Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 147

HR16-32

A Public Hospital

June 18, 2021

Summary:

This investigation file was opened after a public hospital contacted the Office of the Information and Privacy Commissioner/Ontario to report a privacy breach under the *Personal Health Information Protection Act, 2004*. The hospital advised that a patient had made a complaint, which alleged the unauthorized use and disclosure of her personal health information by a named physician. In particular, this investigation related to concerns that a "quality audit" the physician was conducting resulted in referrals of motor vehicle accident patients to his wife, a personal injury lawyer.

This Decision concludes that the quality audit conducted by the physician was an unauthorized use under the *Act*, and that I am unable to determine whether the physician disclosed personal health information in contravention of the *Act.* It also concludes that the hospital's previously vague policies, practices and procedures regarding quality audits, and the complete lack of privacy training for physicians, did not amount to taking reasonable steps to protect the personal health information within the meaning of section 12(1) of the *Act*. However, I also find that the hospital has since remedied these issues.

Lastly, I decide that this review will be concluded without proceeding to the adjudication stage and without an order being issued by this office.

Statutes considered: *Personal Health Information Protection Act, 2004*, sections 2, 3(1), 4(1)(a) and (b), (6)(1), 10(1) and (2), 12(1), 17(2), 18, 20(2), 29, and 37(1).

Decisions considered: HO-010 and HO-013.

INTRODUCTION:

[1] This investigation file was opened after a public hospital (the hospital) contacted the Office of the Information and Privacy Commissioner/Ontario (the IPC or this office) to report a privacy breach under the *Personal Health Information Protection Act, 2004* (the *Act*). The hospital advised that a patient had made a complaint (the patient), which alleged the unauthorized use and disclosure of her personal health information by a named physician[1] (the physician). In particular, this investigation related to concerns that a "quality audit" [2] the physician was conducting resulted in referrals of motor vehicle accident (MVA) patients to his wife, a personal injury lawyer.

[2] While I originally had concerns with a number of the hospital's policies and the adequacy of the privacy training offered to staff at the time of this complaint, the hospital has since updated its policies and training practices to my satisfaction.

[3] I also had serious concerns about the evidence relating to the quality audit and the doctor's actions (particularly around potential disclosures of personal health information to his wife). I concluded that the so-called quality audit conducted by the physician constituted an unauthorized use under the *Act* and this practice has since ceased. However, despite multiple attempts to interview relevant witnesses, they did not respond to communications from the IPC. I recognize that I could compel these individuals to give evidence, but I do not think it would be appropriate to do so on the facts of this case given their apparent unwillingness to participate further in this investigation, and in consideration of the steps that have been taken by the hospital to address the issue of quality audits at the hospital going forward. As such, I am unable to determine whether the physician disclosed personal health information in contravention of the *Act*.

[4] During the hospital's investigation into the patient's allegations, the hospital also identified unauthorized accesses to records of personal health information by a clerk. According to the hospital, the clerk's accesses also appeared to relate to MVA patients. The clerk was since prosecuted and plead guilty to an offence under the *Act*.

[5] As a result of the above, and given the passage of time, I have decided that referring this specific case to an adjudicator would not advance the objectives of the *Act* and would serve no useful purpose at this stage. Accordingly, this matter will be

---

[1] In keeping with the IPC's practices, the hospital, the physician and others have not been identified by name in this decision. Practice direction: https://www.ipc.on.ca/wp-content/uploads/2017/02/2017-he-pd-03-e.pdf

[2] I use the term "quality audit" to refer to the activity of the physician in accessing patient records and telephoning them as described in this decision. I do so for convenience, as that is how this activity was described by the hospital. I note that the physician indicated he did not use this term. In my view, nothing turns on the use of this term, as the actual purpose of these activities can be seen from the more detailed descriptions and evidence obtained in this investigation.

concluded without proceeding to adjudication.

[6] While investigating this matter, I learned that other MVA patients contacted as part of the "quality audit" had similar experiences after leaving the hospital. They reported receiving calls from individuals who knew they had been in a MVA and were seeking to refer them to lawyers and physiotherapy clinics. I conclude this decision with a postscript indicating that hospitals, as well as other health information custodians, should be aware of the monetary value of these patients' personal health information and the related financial incentives that increase the risk of inappropriate disclosure. Accordingly, custodians should specifically turn their minds to, and carefully guard against, these risks when taking reasonable steps in the circumstances to protect personal health information in their custody or control against theft, loss and unauthorized use and disclosure.

BACKGROUND:

[7] On December 5, 2015, the patient attended the emergency department of the hospital as a result of a MVA. During her attendance at the hospital, she was treated for her injuries and then released. The physician was not involved in providing, or assisting in providing, health care to the patient during this attendance at the hospital.

[8] On December 9, 2015, the patient received a phone call from the physician at her home. According to the patient, the physician identified himself and stated that he worked in the emergency department of the hospital and was conducting a courtesy follow-up call to see how she was doing. The physician asked if she was experiencing any pain, if she had any complaints, and if she had started her physiotherapy yet. The patient informed the physician that she had not started physiotherapy as she was attempting to locate a clinic that was more convenient for her. The physician then recommended a clinic he said he was very familiar with and had sent other patients to in the past.

[9] According to the patient, the physician offered to have a specific doctor from the referring clinic contact her. Within minutes of ending her conversation with the physician, the patient received a phone call from the doctor of chiropractic running the clinic who advised he had spoken to the physician and understood she was looking for a physiotherapy clinic as a result of a MVA. The chiropractor indicated he would have his receptionist arrange an appointment. A few minutes later, the patient received a call from the receptionist who arranged for an appointment.

[10] On December 10, 2015, the patient attended the clinic with her husband and was met by the chiropractor she had spoken to. According to the patient's witness statement, the chiropractor was with a female lawyer. The patient and her husband were then ushered into a private room and asked how the clinic could help, and if the patient was interested in a lawsuit. The lawyer proceeded to spend approximately 30 minutes discussing the lawsuit process and MVA injury compensation with the patient and her husband.

[11] After this appointment, the patient began to have concerns about the appropriateness of the physician's access and use of her personal health information, given he had not provided her care when she attended the hospital. As a result, she contacted the hospital with her concerns.

[12] In March of 2016, the hospital contacted the IPC by telephone to report this matter. During this call, the hospital explained that it had looked into the patient's allegations and discovered a hospital clerk and the physician identified by the patient, both of whom were not within the patient's circle of care, had accessed her records of personal health information.

[13] The hospital also reported that the clerk had inappropriately accessed over 600 charts over two years, and the physician had accessed approximately 230 charts for patients that he was not providing care to.

[14] While the clerk's employment at the hospital was terminated as a result of her actions, the physician's accesses were not immediately considered unauthorized. According to the hospital, the physician claimed to be doing a quality audit that he had discussed with his Emergency Room Chiefs. In addition, the hospital reported that they had discovered that the physician's wife was the lawyer the patient met at the clinic.

[15] After providing the above noted information by phone, the hospital submitted a Breach Report dated April 4, 2016, which indicated the breaches related to patients who had been involved in MVAs. The report provided additional details regarding the hospital's investigation into the clerk's actions and the steps taken to address her accesses, which the hospital determined were unauthorized. The Breach Report also advised that an ongoing investigation continued with respect to the accesses of the physician.

[16] During communications with this office, the hospital also advised that "…the issue with respect to [the physician] is not clear regarding whether his activity was a breach or not. He has maintained that those records he viewed which were not patients of his were done so because he was undertaking a Quality Audit. The Hospital did not at any time sanction a Quality Audit, however both Chiefs in his department did have some discussions with him about the idea. There is a formal process that must be followed to conduct such an Audit and that was never brought forward, completed or approved in the case of [the physician]".

[17] On April 20, 2016, this office referred the matter to the Attorney General to consider commencing a prosecution for offences under the *Act*. An investigation was conducted by the Ontario Provincial Police (the OPP) which resulted in the hospital clerk being charged under the *Act*. She plead guilty and was convicted and fined. According to the Agreed Statement of Facts entered in that prosecution, the hospital's Privacy Department concluded that the clerk's accesses reflected a pattern of accessing the personal health information of patients involved in MVAs. The physician however was not charged with an offence under the *Act*.

Transfer to Investigation Stage at the IPC

[18] After referring this matter to the Attorney General, it was moved to the investigation stage of the IPC's process under the *Act*, and I was assigned as the investigator. However, due to the ongoing investigation by the OPP, this matter was placed on hold until the OPP's investigation and the prosecution of the clerk was completed. After the prosecution of the clerk was completed, this office determined that this matter should still be examined by the IPC to determine whether others were involved and whether any systemic or remedial matters should be addressed.

[19] As part of my investigation, I reviewed the information the hospital provided to this office during the Intake Stage, issued Notices of Review to a number of parties including the physician, the clerk, the hospital, the clinic, and the lawyer. I also made a Demand for Production to the OPP and received materials from the OPP[3] relating to its investigation. This office also issued a determination under section 60(13) of the *Act*, in relation to the materials produced by the OPP which contained personal health information.

[20] In addition, I wrote to the hospital and the physician with additional questions about the circumstances surrounding the breach, the hospital's policies and practices regarding quality audits and other related issues. Copies of the relevant information I obtained from the OPP and the hospital, as well as other information gathered by this office, were also provided to the physician.[4]

[21] After reviewing the documents and records and communicating with a number of witnesses, I decided to narrow the scope of my Review to focus only on the hospital and the physician.

[22] Information received from the OPP, the hospital, the physician and the patient, as well as my own conclusions with respect to this matter, are set out in this Decision.

Preliminary matters:

[23] There is no dispute that the person who operates the hospital is a "health information custodian" and the records the physician accessed in order to contact the patients are records of "personal health information" under the *Act*.

---

[3] The process for obtaining these materials was significantly more in-depth and involved discussions regarding redacting the materials. The physician was the only party who requested production so that he could respond to this investigation. Written undertakings were required prior to production being made to the physician (and his counsel). On December 3, 2019, I made a separate decision in the form of a letter addressing the production of records to the physician.

[4] As noted above, the production of materials obtained from the OPP and provided to the physician and his counsel contained redactions and were provided pursuant to signed undertakings. I made a separate decision in the form of a letter addressing this production.

[24] Based on the information set out above, as a preliminary matter, I find that the person who operates the hospital is a "health information custodian" under paragraph 4.i of section 3(1) of the *Act*, and that the information accessed by the physician in relation to the quality audit constitutes "personal health information" including under sections 4(1)(a), (b), and of the *Act*, which was in the custody or control of the hospital.

[25] I further find that the physician, who practiced in the emergency department of the hospital, was an "agent" of the hospital, as that term is defined in section 2 of the *Act*.[5] Although asked to, the physician chose not to provide representations to this question. The hospital does not dispute this finding.

ISSUES:

[26] The facts that led to this investigation raised a number of questions, including the physician's authority under the *Act* to use and potentially disclose patients' personal health information in relation to the quality audit. This investigation also raises the sufficiency of the steps taken by the hospital to protect personal health information in its custody or control from theft, loss and unauthorized use and disclosure.

[27] In this decision, the following issues will be discussed:

1. Was the personal health information at issue "used" in accordance with the *Act*?
2. Was the personal health information at issue "disclosed" in accordance with the *Act?*
3. Did the hospital take reasonable steps to protect personal health information?
4. Should this matter proceed to adjudication at the IPC, where a potential order may be issued?

DISCUSSION:

RESULTS OF THE INVESTIGATION:

Issue 1: Was the person health information at issue "used" in accordance with the *Act*?

Background

[28] During the investigation stage, I asked the physician to describe the quality audit

[5] *PHIPA* Orders HO-002, HO-010, and HO-013

he indicated he was conducting and to confirm that this quality audit was a "use" of "personal health information" under the *Act*.

[29] In a written response, the physician explained that there were two rounds of calls and that the quality audit was an initiative he thought of. He described his communications with both the former[6] and current[7] Chief of Emergency Services at the hospital with respect to contacting patients several days after their discharge from the emergency department in order to "follow-up and ensure that they are receiving any recommended or necessary care". According to the physician, the first Chief of Emergency Services thought "it was a good idea to contact patients, and use the information he collected for improving the quality of care provided to the patients in the [emergency] department".

[30] The physician also explained that in the fall of 2014 he had a conversation with the first Chief of Emergency Services at the hospital, regarding follow-up care. In that context the physician advised him that during his medical training in another country, as well as during various visits to other hospitals in another country in recent years, he had observed a practice by which hospitals contact patients several days after their discharge from the emergency department in order to follow-up and ensure that they are receiving any recommended or necessary care. According to the physician, it was during this conversation that it was agreed he could similarly assist patients at the hospital in this way, and that he could start contacting patients following their discharge from the hospital by telephone. The physician's response to this office described what he did as follows:

> These telephone conversations would consist of me asking patients various questions such as whether there was anything that we could do to assist them, whether they had any questions, whether they had followed up with their family doctors, etc. If a patient asked me to assist in locating a family physician, I directed the patient to contact the emergency department of their local hospital where a list of family physicians in that geographical area. If, and only if, a patient asked me to assist in locating a rehabilitation clinic, I would search online and provide them with the names of several clinics in their geographic area.

[31] During this first round of calls to patients which took place between October 2014 and January 2015, the physician stated that:

> Each time that I made a call to a former [hospital] patient, I made notes of our discussion, which included the patient's responses to my questions and the time at which I had accessed their chart for the purposes of

---

[6] Referred to below as the "first Chief of Emergency Services"
[7] Referred to below as the "second Chief of Emergency Services".

> making the call, which access typically occurred within a few days of the patients discharge…Every few weeks, I offered to provide my notes to [the first Chief of Emergency Services]. However, he made it clear to me he had no interest in reviewing my notes or discussing the details of my conversations with patients as he supported my initiative and the calls that I had been making. Thus, I eventually sent all of the notes I had made to be shredded and did not retain a copy of them, in large part to try to maintain patient confidentiality.

[32] According to the physician, in the spring of 2015, the second Chief of Emergency Services expressed an interest in reviving this initiative and asked him to prepare a list of the questions he intended to ask patients. The physician explained that after having the questions reviewed, he was directed to proceed with his quality audit, however he stopped making the calls in December 2015 due to the Christmas holidays. The physician also stated the following:

> In January 2016, it became clear that the Hospital [the second Chief of Emergency Services, and the Chief of Staff] took issue with my having pursued this initiative. I remain of the view that I had [the second Chief]'s express permission to do so, and that [the Chief of Staff] was aware of the initiative.
>
> …

[33] In support of his position, the physician referred to his communications with the Chiefs of Emergency Services which occurred between November 2014 and November 2015.

[34] The following are quotes from the relevant passages of text messages exchanged by the physicians on December 24, 2014 and relate to the first round of calls to patients. This information was also provided by the hospital in their representations, as well as in the materials produced by the OPP. They state the following in part:

> Physician:
>
> > Quickie update: as we discussed I've been calling/following up with some select pts 1-2 days post-visit (2-10/day) – trial and error re: pt type…simple Paeds/MVC/soft tissue basically all the stuff that is safely discharged (no major/significant pathology) but may still be anxious. Response has been positive+++…pts appreciative. Also a few upset/irritated pts-addressed concerns & at the time it seemed smoothed things out. Certainly puts our Emerg in a good light. Thought you'd like to know buddy…
>
> First Chief of Emergency Services:

> We should formalize it and it may be worth a presentation. Let me talk with patient relations. Great work.

[35] The following is an email sent by the physician on November 21, 2015, to the second Chief of Emergency Services and his response on November 22, 2015. These emails relate to the second round of calls to patients and state the following in part:

> Physician:
>
> > Hi [second Chief of Emergency Services' name],
> >
> > Met with …at the clinic today-glad to hear you are onboard.
> >
> > Followed up with him re: my calling emerg pts (satisfaction with visit, any concerns etc) – he had mentioned that you were okay with it when you both spoke earlier in the week.
> >
> > Just touching base-if there is anything in particular, any protocol/approach that you prefer I use, just let me know – if all is okay, I can start this week (just playing catch-up with some course work this weekend!!).
> >
> > I do not have your number, hence the email – my number is
> >
> > ….
> >
> > …
>
> Second Chief of Emergency Services:
>
> > Hi [the physician's name],
> >
> > I'm glad to hear that you would like to move forward on this plan. I suggest that we approach of [sic] from the patient satisfaction perspective. A standardized set of questions is the best way to go. We need to determine how we can do this best. It may be a good thing for you and I to speak this week. Let me know when you're available.
> >
> > My cell is ….
> >
> > …

[36] Subsequent to the above, on November 23, 2015, the physician sent a text to the second Chief of Emergency Services which stated the following in part:

> Physician:
>
> > Hey [second Chief of Emergency Services' name],

> It's [the physician's name], git [sic] your email – I'm in clinic today – should be free by mid/late afternoon or there's always the eve. Tue: same deal – mid-afternoon onwards. (I'm at clinic in the morning so will not …) BTW, If any of those times work great, or we can plan for later in the week.
>
> Cheers
>
> …

Second Chief of Emergency Services:

> Early evening might work if it's ok for you. How does round 5 work for you today?

Physician:

> No worries. Sounds good…

Second Chief of Emergency Services:

> …I just wanted to follow up on next steps after our phone call. When might be a good time to speak for you?

Physician:

> …Sorry- just got tied up getting things set up at the clinic… I have the form template and questions written out – just at …will email to you later and we can chat once you've had a look…

Second Chief of Emergency Services:

> No rush. I just wanted to reconnect on it. Have a great weekend. I'm in the ED on Monday and around all….

[37] On November 20, 2015, the physician texted a copy of the form he intended to use to keep records of his calls to patients, to the second Chief of Emergency Services and stated the following in part:

> …here's a draft of the satisfaction survey …very similar to the qs I asked previously. I can tweak/make changes and finesse it ongoing…I'm at the clinic this pm…so can pop in later if needed- depending on how I goes.

The second Chief of Emergency Services responded:

> Ok. That works for me.

The physician also stated the following in his submissions:

> I expressly recall that there was a particular evening in late November when [the second Chief of Emergency Services] asked me to call him at a particular time. During that call, [the second Chief of Emergency Services] confirmed that he was satisfied with the form's content and he directed me to proceed[8].

[38] In contrast, the hospital stated that despite the physician's claims that he was conducting a quality audit when he contacted the affected patients, the physician had not received approval to do so. The hospital explained that the quality audit was not approved by either Chief of Emergency Services, and that the physician was advised that formal approval was required. According to the hospital, the physician did not bring the approval request forward. The hospital stated the following:

> In order to conduct such an audit, there must either be Research Ethics Board (REB) approval for any proposed or ongoing research, which in this case, does not apply) or approval from the Medical Quality Assurance Committee, which is a sub-committee of the MAC. All audit requests coming to the Medical QA Committee must first be approved by the Chief of Program. The guidelines for a Medical QA audit are noted in item 17-32.16 of the Medical Staff bylaws, provided to Physicians at [the hospital] and they are reminded each year with reappointment that bylaws are to be followed at all times…

[39] The hospital also provided me with an excerpt from the relevant medical staff bylaws, which I quote from later in this Decision.

[40] According to a witness statement given to the OPP by the First Chief of Emergency Services, about the physician's first round of calls, after receiving a text from the physician about how well it was going he told the physician they needed to formalize the process, however he never heard back from the physician.

[41] The Second Chief of Emergency Services, who was in charge during the second round of calls was also interviewed by the OPP and stated that he did not believe the physician had followed the proper procedure to conduct a quality audit. He explained that doctors can apply to conduct audits to a Medical Quality Committee and that this would require notification on method and presentation of information learned that can be used to improve patient care. For a typical quality audit, when approved, contact via telephone or in person using information gained from the hospital is an acceptable use of that information. However, without the proper permissions, this information may not be used for this purpose. He also stated that there was no agreement in place or expectation that the physician would start contacting patients as they had not finalized

---

[8] The hospital and second Chief of Emergency Services did not have an opportunity to respond to this statement during this investigation as this was not necessary in light of my findings below.

the administrative process.

[42] The hospital, the OPP and the physician provided me with the form referred to above which I have reviewed. The form includes areas for the patient's name, date of birth, phone number, labs, imaging and reason for visit. It also includes an introductory script as follows:

> GREETING/INTRO & PURPOSE OF CALL: "Hello…, I'm Dr. …, a quick follow-up call about your recent ER visit, because how you are feeling and your feedback is important to us"

[43] The form included six questions as follows:

1. Firstly and most importantly, how are you? How are you feeling now?
2. Were all your questions answered/your concerns addressed whilst you were in Emerg?
3. Since your discharge any new Q's/concerns/developments-symptoms/pain/stiffness
4. Did we provide you with follow-up care instructions/where to get your follow up care?
5. Are all your questions answered fully/to your satisfaction?
6. Were you satisfied with your visit/care?

[44] I also reviewed copies of forms, which were filled out by the physician after speaking to patients. According to the information entered by the physician, the discussions with patients typically related to how they were feeling, whether they received follow up care, and their general satisfaction with the care they received at hospital.

[45] I should note that most of the information I received in this investigation related to the second round of calls the physician made as part of the quality audit which coincided with the time frame of the patient's allegations. In particular, I only have confirmation from the hospital on the policies/bylaws in place at the time the second round of calls was made. I also only have detailed evidence about what was discussed by the physician when he called patients (e.g. on the forms completed by the physician and evidence from patient's themselves) in relation to the second round of calls. As such, my below findings on whether the quality audit was an authorized use of personal health information under the *Act* are limited to the second round of calls. That said, the physician indicated that the questions asked in the second round of call were similar to the first round of calls, and some of the evidence in relation to the first round of calls is plainly relevant to my analysis of the second round of quality audit calls, discussed below.

Did the Quality Audit involve the "use" of Personal Health Information

[46] Section 2 of the *Act* defines the term "use" as follows:

> "use", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to handle or deal with the information, subject to subsection 6 (1), but does not include to disclose the information, and "use", as a noun, has a corresponding meaning;[9]

[47] In response to my question regarding whether his quality audit was a use of personal health information, the physician stated that:

> …I personally never used the words "quality audit" when calling patients. That being said, a complete description of the calls that I made can be found above. Again, as a physician, I do not feel that I am able to comment on whether the calls that I made fit any specific legal definition.

[48] After receiving the physician's responses to my questions, I contacted his legal representative and asked if they wished to make representations as his counsel. I received confirmation that no further representations would be made.

[49] The hospital stated the following with respect to whether the physician's accesses to the personal health information at issue were a use under the *Act*:

> As defined in PHIPA, "use" of personal health information (PHI) in the custody or control of a health information custodian (HIC) is the handling of and dealing with said information. "Use also includes relying on the information to undertake another activity, such as providing health care, carrying out research, evaluating services, or contacting the patients to whom the information relates." Properly approved quality audits would fit the PHIPA definition of "use", however, in [the physician's] case, it does not because it was not sanctioned or approved by [the hospital].

[50] I do not accept the hospitals position in this regard. In my view, the issue of whether the audit was approved is not relevant to determining whether the physician's accessing and dealing with personal health information was a "use" within the meaning of the *Act*. If that argument were accepted, the reference to protecting personal health information against "unauthorized use" in section 12(1) of the *Act* would be contradictory – because a "use" could not be unauthorized. I further note that section 6(1) of the *Act* specifically provides:

---

[9] This definition of "use" was in force at the time of these events. The definition has since been amended.

> For the purposes of this *Act*, the providing of personal health information between a health information custodian and an agent of the custodian is a use by the custodian, and not a disclosure by the person providing the information or a collection by the person to whom the information is provided.

[51] This provision makes no distinction between an authorized and unauthorized provision of personal health information to an agent. Further, in this case, there does not appear to be any dispute that the personal health information at issue was provided by the hospital to the physician – in that the hospital provided the physician with access to the EMR and the physician accessed personal health information in this EMR.

[52] The argument advanced by the hospital is somewhat analogous to the argument advanced in IPC Order HO-013, in which the hospital in that case argued that two employees were not "agents" because the employees were acting beyond the authority delegated by that hospital. In that case, Commissioner Beamish found, among other things, that:

> …if the Hospital's submissions were accepted, it would result in persons constantly transitioning between acting as agents and non-agents, potentially from one moment to the next, throughout the course of a day. The effort that would be required to determine exactly when each person was acting as an agent would create unnecessary confusion and ultimately frustrate the ability of the Commissioner and the courts to achieve the objects and purposes of the Act. The objects and purposes of the Act are not to apportion liability between the health information custodian and persons acting for or on its behalf. Its main object or purpose is to protect privacy and confidentiality of individuals in a health care setting.[10] [footnote in original omitted]

[53] In this case, I see no reason, or statutory support, for introducing the complexity suggested by the hospital in the categorization of a "use". In keeping with the plain meaning of the phrase "to handle or deal with the information" as set out in the definition of "use" in section 2 of the *Act*, and in light of section 6(1) of the *Act,* I find that the physician accessing personal health information for the purposes of the quality audit was a "use" within the meaning of section 2 of the *Act,* even if it were not sanctioned or authorized by the hospital.

Was this "use" authorized?

[54] Since I have found that the physician used the personal health information at issue in relation to the quality audit, I will now determine whether this use was

---

[10] HO-013, p. 15. See also HO-002 at p. 5 and HO-010 at p. 7.

authorized under the *Act*.

[55] Under the *Act*, personal health information is permitted to be used or disclosed if the use or disclosure complies with section 29, which states:

> 29. A health information custodian shall not collect, use or disclose personal health information about an individual unless,
>
> (a) it has the individual's consent under this *Act* and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or
>
> (b) the collection, use or disclosure, as the case may be, is permitted or required by this *Act*.

[56] There is no information or evidence before me to suggest that the patients contacted by the physician for the purposes of the quality audit consented (expressly or impliedly) to their personal health information being accessed by him or that he could assume the patients' implied consent.[11] No party has stated that the physician was accessing the personal health information of patients for the purpose of providing or assisting in the provision of health care (which would be relevant to some of the consent provisions of the *Act*).[12] As such, I find that the quality audit was not authorized on the basis of consent.

[57] When I asked the physician to explain his legal authority to conduct the quality audit, he did not point to a particular section of the *Act*, but rather advised that he believed that he had the "express authorization" of his Department Chiefs.

[58] In the physician's representations, he also referred to an excerpt from minutes of an Emergency Department meeting stating that "patient charts should only be accessed by those directly involved in the patient's circle of care unless part of a quality review". He went on to say that:

---

[11] See section 20(2) of the *Act*.

[12] See sections 18 and 20(2) of the *Act*.

I note that there was apparently one instance where, during a call with a patient, the physician provided a prescription for medication. This would fall under the definition of "health care" under the *Act*. This would appear to be an exception, and does not alter the overall characterization of the physician's purposes in conducting the quality audit.

I further note that the physician, at one point in his representations, refers to himself as being in the patient's circle of care in conducting the quality (see the quoted passage in the body of this decision). It is not clear to me that this general reference to the circle of care is meant to suggest that he could rely on the statutory authorities in the *Act* relating to using personal health information for providing, or assisting in the provision of, health care in conducting this audit. Elsewhere, he refers to the purpose of the audit as "being for the purpose of improving quality of care" – which I think is a more accurate description of his purpose and is distinct from providing or assisting in the provision of health care.

> I did not view my follow-up initiative as being in breach of this policy for three (3) reasons. First, I only pursued this initiative when I had (what I at least thought was) the clear authorization of my Chief at any given time – i.e. [names of the Chiefs of Emergency Services]. Second, the follow-up initiative seemed to be precisely the type of quality review for which accessing patient charts is allowed, as set out above. Third, it seems to me that by contacting patients for the sole purpose of ensuring that they were receiving appropriate follow-up care, I was in fact involved in that patients' circle of care.

[59] As noted above, when the breach was reported to this office, the hospital stated that "…the issue with respect to [the physician] is not clear regarding whether his activity was a breach or not. He has maintained that those records he viewed which were not patients of his were done so because he was undertaking a Quality Audit. The Hospital did not at any time sanction a Quality Audit, however both Chiefs in his department did have some discussions with him about the idea. There is a formal process that must be followed to conduct such an Audit and that was never brought forward, completed or approved in the case of [the physician]".

[60] Later, the hospital submitted:

> In order to conduct such an audit, there must either be Research Ethics Board (REB) approval for any proposed or ongoing research, which in this case, does not apply) or approval from the Medical Quality Assurance Committee, which is a sub-committee of the MAC. All audit requests coming to the Medical QA Committee must first be approved by the Chief of Program. The guidelines for a Medical QA audit are noted in item 17-32.16 of the Medical Staff bylaws, provided to Physicians at [the hospital] and they are reminded each year with reappointment that bylaws are to be followed at all times… As a result of this incident, one that [the hospital] has not previously experienced, the current Chief of Staff has since formalized the Medical QA process.
>
> …

[61] The most relevant portions of the Medical Staff bylaws state as follows:

> **17-32.8 Medical Advisory Sub-Committees - Quality Management**
>
> Each sub-committee of the Medical Advisory Committee will participate in a self-evaluation process and report on same through the Medical Quality Assurance Committee.
>
> …
>
> **17-32.16 Medical Quality Assurance Committee Duties**

The Medical Quality Assurance Committee shall:

.1 develop, implement and periodically evaluate and where appropriate modify a Medical Quality Assurance in accordance with legislation and accreditation standards, which includes mechanisms to:

.1-1 monitor appropriate trends and activities;

.1-2 identify potential problem areas;

.1-3 develop corrective action plans and provide follow-up;

.2 develop a mortality and morbidity review process and to support institution or departmental programmatic Clinical Practice Guideline initiatives;

.3 recommend procedures to assure that an ongoing peer review process is established for assessment of quality of patient care, i.e. but not exclusive to:

.3-1 review or cause to be reviewed regular medical records;

.3-2 identify the continuing medical educational needs of the Medical/Dental, Midwifery and Extended Class Nursing staff, and assure that actions are taken on the recommendations;

.3-3 assure that other medical audits are undertaken as necessary;

.4 monitor response to recommendations which are approved by the Medical Advisory Committee and Hospital Management and report back on progress achieved; and

.5 performs such other duties as may be requested from time to time by the Medical Advisory Committee.

[62] According to the hospital, the policies in place at the time of the physician's quality audit required formal approval and the physician did not bring the approval request forward. The hospital also advised that:

[the physician's] quality audit did not follow the usual process in the following ways:

- There was not formal approval from the Chief of the program.
- There was no formal approval, or even awareness, by the Medical QA Committee.

- There was no involvement of Health Information Services to obtain a list of cases needed for the audit, which is the normal procedure.

[63] I asked the hospital whether the quality audit was relevant to risk management, error management, or activities to improve or maintain the quality of care at the hospital. In response, the hospital stated the following:

> The "quality audit" conducted by [the physician] had no mandate, no clear objective, no protocol, nor formal approval. Therefore this "quality audit" would not be relevant to any activities listed above.

[64] I note that the physician indicated his view that "this initiative would best be described as being for the purpose of improving quality of care".

[65] Section 37(1) of the *Act* provides various authorities to use personal health information without patient consent:

> 37. (1) A health information custodian may use personal health information about an individual,
>
> (a) for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, but not if the information was collected with the consent of the individual or under clause 36 (1) (b) and the individual expressly instructs otherwise;
>
> …
>
> (c) for planning or delivering programs or services that the custodian provides or that the custodian funds in whole or in part, allocating resources to any of them, evaluating or monitoring any of them or detecting, monitoring or preventing fraud or any unauthorized receipt of services or benefits related to any of them;
>
> (d) for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian;
>
> …

[66] Further, at the time of the quality audit, section 17(2) of the *Act* stated the following:

> (2) Except as permitted or required by law and subject to the exceptions and additional requirements, if any, that are prescribed, an agent of a health information custodian shall not collect, use, disclose, retain or dispose of personal health information on the custodian's behalf unless

the custodian permits the agent to do so in accordance with subsection (1).

[67] The term "Agent" is defined in section 2 of the *Act* as:

> "agent", in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated;

[68] Further, sections 10(1) and (2) provide:

> 10. (1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations.
>
> (2) A health information custodian shall comply with its information practices.

[69] In turn, "information practices" are defined in section 2 of the *Act* as:

> "information practices", in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including,
>
> (a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and
>
> (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;

[70] In light of the above statutory provisions, in order for the quality audit to be an authorized use of personal health information by the physician as an agent of the hospital, this activity must (among other things):

- be done in compliance with the hospital's information practices under section 10 of the *Act,*
- be permitted by the custodian under section 17 of the *Act,* and
- be authorized under section 29 the *Act* (e.g. for a purpose authorized under section 37 of the *Act*).

[71] I conclude that this quality audit is not authorized under the *Act*, as it does meet

the first two requirements indicated above.[13]

[72] First, there is no evidence that the hospital's information practices under section 10 (1) of the *Act* in relation to quality audits were followed (and there does not appear to be any dispute that they were not). The hospital has provided its medical staff bylaws, quoted above, relating to medical quality assurance initiatives and submitted that these bylaws are applicable. As noted above, the physician informed the IPC that this initiative would best be described as being for the purpose of improving quality of care. This bylaw would appear to be applicable to this quality audit, and no one has submitted that it was not. As discussed below under Issue 3, the exact scope and requirements of the hospital bylaws was far from clear, and left significant room for interpretation. While recognizing these shortcomings, I accept that the hospital bylaws were applicable and that the hospital's information practices contemplated a role for the Medical Quality Assurance Committee, which did not occur. It is clear the hospital's information practices were not complied with in relation to the quality audit (in contravention of section 10 (2) of the *Act*).

[73] Second, I am unable to conclude that this use of personal health information was permitted by the hospital for the purposes of section 17 (2) of the *Act*. I draw this conclusion for the same reasons discussed above for explaining why this quality audit did not comply with the hospital's information practices. Further, in my view, the text messages and other communications exchanged between the physician and the two Chiefs of Emergency Services do not constitute permission by the hospital for this quality audit. The text messages and emails are, at best, ambiguous[14]. With respect to the call the physician says occurred between him and the second Chief of Emergency Services[15], even if this conversation occurred, the quality audit still did not comply with the hospital's information practices and that, alone, is sufficient to find this use contrary to sections 17 (2) and 10 (2) of the *Act*.

[74] I also have a great deal of difficulty accepting that such a broad audit involving calling hospital patients to whom the physician had not provided health care could reasonably be considered to be permitted in such a vague and ill-defined manner. In my view, in order for such a use of personal health information as this quality audit to be permitted by the hospital under s. 17 (2) of the *Act*, there must be a greater degree of detail in what is actually being permitted.

---

[13] As noted above, this finding is limited to the second round of quality audit calls.

[14] Among other things, I note that the physician stated that he took the phrase "works for me" from the second Chief of Emergency Services (quoted above) to mean that he had authorization and direction to resume the quality audit. In the context, this phrase is ambiguous and would appear to be in response to a suggestion that they could meet to make changes to the form.

[15] As noted above, in his submissions the physician described a call he had with the second Chief of Emergency Services, in which the physician says the second Chief of Emergency Services "confirmed that he was satisfied with the form's content and he directed me to proceed".

[75] In making these findings, I note that the physician indicated his belief that he complied with a statement in Emergency Department Minutes that "Patient charts should only be accessed by those directly involved in the patient's circle of care unless part of a quality review." I do not think that compliance with this statement, which appears to be nothing more than a summary reminder, guarantees compliance with the hospital's broader information practices, nor that this statement grants permission for any particular use. I note that the physician has further indicated that he was not aware of the hospital's policies, practices and procedures applicable to quality audits.

[76] Third, as I have found that this audit was not authorized under sections 10 (2) and 17 (2) of the *Act*, it is not necessary for me to consider whether the audit was authorized under sections 29 and 37.

[77] For the above reasons, I find the use of patient's personal health for the purposes of conducting the "quality audit" was not authorized under the *Act*.

[78] While the physician was not trained on the hospital's policies, practices and procedures in relation to quality audits, and the hospital's applicable policies, practices and procedures were certainly lacking in clarity and detail (as will be elaborated under Issue 3 below), this does not affect my conclusion that the quality audit was ultimately not authorized under the *Act*.

Issue 2: Was the personal health information at issue "disclosed" in accordance with the *Act*?

Background

[79] While I have found that the use of personal health information for the purposes of the quality audit was not in accordance with the *Act*, the next question that arises in this investigation is whether the physician disclosed this information, particularly to his wife as a personal injury lawyer, and whether this disclosure would have been authorized under the *Act.*

[80] As indicated earlier in this Decision, the physician referred the patient to a clinic where she was met by a personal injury lawyer (the physician's wife). This encounter raised questions with respect to whether her presence at the clinic was a coincidence; was the result of a disclosure from the physician to his wife, or if there was some other arrangement through which his wife knew that a MVA patient would be attending to the clinic that day.

[81] In response to questions about this matter, the physician confirmed to this office that his wife is a personal injury lawyer and the principal lawyer at a named law firm[16] but denied disclosing any information to her or any clinic, stating the following:

---

[16] The physician and his wife do not share the same last name.

> As a personal injury lawyer, my wife's clients are frequently patients who have visited Emergency Rooms throughout Ontario, including at the Hospital, as well as various rehabilitation clinics. As such, it would not be surprising if there were some overlap between the Hospital's patients and my wife's clients. However, my wife and I both take our respective duties of confidentiality very seriously, and have never divulged information about our patients/clients to one another, and we have certainly never shared our patients'/clients' identities with each other.

[82] According to the physician, he contacted the patient and asked her the questions set out in his questionnaire. The physician also explained that it was the patient who advised him that her insurance company had suggested she seek treatment at a particular clinic, but that clinic was inconvenient for her. The physician then indicated to her that she should consider going to another clinic, which might be more convenient for her. The patient then asked him to assist her with locating a convenient clinic, and based on her geographical location, he looked up and provided her with various rehabilitation clinics that would be convenient for her but did not highly recommend the particular clinic she ultimately attended. The physician also stated the following in part,

> I did not, and do not, have any affiliation with any of the practitioners or owners at [the clinic]. Moreover, I do not have a financial interest in [the clinic], nor does any member of my family. Contrary to what is alleged, I did not state that I would personally call the doctor at the clinic to help arrange an appointment for her. Rather, [the patient] asked me if I could facilitate connecting her with [the clinic] While this was not something that I typically did as part of this follow-up initiative, I agreed to contact [the clinic] on her behalf. I called the clinic and left a voicemail message asking them to contact [the patient] directly. That voicemail message was the only contact that I have ever had with [the clinic].
>
> It seems [the patient] ultimately went to [the clinic]. On the day of [the patient's] appointment, it just so happened that my wife was visiting [the clinic] with respect to an ongoing client file of hers, i.e. entirely independent from [the patient's] visit. As set out above, my wife works with various rehabilitation clinics throughout Ontario, though she does not have a financial interest in any particular clinic. When I provided [the patient] with the contact information for [the clinic], I had no idea that my wife even knew of that clinic. In short, it was a complete fluke and coincidence that my wife happened to be at [the clinic] the same day as [the patient]. It seems that, because my wife was at [the clinic] the clinic's owner asked my wife to meet with [the patient] to see if she could benefit from retaining a personal injury lawyer. According to my wife, she met with [the patient], however she was never retained by [the patient] and no substantive legal advice was ever imparted by her to [the patient]. When I was asked by the Hospital to explain why a patient was

> confronted by my wife, I expressly recall advising them that my wife has never confronted anyone to my knowledge.
>
> …

[83] Despite the physician's indication that the presence of his wife at the clinic was a total fluke and a coincidence, I note that the OPP spoke to two other individuals who had similar experiences to the patient, and unrelated to the clinic. I describe these individuals' experiences in more detail below.

[84] According to the hospital, the physician never informed them that he was referring patients to health care providers, lawyers/law firms, or service providers as part of his quality audit, and confirmed such referrals would not be permitted by the hospital. In addition, the hospital advised that a referral to his wife for legal services or to her law firm would be considered a conflict of interest.

[85] The hospital provided a copy of its "Conflicts of Interest, Hospital-Wide" policy dated October 17, 2013. This policy was in place during the time the physician was conducting his second round of calls for the quality audit and includes a policy statement, the hospital's expectations, the responsibility of employees, volunteers, or physicians, and a section titled "Identifying Real or Perceived Conflicts of Interest". This section states the following:

> An employee, volunteer, or Physician is said to be in a conflict of interest when:
>
> - he or she has the opportunity to influence, in any manner, a decision about Hospital business, reputation or financial position, AND
>
> - he or she or a family relation or a person with whom a relationship exists, will gain a financial or other personal benefit, gift or gratuity from the Hospital's or patient's decision to purchase/use supplies or services from a particular vendor or service provider.
>
> - when others perceive that both of the situations stated above exist, even if the situations do not exist.

[86] The policy also sets out the responsibilities of employees, physicians, surgeons and consultants to avoid real or perceived conflicts of interest and states they should ensure they diffuse any real or perceived conflict of interest by ensuring he or she:

- are not involved in any evaluation processes for the product or service being purchased in the conflict of interest situation;

- do not exert any influence over the hospital personnel making the decision as to which supplies or services to purchase or the process used to decide which supplies or services should be purchased;

- are not involved, in any manner, with any negotiations completed with the person or company with whom the conflict of interest exists;

- do not solicit patients to purchase supplies or services from any vendor or service provider with which they are in a conflict of interest situation.

[87] Further the policy required physicians to ensure they diffuse any real or perceived conflict of interest by ensuring that they do "not solicit patients to purchase supplies or services from any vendor or service provider with which they are in a conflict of interest situation."

[88] The hospital advised that in their view, this policy would apply because "referring patients to a family member's law firm for financial or other personal benefit would be considered a conflict of interest" and that the physician had "access to [the hospital's] PPM System which houses all polices and procedures that are to be followed by all staff, including physicians".

[89] The hospital advised that, at the time of the second round of calls to patients, the following policies were in force and made available to all agents of the hospital via their Policy and Procedures Management system which all staff have access to via their intranet:

- Assembly & Quantitative Analysis of In-Patient Records revised 30/07/15

- Code of Conduct Policy revised 29/07/15

- Confidentiality Agreements Policy revised 05/06/15

- Conflicts of Interest, Hospital-Wide Policy revised 17/10/13

- Conflicts of Interest, Procedure revised 17/10/13

- Privacy of Personal Information Policy revised 06/09/13

- REB Review of Research, The Review Process Policy revised 09/04/15

- Reporting Privacy Breaches, Policy revised 13/12/11

- Reporting Privacy Breaches, Procedure revised 13/12/11

- Research Compliance, QA-QC Program Policy revised 09/04/15

- Retention and Destruction of Personal Health Information Policy revised 04/08/15

- Staff Members Accessing Own Personal Health Information Policy revised 07/07/10

- Standards of Behaviour Confidentiality and Privacy Guideline revised 13/10/15

[90] The hospital also provided page four of a Declaration which was signed by the physician on 04/02/14. The Declaration stated the following in part:

> I will also comply with all Policies and Procedures within the hospital relating to the Personal Health Information Protection Act (PHIPA), and Policies relating to the appropriate use of Electronic Mail (email) and MOX. As a condition of my reappointment to the Medical/Dental Staff, I further agree to follow [hospital] Confidentiality and Release of Information policies at all times…

[91] In response to questions posed by this office, the physician advised that he was not aware of any policies, procedures or practices in place at the hospital with respect to conflicts of interest or perceived conflicts of interest including in relation to using or disclosing personal health information of patients for personal gain or perceived personal gain.

[92] Although the physician advised he was not aware of the above noted policy, according to the hospital it was made available to him on the hospital's intranet.

[93] The physician denied disclosing any of the personal health information that he used as part of the quality audit to any person or organization. He also denied referring any patients to any lawyer/law firm for legal advice (including his wife's law firm), which he agreed the hospital did not permit[17].

Was the personal health information disclosed and was this disclosure authorized?

[94] Section 2 of the *Act* defines the term "disclose" as follows:

> "disclose", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information, and "disclosure" has a corresponding meaning;

[95] There does not appear to be any dispute that, if the physician had provided personal health information to his wife relating to the patients he contacted as part of the quality audit, this would be a "disclosure" as that term is defined in the *Act*. There also does not appear to be any dispute that, if these disclosures took place, they would be unauthorized (among other things, as it would not be permitted under s. 17(2) of the *Act*, quoted above).

---

[17] I note that the evidence before me in regards to the physician referring patients to his wife for legal services relates only to the second round of calls.

[96] The patient and the physician have provided different versions of what was discussed during the call at issue in this matter. Despite this, the patient does not dispute that she was aware and agreed that the physician could call the clinic and would be providing her contact information so that an appointment could be arranged. What is not clear is whether the physician disclosed the patient's personal health information to his wife, if there was some other arrangement through which his wife knew that a MVA patient would be attending to the clinic that day, or if her presence there was "a complete fluke".

[97] The physician's position is that his wife's presence at the clinic was coincidental, and not related to the quality audit he was conducting. Even if I were to accept that this one instance relating to the patient was a coincidence, other individuals indicated to the OPP that they had similar experiences with the same physician. Specifically, one individual indicated to the OPP that during the quality audit call the physician [who she identified by name] asked her if she had retained a lawyer or sought legal advice. He also advised her that he knew a lawyer at a specific law firm [he named his wife's law firm] and advised the individual that he could have the lawyer contact her as soon as possible to assist with what she needed to do next. Within an hour, this individual received a message from a female, who identified herself as a lawyer from a named law firm [the physician's wife's law firm], and offered to speak to her about her options. The lawyer's message also explained that she had been provided the individual's information by the physician and that she understood the individual was seeking legal advice. The individual also advised that after being contacted by the lawyer, the physician left her several messages and in one of the messages the physician indicated he wanted to follow up in regards to whether she had heard from the law firm. The individual received three messages from the lawyer over the period of a week. The individual did not contact the lawyer and did not return the physician's calls.

[98] Another individual indicated to the OPP that, after the quality audit call from the physician, she was contacted by a different clinic. When she attended to that different clinic, she was also met by a representative of the physician's wife's law firm.

[99] I note that the physician stated that:

> To the extent that some other patients allege that they met "a representative from [his wife's law firm]" at their rehabilitation clinic, I have no knowledge of same as, again, my wife and I have never shared any information with one another regarding my patients/her clients. Similarly, I have never referred a patient to [his wife's law firm]. Indeed it seems as though some patients received telephone calls from [his wife's law firm] after their charts were also accessed by [the hospital clerk]. Again, I have no knowledge of [the hospital clerk's] access of patient charts.

[100] The physician also broadly stated, without referring to these two other patients specifically, that it is possible that patients who were interviewed were conflating their conversations with him with their conversations with others.

[101] As noted earlier, the hospital's Conflict of Interest policy specifically states that a physician would be in a conflict of interest if "he or she or a family relation or a person with whom a relationship exists, will gain a financial or other personal benefit, gift or gratuity from the Hospital's or patient's decision to purchase/use supplies or services from a particular vendor or service provider" or if others perceive that this situation exists, "even if the situations do not exist". The policy also sets out the expectation that:

- perceived conflicts of interest should be avoided with the same veracity as real conflicts of interest;
- failure to disclose conflict of interest situations may result in disciplinary action up to and including termination: and
- there's a responsibility to ensure no involvement in any evaluation processes for the product or service being purchased in the conflict of interest situation

[102] Further the policy required that the physician should ensure that he diffuse any real or perceived conflict of interest by ensuring he does "not solicit patients to purchase supplies or services from any vendor or service provider with which they are in a conflict of interest situation."

[103] In my view, a physician using a position as an agent of the hospital to refer MVA patients to his spouse as a personal injury lawyer would clearly contravene the hospital's policy and not be authorized under section 17 (2) the *Act* (among other provisions) - this does not appear to be in dispute.[18] However, what is in dispute is whether these disclosures actually took place in this case. In order to make a finding on whether the disclosures took place, it would likely be necessary for me (or an IPC adjudicator) to communicate directly with these two other individuals and would further likely involve an assessment of the credibility and reliability of the evidence of the patient, these other individuals, and the physician.

[104] As part of my investigation, and in addition to discussions with the patient, I contacted these other two individuals who had similar experiences. Unfortunately, despite some initial contact, they did not respond to later attempts to become involved in my investigation. While the previous accounts from these two other individual's would certainly cast doubt on the physician's representations that the presence of his

---

[18] I note that the physician indicated that "at no time did I benefit financially in any way from this initiative.
Quite the opposite, I was essentially doing additional work, free of charge, purely for the purpose of ensuring that patients who had visited the Hospital were receiving appropriate follow-up care as needed." I read this statement in light of the physician's broader denial that he referred individuals contacted as part of the quality audit to his wife in her capacity as personal injury lawyer. I do not read this statement to suggest that, if such a disclosure were made, it would not result in a conflict of interest.

wife at the clinic attended by the patient was coincidental, these individuals did not participate further in this investigation and did not respond to further communications from the IPC.

[105] In my view, on the facts of this case it would not be proper to determine whether this disclosure took place and potentially make findings of credibility and reliability in the context of this investigation (which was largely conducted in writing) without greater participation of these two other individuals.[19]

[106] In light of the above, I am unable to determine whether the physician disclosed personal health information in contravention of the *Act*. [20]

Issue 3: Did the hospital take reasonable steps to protect personal health information?

Administrative Measures and Safeguards

[107] In this case, I have found that that, as part of the quality audit, the physician accessed the personal health information of patients, without their consent and that this use was contrary to the *Act*.

[108] The facts of this case, and in particular the lack of clarity and training around the process the physician would have had to take to have his quality audit approved, also raised concerns about the administrative measures and safeguards taken by the hospital to protect personal health information.

[109] Section 12(1) of the *Act*, requires that health information custodians take "reasonable" steps to protect personal health information against theft, loss and unauthorized use and disclosure, among other things. Specifically, section 12(1) of the *Act* states:

> 12. (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

[110] In Order HO-010, the IPC stated that measures or safeguards must be reviewed

---

[19] I recognize that I could compel these individuals to give evidence, but I do not think it would be appropriate to do so on the facts of this case given their apparent unwillingness to participate further in this investigation, and in consideration of the steps that have been taken by the hospital to address the issue of quality audits at the hospital going forward.

[20] Of course, I also have not made any findings on the physician's wife's or clinic's conduct in relation to the above facts.

from time to time to ensure that they continue to be "reasonable in the circumstances" in order to protect personal health information from theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal.

[111] As part of my investigation, I reviewed the hospital's policies, practices and procedures regarding quality audits (and related training and communication of the policies, practices and procedures). The hospital also provided me with training material, communications to staff, and other relevant documents. The information provided included what was in force at the time of the second round of calls, as well as updated/current material.

Policies

[112] At the time of the breach, the hospital had a "Research Compliance, QA-QC Program Policy", however that policy only applied to the quality assurance of Research Ethics Board applications. The hospital confirmed that it did not have a formal quality audit policy that would apply to the type of quality audit at issue in this matter. The hospital also advised that guidelines for a Medical Quality Audit are/were noted in the Medical Staff bylaws provided to physicians at the hospital. As previously indicated, the hospital advised that it had a formal process that must be followed to conduct such an audit. The process required approval from either a Research Ethics Board or from the Medical Quality Assurance Committee, which must first be approved by the Chief of the Program.

[113] In response to questions I posed about quality audits, the hospital explained that agents of the hospital (including physicians), are made aware of the quality audit process as follows:

> …agents are made aware of the quality audit process by the Chief. Once an audit is identified, the Chief works with Health Information Services, who would then provide the data required for the audit. Chiefs work with their department members in conducting Medical QA Audits, or Chiefs undertake the audits themselves. It is important to note that the Medical QA Committee has had a process in place for several years, which requires Chiefs to submit QA audits each year. The expectation is that departments will undertake at least one QA audit annually. Chiefs identify audits through their department meetings. However, [the physician] did not follow this process.

[114] I note from my review of the information provided by the hospital, which included the texts and emails exchanged between the doctors, that there was a lack of clarity on what was, and was not, required to conduct a quality audit such as the one described in this matter. The hospital did not have any privacy training related to quality audits, nor did it have a dedicated quality audit policy for this type of quality audit at the time of the breach. It also did not have documented steps that staff could reference to determine how to seek approval. The guidelines for a Medical Quality Audit

which the hospital indicated are included in the medical staff bylaw 17-32.16, quoted above, is a high level, brief half page document that in my view does not provide sufficient detail regarding the approval process.

[115] The hospital also provided me with a copy of a new policy entitled "Performing Quality Audits" which was created in response to this breach. I have reviewed this policy and am generally satisfied that it adequately sets out the purpose of the policy, the process for submitting and receiving approval, as well as other relevant information that is helpful for staff to understand exactly what is expected and necessary for these types of audits, including who needs to approve them and how.

[116] For example, the policy states the following:

> An audit is a systematic, independent and documented process for obtaining data and evaluating it objectively to determine the extent to which audit criteria are fulfilled. All quality audits must have a purpose and a clearly outlined protocol that details how and why the data will be collected, data analysis, and data feedback. Audits must have the potential to lead to meaningful and worthwhile change; and where change is not the outcome, they must provide assurance that the current [hospital] practices are appropriate. Audits for improved performance looks for opportunities for preventative action and best practices that could be applied to other areas.

[117] The policy also sets out a number of principles that must be adhered to by all auditors in order to ensure that the internal quality audit process provides useful outcomes based on evidence. Some relevant key principles in the policy include:

- Ethical conduct through the demonstration of integrity, confidentiality and discretion;
- Fair presentation through the obligations to report truthfully and accurately;
- The auditor must be independent of the activity being audited and free from bias and conflict of interest;
- Audit evidence-based approach must be verifiable;
- Searching is limited to within the hospital's system;
- A list of patients will be provided to the auditor to search with the hospital's system.

[118] The policy also indicates that additional searching for patients that are not on the list would be considered a privacy breach, subject to disciplinary action and reporting to the relevant college.

[119] This policy is made available on the hospital's intranet and, as discussed

immediately below, is part of the Medical Affairs onboarding process and annual privacy training for physicians.

Training

[120] According to the information provided by the hospital, at the time of the quality audit at issue in this case the hospital was conducting one-time privacy training orientations for new staff (excluding physicians), which included a privacy presentation. In addition, on an annual basis all agents of the hospital (other than physicians), were expected to complete a module on Confidentiality and Privacy.

[121] With respect to physician's privacy training, the hospital explained that as part of their Application process for appointment to the medical staff, physicians sign a Confidentiality Agreement, which includes a Declaration on the Application form. They also sign an annual Declaration during their Application for Reappointment. This was the extent of what the hospital provided physicians in relation to what they described as privacy training at the time of the quality audit. [21] As mentioned earlier in this Decision, the hospital provided this office with page four of the physician's Declaration which included his signature.

[122] It is important to note that the training provided by the hospital at the time of the breach did not include training related to quality audits, which is central to the circumstances surrounding the unauthorized accesses in this matter.

[123] In response to the breach the hospital made a number of changes and explained that:

- the Medical Affairs onboarding process now includes providing new credentialed staff members (physicians) with information about key policies, including the Performing Quality Audits policy which requires the auditor be free from bias and conflict of interest.

- policy orientations are also provided by Departments and Programs;

- the Performing Quality Audits policy, like all the other hospital policies is on-line in the Policy and Procedure repository on the hospital's intranet;

- physician orientation involves signing a declaration that they understand and will comply with hospital processes and policies; and

[21] In addition to the above, the hospital also had a Privacy Advisory notice that required hospital staff to agree to when signing into any hospital computer as well as a screensaver regarding privacy which appears on every screen when it is inactive for a certain amount of time.

- new physicians also must complete a privacy e-learning module as part of the on-boarding process.

[124] In addition to the above, the hospital took the following steps:

- created/updated a number of policies relating to research and medical quality audits;
- started sending periodic reminders to all staff and physicians about privacy and the appropriateness of accessing patient records;
- quarterly audits to identify inappropriate access; and
- mandatory annual privacy training for all physicians and staff.

[125] The hospital also provided me with copies of various training materials, including one step-by-step guidance document related to conducting quality audits.

Analysis

[126] I was originally concerned with the adequacy of the hospital's policies, practices and procedures based on the facts of this case. There was a lack of clarity regarding quality audits at the time of the breach. The hospital policies (and in particular the above-noted bylaw) were vague and did not set out any clear process for how quality audits were to be initiated and approved. Further, the hospital did not have any training with respect to quality audits (and did not have mandatory privacy training for physicians at all). The general declarations and agreements signed by physicians at the time are important, but are no substitute for an effective training program that actually explains the hospital's privacy and security policies, practices and procedures. I agree with the comments of former Commissioner Brian Beamish in IPC Order HO-013, when he held that:

> Comprehensive and frequent privacy training is essential to the development and maintenance of a culture of privacy within any organization. It is even more essential in an organization with custody or control of sensitive personal health information that is made widely available through electronic information systems.[22]

[127] In my view the hospital's previously vague policies, practices and procedures regarding quality audits, and the complete lack of privacy training for physicians, did not amount to taking reasonable steps to protect the personal health information within the meaning of section 12(1) of the *Act*. However, I also find that the hospital has since remedied these issues.

---

[22] HO-013, p. 36

Issue 4: Should this matter proceed to adjudication at the IPC, where a potential order may be issued*?*

[128] The issue as to whether this matter should proceed to adjudication is twofold. First, with respect to the physician, I must consider if it is necessary to move this matter along to a stage where a potential order could be made to address the unauthorized uses of personal health information I have found in relation to the quality audit. My investigation also raised questions with respect to whether the physician disclosed personal health information to his wife in contravention of the *Act*.

[129] In my view, there does not seem to be any purpose in making an order specifically with respect to the uses of personal health information in relation to the quality audit. This audit was discontinued long ago and it does not appear likely that it will occur again.[23] Therefore, issuing an order to cease the practice at this stage would seem to be moot and not necessary to advance the purposes of the *Act*.

[130] With respect to the potential unauthorized disclosures, in order to answer this question it would likely be necessary to obtain evidence from the above noted witnesses identified in the OPP's investigation and make findings of credibility and reliability. However, as indicated above, the witnesses have not responded to my most recent attempts to have them participate in this process and I have no reason to think these witnesses would have any more willingness to voluntarily participate in the IPC's process if this matter were transferred to adjudication. As previously indicated, I recognize that I could compel these individuals to give evidence, but I do not think it would be appropriate to do so on the facts of this case given their apparent unwillingness to participate further in this investigation, and in consideration of the steps that have been taken by the hospital to address the issue of quality audits at the hospital going forward (discussed in the next paragraph). In the circumstances of this case, insisting on pursuing this matter with unwilling witnesses would serve no useful purpose and therefore, I do not believe moving this particular issue to adjudication is warranted.

[131] Secondly, with respect to the hospital, another issue raised by these facts is whether the hospital took reasonable steps in the circumstances to protect the personal health information from unauthorized uses, such as this quality audit, among other things. I have found that it did not take such reasonable steps contrary to section 12(1) of the *Act*. However, after considering the steps taken in response to this breach, I am satisfied that the hospital has since addressed this issue by creating a quality audit policy, and implementing, among other things, mandatory annual privacy training for all

[23] The records related to the second round of calls were provided to the hospital. However, the physician obtained copies in order to respond to this investigation, subject to the previously mentioned undertaking relating to materials obtained from the OPP. Among other things, the undertaking requires the return or secure disposal of the disclosed information and all copies made, within 30 days after the date the IPC's review, and any related appeals or judicial reviews, are concluded by the physician.

staff and physicians, which includes a component related to quality audits. As such, I again do not believe transferring this matter to adjudication is warranted.

[132] In accordance with my delegated authority under the *Act*, and for the reasons set out above, this review will be concluded without proceeding to the adjudication stage and without an order being issued by the IPC.

POSTSCRIPT:

While this file will not be proceeding in regards to the particular concerns about the physician and the hospital's quality audit policies and training, the information gathered raises questions about the potential for inappropriate use of MVA patients' personal health information. Hospitals, as well as other health information custodians, should be aware of the monetary value of these patients' personal health information and the related financial incentives that increase the risk of inappropriate disclosure. Accordingly, custodians should specifically turn their minds to, and carefully guard against, these risks when taking reasonable steps in the circumstances to protect personal health information in their custody or control against theft, loss and unauthorized use and disclosure.

Original signed by: June 18, 2021

Lucy Costa
Manager of Investigations