a suggested course of action that will ultimately be accepted or rejected by the person being advised. It includes suggestions for a course of action as well as the rationale or substance for a suggested course of action. A recommendation, whether express or inferable, is still a recommendation (*Guide to FOIP*, Ch. 4, p. 125).

[17] "Analyses" (or analysis) is the detailed examination of the elements or structure of something; the process of separating something into its constituent elements (*Guide to FOIP*, Ch. 4, p. 125).

[18] Advice, proposals, recommendations, analyses or policy options can be revealed in two ways:

- the information itself consists of advice, proposals, recommendations, analyses or policy options; or
- the information, if disclosed, would permit the drawing of accurate inferences as to the nature of the actual advice, proposals, recommendations, analyses or policy options.

[19] Upon review of these pages, my office noted the following regarding each item:

a. Pages 20 to 48 of the DFA Report - Most of these pages did contain advice from SaskTel to eHealth regarding decisions for future actions. However, parts of pages 20 and 33, lay out some facts about the incident that led to the breach.

   I note that paragraphs 1 to 3 on page 20 of the DFA Report discuss some of the details surrounding the incident that led to the breach, however, these paragraphs have already been referenced in my Investigation Report 009-2020, 053-2020, 224-2020 at paragraphs 12, 36 and 37. I also note that paragraphs 1 to 3 on page 20 of the DFA Report, list the name of an employee and the names of eHealth's ports/ computer systems, where the ransomware attack occurred. I recommend that eHealth redacts that information and release the remainder of the information in paragraphs 1 to 3 on page 20 of the DFA Report.

In addition, paragraphs 132 and 134 of my Investigation Report 009-2020, 053-2020, 224-2020 also quote some of the information found in paragraphs 3 and 4 on page 33 of the DFA Report. Therefore, it appears that this information has already been released. As such, I recommend that eHealth releases paragraphs 3 and 4 of page 33 of the DFA Report.

Therefore, I find that all pages from 20 to 48, except part of pages 20 and 33, meet the first part of the test for section 17(1)(a) of FOIP.

b. Pages 49 to 51 of the DFA Report are in fact recommendations from SaskTel to eHealth regarding its cyber security maturity levels and the recommended options and steps required to reach those maturity levels. Therefore, these pages meet the first part of the test for section 17(1)(a) of FOIP.

c. Pages 52 to 290 of the DFA Report are pages containing detailed analyses conducted by SaskTel for eHealth. In these pages, SaskTel details: data analysis methodology, live response analysis, cyber triage analysis, forensic analysis and malware analysis for multiple computer systems/ports where the attack occurred. Therefore, these pages meet the first part of the test for section 17(1)(a) of FOIP.

2. Was the advice, proposals, recommendations, analyses and/ or policy options developed by or for a government institution or a member of the Executive Council?

[20] "Developed by or for" means the advice, proposals, recommendations, analyses and/or policy options must have been created either: 1) within the government institution, or 2) outside the government institution but for the government institution and at its request (for example, by a service provider or stakeholder) (*Guide to FOIP*, Ch. 4, p. 126).

[21] For information to be developed by or for a government institution, the person developing the information should be an official, officer or employee of the government institution, be contracted to perform services, be specifically engaged in an advisory role (even if not paid), or otherwise have a sufficient connection to the government institution (*Guide to FOIP*, Ch. 4, p. 127).

[22] The advice, proposals, recommendations, analyses and/or policy options can be developed by or for a government institution other than the one relying on the exemption.

[23] In its submission to my office, eHealth explained:

> SaskTel was engaged to assist in incident response services in relation to the Ransomware Attack and, in this role, SaskTel prepared the DFA Report. Furthermore, the cover page of the DFA Report explicitly states that the report was prepared for eHealth.

[24] Upon review, my office noted that the DFA Report was prepared by SaskTel's "Business Sales and Solutions – Digital Forensics" unit for eHealth exclusively, to assist with eHealth's investigation of the Ryuk ransomware attack. Moreover, along with its submission to my office, eHealth also provided my office with a copy of the "Confidentiality and Non-Disclosure Agreement" signed between eHealth and SaskTel. That agreement indicates that SaskTel was retained to provide incident response support services to eHealth in connection with a cybersecurity ransomware incident. This agreement was signed between the Vice President (VP)/ Chief Financial Officer (CFO) of eHealth and the VP Business Sales of SaskTel.

[25] Therefore, I find that the DFA Report was developed by SaskTel exclusively for eHealth. As such, the second part of the test for section 17(1)(a) of FOIP is met.

[26] As both parts of the test have been met, I find that eHealth appropriately applied section 17(1)(a) of FOIP to parts of the DFA Report. I recommend that eHealth continue to withhold the parts of the record where it applied section 17(1)(a) of FOIP appropriately and release the remining parts as outlined above. For details, see Appendix A of this Report.

[27] eHealth also applied sections 15(1)(m), 21 and 22(a) of FOIP to the entire DFA Report. However, as I have found that section 17(1)(a) of FOIP applies to pages 20 to 48, 49 to 51 and 52 to 290, there is no need to consider other exemptions on these pages. I will, however, consider these exemptions for the remaining information, which includes pages 1 to 19 and 291 to 870 of the DFA Report.

3. Did eHealth properly apply section 15(1)(m) of FOIP?

[28] eHealth applied section 15(1)(m) of FOIP to all the information on pages 1 to 19 and 291 to 870 of the DFA Report. eHealth also applied sections 15(1)(c) and (e) of FOIP to this information. However, in its submission to my office, eHealth stated that it was focusing only on the key exemptions that support its decision to deny access in full. eHealth did not provide any arguments to my office, to support sections 15(1)(c) and (e) of FOIP. Therefore, I will only review the application of section 15(1)(m) of FOIP in this matter.

[29] Section 15(1)(m) of FOIP provides:

> **15**(1) A head may refuse to give access to a record, the release of which could:
>
> …
> (m) reveal the security arrangements of particular vehicles, buildings or other structures or systems, including computer or communication systems, or methods employed to protect those vehicles, buildings, structures or systems.
> …

[30] Section 15(1)(m) of FOIP is a discretionary class-based exemption. It permits refusal of access in situations where release of a record could reveal the security arrangements of particular vehicles, buildings or other structures or systems, including computer or communication systems, or methods employed to protect those vehicles, buildings, structures or systems (*Guide to FOIP*, Ch. 4. p. 89).

[31] "Including" means that the list of information that follows is not complete (non-exhaustive). The examples in the provision are the types of information that could be presumed to qualify as "security arrangements" (*Guide to FOIP*, Ch. 4. p. 89).

[32] The following two-part test can be applied. However, only one of the questions needs to be answered in the affirmative for the exemption to apply. There may be circumstances where both questions apply and can be answered in the affirmative:

1. Could release reveal security arrangements (of particular vehicles, buildings, other structures or systems)?

2. Could release reveal security methods employed to protect the particular vehicles, buildings, other structures or systems?

   (*Guide to FOIP*, Ch. 4, pp. 88-91)

[33] In its submission to my office, eHealth provided arguments for both parts of the test for section 15(1)(m) of FOIP.

1. Could release reveal security arrangements (of particular vehicles, buildings, other structures or systems)?

[34] Section 15 of FOIP uses the word "could" versus "could reasonably be expected to" as seen in other provisions of FOIP. The threshold for *could* is somewhat lower than a reasonable expectation. The requirement for "could" is simply that the release of the information could have the specified result. There would still have to be a basis for the assertion. If it is fanciful or exceedingly remote, the exemption should not be invoked. For this provision to apply there must be objective grounds for believing that disclosing the information could reveal security arrangements of particular vehicles, buildings, other structures or systems (*Guide to FOIP*, Ch. 4. p. 89).

[35] "Reveal" means to make known; cause or allow to be seen (*Guide to FOIP*, Ch. 4. p. 89).

[36] "Security" means a state of safety or physical integrity. The security of a building includes the safety of its inhabitants or occupants when they are present in it. Examples of information relating to security include methods of transporting or collecting cash in a transit system; plans for security systems in a building; patrol timetables or patterns for security personnel; and the access control mechanisms and configuration of a computer system. Security means sufficient security (*Guide to FOIP*, Ch. 4. p. 90).

[37] "Other structures or systems" includes computer and communication systems. An example of a communication system could be a radio communication system such as two-way radios (*Guide to FOIP*, Ch. 4. p. 90).

[38] In its submission to my office, eHealth states:

Section 15(1)(m) is intended to protect exactly the type of information contained in the DFA Report from malicious actors who would misuse the information.

Your office has previously confirmed that structures or systems protected by this exemption include "computer and communication systems including the access control mechanisms and configuration of a computer system."

There are objective grounds to believe the disclosure of the DFA Report could reveal the security arrangements of eHealth's computer systems. In particular:

- The DFA Report contains extensive detail and background information regarding the security arrangements, including the access control methods and configurations, of eHealth's network and computer systems. For example, pages 55 through 258 of the DFA Report contain specific reports analyzing and outlining eHealth's specific computer systems.

- The remainder of the DFA Report holds sensitive details about eHealth's computer systems including eHealth's network and security system.

[39] Upon review of the DFA Report, it appears that this report extensively deals with the ransomware attack on eHealth's computer systems and the configuration of the network of such computer systems. The DFA Report identifies each computer system/ port where the virus attacked, provides a summary of findings regarding issues in eHealth's security systems, and includes SaskTel's analysis and recommendations to address and resolve those issues.

[40] Upon review of the DFA Report, my office noted the following:

a. Page 1 - is the title/cover sheet of the DFA Report. Some of the information listed on the title page includes who the DFA Report was prepared by (SaskTel), prepared for (eHealth), the business address of eHealth, case information and the name of the examiner. Some of this information was already discussed in my Investigation Report 009-2020, 053-2020, 224-2020 multiple times and is publicly available in newspapers, websites etc. The remaining information is factual information (e.g., name of the examiner, address of eHealth);

b. Pages 2 to 14 – provide the "Table of Contents". I note that a few lines items on pages 3 to 14, list the name of an employee and the names of eHealth's computer systems/ports, where the ransomware attack occurred;

c. Pages 15 to 19 - contain the "Examination Report" completed by SaskTel. These pages explain items such as the executive summary, ransomware note and anatomy of the attack. These five pages provide a list of computer system names/port identifications where the ransomware attack initiated and how it appeared to have moved laterally within eHealth's computer systems to infect more computer systems;

d. Pages 291 to 828 – appear to show the contents, commands and results of multiple malwares files/scripts identified by SaskTel on eHealth's computer systems to detect and undo the effects of the ransomware attack. These pages simply provide the results of these commands listing the names, addresses and drive path for each computer/port where the attack occurred; and

e. Pages 829 to 870 - SaskTel appears to provide guidance to eHealth to promote security of its computer network operating system. These pages also list multiple malware programs discussing various scripts that data attackers may follow, their strategy, activity movements, technical analysis of such malware and recommendations to identify and address those issues. These pages also provide scripts and drive paths for such malware attacks and system errors. To some malicious actors, such information may also identify potential security gaps and loopholes, inviting further attacks.

[41] It is clear that if released, these pages could identify the exact computer systems/ports which were vulnerable to a malware attack in the past and the movement of such an attack within eHealth's network. Release of such information could be of interest to malicious actors and could leave eHealth's configuration of the security of these computer systems vulnerable.

[42] Therefore, I find that all pages listed above, except page 1 containing the title page and parts of pages 2 to 14 containing the "Table of Content", contain security arrangements of eHealth's computer network operating systems and thus, meet the first part of the test for section 15(1)(m) of FOIP. As such, I find eHealth appropriately applied section 15(1)(m) of FOIP to parts of pages 2 to 14, all of pages 15 to 19 and 291 to 870 of the DFA Report. As only one part of the test must be met for the exemption to be found to apply, I do not need to consider the second part of the test for these pages. I will only consider if the second part of the test applies to pages 1 to 14 of the DFA Report.

2. ***Could release reveal security methods employed to protect the particular vehicles, buildings, other structures or systems?***

[43] Definitions of words such as "could", "reveal", "security" and "other structures or systems" are explained above at paragraphs [34], [35], [36] and [37] of this Report.

[44] "Method" means a mode of organizing, operating, or performing something (*Guide to FOIP*, Ch. 4. p. 90).

[45] The government institution must demonstrate that the information in the record is information that would reveal security methods employed to protect particular vehicles, buildings, other structures or systems to meet this part of the test.

[46] In its submission to my office, eHealth further explained:

> For the same reasons outlined above, eHealth submits that the release of the DFA Report could reveal security methods employed to protect eHealth's computer and network systems… The DFA Report contains extensive technical details regarding the methods and modes eHealth uses in the operation of its network and computer system…

[47] Earlier in this Report at paragraph [40], I explained the contents of pages 1 to 14 in detail.

[48] I note that most of the information contained in the DFA Report, is clearly intended to identify and remedy the issues of security of eHealth's network of computer systems. As explained above, that is not the case for pages 1 to 14 of the DFA Report. As such, I find that pages 1 to 14 of the DFA Report do not meet the second part of the test for section 15(1)(m) of FOIP.

[49] Therefore, I find that eHealth appropriately applied section 15(1)(m) of FOIP to the employee's name and the names of the computer systems/ports on pages 3 to 14, all of pages 15 to 19 and 291 to 870. I also find that eHealth did not appropriately apply section 15(1)(m) of FOIP to pages 1 to 2 and the remaining information on pages 3 to 14.

[50] As such, I recommend that eHealth continue to withhold the parts of the record where it appropriately applied section 15(1)(m) of FOIP. For details, see Appendix A of this Report.

[51] eHealth also applied sections 21 and 22(a) of FOIP to the entire DFA Report. However, as I have found sections 17(1)(a) and 15(1)(m) of FOIP applies to most of the DFA Report, I will only consider if sections 21 and 22(a) of FOIP apply to pages 1, 2 and the remaining parts of pages 3 to 14, of the DFA Report.

4. Did eHealth properly apply section 21 of FOIP?

[52] eHealth applied section 21 of FOIP, to the title page and the Table of Contents on pages 1 to 14 of the DFA Report.

[53] Section 21 of FOIP provides:

> **21** A head may refuse to give access to a record if the disclosure could threaten the safety or the physical or mental health of an individual.

[54] Section 21 of FOIP is a discretionary, harm-based exemption. It permits refusal of access in situations where disclosure of a record could threaten the safety or the physical or mental health of an individual (*Guide to FOIP*, Ch. 4, pp. 251 - 254).

[55] The following test can be applied:

> ***Could disclosure of the record threaten the safety or the physical or mental health of an individual?***

[56] For section 21 of FOIP, the question that must be answered is "could" disclosure of the record threaten the safety or the physical or mental health of an individual? The threshold for "could" is somewhat lower than a reasonable expectation but well beyond or considerably above mere speculation. On the continuum, speculation is at one end and certainty is at the other. The threshold for "could" therefore, is that which is possible (*Guide to FOIP*, Ch. 4, p. 251).

[57] "Speculative" means engaged in, expressing, or based on conjecture rather than knowledge. "Conjecture" is an opinion or conclusion based on incomplete information. Speculation generally has no objective basis. If the harm is fanciful or exceedingly remote, it is in the realm of speculation or conjecture (*Guide to FOIP*, Ch. 4. pp. 251-252).

[58] "Possible" means capable or existing, happening, or being achieved; that which is not certain or probable (*Guide to FOIP*, Ch. 4. p. 252).

[59] "Probable" means likely to happen or be the case (*Guide to FOIP*, Ch. 4. p. 252).

[60] Generally, in determining whether this exemption should be applied, the government institution must assess the risk and determine whether there are reasonable grounds for concluding there is a danger to the health or safety of any person. The assessment must be specific to the circumstances under consideration. Inconvenience, upset or the unpleasantness of dealing with difficult or unreasonable people is not sufficient to trigger the exemption. The threshold cannot be achieved based on unfounded, unsubstantiated allegations. The government institution should be able to detail what the harm is and to whom the harm threatens if the information were released.

[61] To "threaten" means to be likely to injure; be a source of harm or danger to. It means to create the possibility or risk of harm or jeopardize an individual's safety or mental or physical well-being (*Guide to FOIP*, Ch. 4. p. 252).

[62] "Safety" means the state of being protected from or guarded against hurt or injury; freedom from danger (*Guide to FOIP*, Ch. 4. p. 252).

[63] "Physical health" refers to the well-being of an individual's physical body. Determination of the effect of a release of information on an individual's physical health must consider the current or normal state of health of persons who may be affected by the release of information, as well as the decline in health that is expected to occur if the information is disclosed to the applicant (*Guide to FOIP*, Ch. 4. pp. 252-253).

[64] "Mental health" means the condition of a person in respect of the functioning of the mind. It means the ability of a person's mind to function in its normal state. Determination of the effect of a release of information on a person's mental health must, where practicable, be based on a subjective evaluation made on a case-by-case basis. It may be helpful for the head to obtain the assistance of an expert (e.g., a psychiatrist) when making this determination (*Guide to FOIP*, Ch. 4. p. 253).

[65] In its submission to my office, eHealth explained:

> In this case, the release of the DFA Report increases the risk of another cybersecurity incident occurring and such incidents have the real risk of threatening the safety and health of individuals:
>
> - As noted in the eHealth Investigation Report, the DFA outlines weaknesses in eHealth's network security and network infrastructure and the disclosure of such details would compromise eHealth's network security. These weaknesses can easily be exploited by malicious actors, who are clearly interested in exploiting this information as evidenced by the Ransomware Attack.
>
> - Similarly, the details about preventative measures and responses to incidents should not be made publicly available as this information can also be misused by malicious actors in future attacks to thwart such measures and responses.
>
> - Should the DFA Report be released, there is a very high risk that malicious actors or criminals would use the information to carry out additional cyber-attacks or ransomware against eHealth. The DFA Report reads as a playbook for how to inflict the maximum amount of damage to eHealth's network and computer systems. Given the sensitive nature of the personal and personal health information in eHealth's possession and control, and the essential function eHealth performs in providing healthcare related services to Saskatchewan residents, additional ransomware or cyber-attacks against its security network pose a grave and serious risk to the safety and health of individuals and the public generally. As such, protecting the DFA Report promotes public safety.

[66] As noted earlier, pages 1 to 14 constitute the title page and the Table of Contents for the DFA Report. The information on these pages is not sensitive (except for the limited information I found should be severed on pages 3 to 14 pursuant to section 15(1)(m) of FOIP). The Table of Contents provides a high-level list of the areas addressed and the order

they were addressed in. I expect any investigation of this nature would follow a similar format.

[67] As such, I find that eHealth did not appropriately apply section 21 of FOIP to pages 1, 2 and the remaining parts of pages 3 to 14 of the DFA Report. eHealth also applied section 22(a) of FOIP to this information. I will consider whether that exemption applies.

5. Did eHealth properly apply section 22(a) of FOIP?

[68] eHealth applied section 22(a) of FOIP, to the entire record. As explained above, I only need to consider if section 22(a) of FOIP applies to pages 1, 2 and the remaining parts of pages 3 to 14 of the DFA Report.

[69] Section 22(a) of FOIP provides:

> **22** A head may refuse to give access to a record that:
>
> (a) contains any information that is subject to any privilege that is available at law, including solicitor-client privilege;
>
> …

[70] Section 22(a) of FOIP is a discretionary, class-based exemption. It permits refusal of access in situations where a record contains information that is subject to any legal privilege, including solicitor – client privilege (*Guide to FOIP*, Ch. 4, pp. 255 – 277).

[71] "Including" means that the list of information that follows is not complete (non-exhaustive). The example in the provision is the type of information that could be presumed to qualify as a "privilege available at law" (*Guide to FOIP*, Ch. 4. p. 256).

[72] "Privilege" is a special right, exemption, or immunity granted to a person or class of persons (*Guide to FOIP*, Ch. 4. p. 256).

[73] There are several types of privilege; however, in this matter eHealth has cited solicitor-client privilege. The purpose of solicitor-client privilege is to assure clients of

confidentiality and the ability to speak honestly and candidly with their legal representatives. The privilege has long been recognized as "fundamental to the proper functioning of our legal system" and a cornerstone of access to justice. It has evolved from a rule of evidence to a substantive rule that is more nuanced than simply any communications between lawyer and client (*Guide to FOIP*, Ch. 4. p. 258).

[74] Further, solicitor-client privilege must be claimed document by document, and that each document must meet the three-part test. The following three-part test can be applied:

1. Is the record a communication between solicitor and client?
2. Does the communication entail the seeking or giving of legal advice?
3. Did the parties intend for the communication to be treated confidentially?

[75] As explained above, I only need to consider if section 22(a) of FOIP applies to pages 1, 2 and the remaining parts of pages 3 to 14 of the DFA Report.

1. Is the record a communication between solicitor and client?

[76] In *Descoteaux et al. v. Mierzwinski*, (1982), Justice Lamer outlined a very liberal approach to the scope of the privilege by extending it to include all communications made "within the framework of the solicitor-client relationship." The protection is very strong, as long as the person claiming the privilege is within the framework.

[77] A "communication" is the process of bringing an idea to another's perception; the message or ideas so expressed or exchanged; the interchange of messages or ideas by speech, writing, gestures or conduct (*Guide to FOIP*, Ch. 4. p. 258).

[78] "Client" means a person who:

- consults a lawyer and on whose behalf the lawyer renders or agrees to render legal services; or
- having consulted the lawyer, reasonably concludes that the lawyer has agreed to render legal services on his or her behalf; and

- includes a client of the law firm of which the lawyer is a partner or associate, whether or not the lawyer handles the client's work.

(*Guide to FOIP*, Ch. 4. pp. 258-259)

[79] In its submission to my office, eHealth explained the following:

- In this case, the client was eHealth and the solicitors were lawyers from MLT Aikins LLP ("MLT").

- SaskTel was engaged to provide incident response support services in order to assist MLT Aikins to provide confidential and privileged legal advice to eHealth and to prepare for any future litigation related to the Ransomware Attack.

- Pursuant to this engagement, eHealth and SaskTel entered into both a Confidentiality and Non-Disclosure Agreement and a Statement of Work. In addition, SaskTel signed an acknowledgment of a letter from MLT Aikins that confirmed the nature of the engagement and explicitly stated that information generated during the course of the engagement is subject to privilege including solicitor-client privilege and litigation privilege, and that the sharing of privileged material "is not intended to waive or diminish in any way the confidentiality of such material or its continued protection under solicitor-client privilege."…

[80] Earlier in this Report at paragraph [25], I found that the DFA Report was developed by SaskTel exclusively for eHealth. That means that the record in question, in its entirety was developed by SaskTel for eHealth (a government institution). In addition, based on submissions to my office, SaskTel appears to have provided the DFA Report directly to eHealth. Even if legal counsel was copied in the communication to eHealth, it does not make the communication privileged. As such, this record does not appear to be a communication between solicitor and client, i.e., MLT and eHealth. Therefore, I find that pages 1, 2 and the remaining parts of pages 3 to 14 do not meet the first part of the test for section 22(a) of FOIP.

[81] As all parts of the three-part test must be met, there is no reason to consider the remaining two parts of the test for section 22(a) of FOIP.

[82] Therefore, I find that eHealth did not appropriately apply section 22(a) of FOIP to pages 1, 2 and the remaining parts of pages 3 to 14 of the DFA Report. For details, see Appendix A of this Report.

6. Did eHealth meet its obligations pursuant to section 8 of FOIP?

[83] In its submission to my office, eHealth stated that it denied access to the requested record in full pursuant to sections 15(1)(c), (e), (m), 17(1)(a), 21 and 22(a) of FOIP.

[84] Section 8 of FOIP provides:

> **8** Where a record contains information to which an applicant is refused access, the head shall give access to as much of the record as can reasonably be severed without disclosing the information to which the applicant is refused access.

[85] My office's *Guide to FOIP*, Chapter 3: "Access to Records", updated on June 29, 2021, (*Guide to FOIP*, Ch. 3) explains "severability" is the principle described in section 8 of FOIP requiring that information be disclosed if it does not contain, or if it can be reasonably severed from, other information that the head of a government institution is authorized or obligated to refuse to disclose under the Act (*Guide to FOIP*, Ch. 3, pp. 44-46).

[86] "Severing" is the actual exercise by which portions of a document are blacked or greyed out before the document is provided to an applicant. It is the physical masking or removal from a record any information that is being exempted from disclosure in order that the remainder of the record may be disclosed (*Guide to FOIP*, Ch. 3, pp. 44-45).

[87] "Reasonable severability" – section 8 uses the phrase "can reasonably be severed." FOIP does not elaborate on what constitutes reasonable severability. One principle that has emerged from decisions of other IPC offices and the courts is that information that comprises of only disconnected or meaningless snippets is not reasonably severable, and such snippets need not be released. In this regard, an important consideration is whether the degree of effort to sever the record is proportionate to the quality of information remaining in the record. The process of reaching the conclusion that information is not

reasonably severable is one which should be approached with caution. It is not an issue of "what purpose is to be served by disclosure" so much as an issue of "whether there is any information which is reasonably being conveyed by the exercise of severance". If there are more than disconnected snippets being disclosed, the information can be considered reasonably severable.

[88] In order to comply with section 8 of FOIP, a line-by-line analysis of the record at issue is required to determine which exemptions apply to which portions of the record and what can reasonably be severed. The government institution is required to sever those portions that may qualify for a mandatory or discretionary exemption and release the balance of the record to an applicant.

[89] In this case, it appeared as though eHealth used a blanket approach in denying access to the DFA Report, in full. As explained in my analysis above, pages 1 to 14 could have been reasonably severed and released to the Applicant.

[90] As such, I find that eHealth did not comply with section 8 of FOIP. Therefore, I recommend that eHealth review its policies and procedures to ensure that it is consistent with its obligations pursuant to section 8 of FOIP.

IV FINDINGS

[91] I find that eHealth appropriately applied section 17(1)(a) of FOIP to parts of the record, except to parts of pages 20 and 33.

[92] I find that eHealth appropriately applied section 15(1)(m) of FOIP to parts of the record.

[93] I find that eHealth did not appropriately apply section 21 of FOIP to pages 1, 2 and parts of pages 3 to 14.

[94] I find that eHealth did not appropriately apply section 22(a) of FOIP to pages 1, 2 and parts of pages 3 to 14.

[95] I find that eHealth did not comply with section 8 of FOIP.

V RECOMMENDATIONS

[96] I recommend that eHealth continue to withhold and release the record according to Appendix A of this Report.

[97] I recommend that eHealth review its policies and procedures to ensure that it is consistent with its obligations pursuant to section 8 of FOIP.

Dated at Regina, in the Province of Saskatchewan, this 2nd day of March, 2022.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner

Appendix A

Page #	Description	Exemption of FOIP eHealth Applied	Withheld in Full (F) or Part (P)	FOIP Exemption found to Apply
1	Title page	15(1)(m)	F	Release
2 – 14	Table of Contents	15(1)(m)	F	15(1)(m) in part, release remaining
15 – 19	Examination Report	15(1)(m)	F	15(1)(m), continue to withhold
20 – 48	Advice	17(1)(a) and 15(1)(m)	F	17(1)(a) in part, release parts of pages 20 and 33
49 – 51	Recommendations	17(1)(a) and 15(1)(m)	F	17(1)(a), continue to withhold
52 – 290	Analysis	17(1)(a) and 15(1)(m)	F	17(1)(a), continue to withhold
291 – 828	Program scripts	15(1)(m)	F	15(1)(m), continue to withhold
829 – 870	Ransomware attack and program scripts	15(1)(m)	F	15(1)(m), continue to withhold