Information and Privacy Commissioner,
Ontario, Canada

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

# PHIPA DECISION 144

Complaint HC17-13 and HC18-60

The Ottawa Hospital

April 20, 2021

**Summary:** This decision finds that The Ottawa Hospital failed to take reasonable steps to implement the complainant's lock-box request from October 2016 to June 2019 and, as a result, certain hospital caregivers used the complainant's personal health information without consent or other authority. Other allegations of unauthorized use are dismissed. With the introduction of a new electronic medical records system in June 2019, the hospital remedied the deficiencies in its procedures for implementation of consent directives. The adjudicator makes one recommendation, to improve the directions given to users of the hospital's electronic medical records. The adjudicator dismisses allegations that unauthorized uses were deliberate and malicious violations of the complainant's privacy, concluding that they resulted from systemic failures in the hospital's practices.

**Statutes Considered:** *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3; sections 10, 12, 19, 29, 30(2), 37(1)(c), 37(1)(d), 43(1)(b), Ontario Regulation 329/04, section 6.2(1).

**Decisions Considered:** PHIPA Decision 35

**Cases Considered:** *Starson v. Swayze*, 2003 SCC 32 (CanLII), [2003] 1 SCR 722

## INTRODUCTION:

[1] In these complaints, a patient of the Ottawa Hospital (the hospital) alleges that the hospital has contravened the *Personal Health Information Protection Act, 2004* (the *Act*) by failing to implement her request for a "lock-box" on her records of personal health information (or "PHI"), and that agents of the hospital have used and disclosed

this information without authority under the *Act*.

[2] As the two complaints deal with overlapping facts and issues, I have combined them for the purposes of a review under the *Act*. During my review, I invited the hospital and complainant to submit written representations on the facts and issues raised by these complaints. Both have had the opportunity to review and respond to the submissions of the other, except to the extent described below.

[3] In this decision, I find that the hospital contravened the *Act* when it failed to take reasonable steps to implement the complainant's lock-box request, or her "consent directives", on the use of her personal health information.[1] As a result, hospital caregivers continued to use her PHI without authority, despite those restrictions. I find that the hospital has remedied the deficiencies in its procedures for implementation of consent directives but I make one recommendation to improve the directions given to users of its electronic medical records.

[4] I dismiss the complainant's allegations that the hospital's health care providers or other staff used her personal health information deliberately and maliciously, for their own purposes, and unrelated to their duties. Although I find that in some instances hospital caregivers accessed her information contrary to the lock-box request, those actions are more attributable to failures by the hospital to adequately inform its agents of the request and its impact, than a failure on the part of those caregivers.

## PRELIMINARY MATTERS

[5] There is no dispute in this complaint that the operator of the hospital is a "health information custodian" within the meaning of the *Act*. The complainant has been and is a patient of the hospital, and the personal health information at issue in these complaints is within the custody or control of the hospital.

[6] There is also no dispute that the complainant's allegations relate to uses or disclosures of her personal health information by individuals who are "agents" of the hospital as defined in section 2, including health care providers.

## LOCK-BOX

[7] Section 29 of the *Act* requires that a custodian have a patient's consent to the collection, use or disclosure of their personal health information, unless the *Act* permits

---

[1] The hospital uses the terms "consent directive" and "lock box" interchangeably and I have adopted its usage in this decision. I am not deciding how consent directives operate under Part V.1 of the *Act*, which came into force after the relevant times covered in this decision.

such actions to be taken without consent.

[8] The term "lock box" is not defined in the *Act*. It is a term commonly used to describe the right of individuals to withhold or withdraw their consent to the collection, use or disclosure of their personal health information for health care purposes and to provide express instructions to custodians not to use or disclose their personal health information for health care purposes without consent. This right is delineated by sections 19, 20(2), 37(1)(a), 38(1)(a) and 50(1)(e) of the *Act*. Notably, section 19 of the *Act* states:

1. If an individual consents to have a health information custodian collect, use or disclose personal health information about the individual, the individual may withdraw the consent, whether the consent is express or implied, by providing notice to the health information custodian, but the withdrawal of the consent shall not have retroactive effect.

2. If an individual places a condition on his or her consent to have a health information custodian collect, use or disclose personal health information about the individual, the condition is not effective to the extent that it purports to prohibit or restrict any recording of personal health information by a health information custodian that is required by law or by established standards of professional practice or institutional practice.

[9] The importance of a lock-box often arises in the context of the assumed implied consent (or "circle of care") provisions of the *Act*. Adjudicator Ryu explained these provisions in PHIPA Decision 35[2] as follows:

> [23] The term "circle of care" is not defined in the Act. It has been used to describe the provisions of the Act that enable certain health information custodians to assume an individual's implied consent. Section 20(2) of the Act specifies when implied consent may be assumed:
>
> > A health information custodian described in paragraph 1, 2, 3 or 4 of the definition of "health information custodian" in subsection 3 (1), that receives personal health information about an individual from the individual, the individual's substitute decision-maker or another health information custodian for the purpose of providing health care or assisting in the provision of health care to the individual, is entitled to assume that it has the individual's implied consent to collect, use or disclose the information for the purposes of providing health care or assisting in providing health care to the individual, unless the

[2] 2016 CanLII 85807 (ON IPC)

> custodian that receives the information is aware that the individual has expressly withheld or withdrawn the consent.
>
> [24] In order to rely on assumed implied consent to collect, use or disclose personal health information, therefore, the following conditions must be met:
>
> - the health information custodian must fall within a particular category of health information custodians; and
>
> - the health information custodian must receive the personal health information from the individual to whom the information relates, or that individual's substitute decision-maker or another health information custodian; and
>
> - the health information custodian must receive that information for the purpose of providing health care or assisting in the provision of health care to the individual; and
>
> - the purpose of the health information custodian's collection, use or disclosure of that information must be for the purposes of providing health care or assisting in providing health care to the individual; and
>
> - in the context of a disclosure, the disclosure of personal health information by the health information custodian must be to another health information custodian;[3] and
>
> - the health information custodian that receives the information must not be aware that the individual to whom the personal health information relates has expressly withheld or withdrawn the consent.
>
> [Footnote in original, but renumbered]

[10] As the last bullet in the above list indicates, custodians can only rely upon assumed implied consent where the custodian is not aware that the individual has expressly withheld or withdrawn consent.[4] A withdrawal of consent, or a refusal to give consent, however, does not prevent a custodian from collecting, using or disclosing information where it is otherwise permitted or required under the *Act*.[5] For example,

---

[3] *Act*, section 18(3).

[4] Of course, more broadly a withholding or withdrawal of consent also means that a given collection, use or disclosure of personal health information is not authorized by an express or implied consent.

[5] Unless the authority to use or disclose the information without consent under the *Act* is subject to a requirement that the individual must not have expressly instructed otherwise, and the individual has given such an instruction.

consent of a patient is not required when a custodian uses PHI for risk management purposes (s. 37(1)(d)) or for research (s. 37(1)(j)). Further, a previous withdrawal or withholding of consent does not prevent a custodian from obtaining a new valid consent under section 18 of the *Act* permitting the collection, use or disclosure at issue.

[11] Also relevant to the lock-box is section 37(1)(a), under which a patient's express instruction prevents a custodian from using information it otherwise may use without consent:[6]

> 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;

[12] It is important to note that the right to withhold or withdraw consent or provide express instructions not to use personal health information can take various forms. An individual may instruct that a particular part of their record of PHI not be used or disclosed by their health care providers without their express consent. They may instruct that their entire record not be used or disclosed without that consent. Or, they may wish that specific health care providers not be given access to their record (see the IPC's Lock-Box Fact Sheet, July 2005).[7]

[13] In the *Guide to the Ontario Personal Health Information Protection Act*, the authors observe that "the expression 'lock box' does not appear in PHIPA and is prone to misinterpretation, particularly since it suggests a control more absolute than PHIPA actually provides."[8] As described above, the lock-box right is a right to withhold or withdraw consent or give express instructions relating to the collection, use or disclosure of personal health information. However, it does not give individuals complete control over their personal health information.

[14] The *Act* requires, generally, that health information custodians must take reasonable steps to protect PHI from theft, loss and unauthorized use or disclosure (s. 12) and must "have in place information practices that comply with the requirements of this Act and its regulations" (s. 10(1)). "Information practices" is defined in the *Act* to

---

[6] For disclosure authorities subject to contrary express instructions, see ss. 38(1)(a) and 50(1)(e).
[7] Information and Privacy Commissioner of Ontario. (July 2005). Lock-box Fact Sheet. No. 8. Retrieved from https://www.ipc.on.ca/wp-content/uploads/resources/fact-08-e.pdf
[8] Halyna Perun, Michael Orr and Fannie Dimitriadis, *Guide to the Ontario Personal Health Information Protection Act* (Irwin Law: Toronto, 2005), p. 284.

mean "the policy of the custodian for actions in relation to personal health information, including… administrative, technical and physical safeguards and practices…"

[15] The *Act* does not set out what steps a custodian must take to implement a lock-box request. The IPC has noted (see the IPC's Lock-Box Fact Sheet) that compliance with the lock-box provisions of the *Act* may be achieved by health information custodians through a variety of means, which could include:

- policies, procedures or manual processes;
- electronic or technological means; or
- a combination of policies, procedures or manual processes and technological means;

depending on the avenue chosen by the health information custodian.

[16] Reading together all of these provisions, the hospital and its agents have an obligation to not collect, use or disclose the complainant's personal health information contrary to the complainant's lock-box, without other authority under the *Act*. In implementing this obligation, the hospital must take steps that are reasonable in the circumstances.

## BACKGROUND

[17] It is not in dispute that, in August 2013, the complainant contacted the hospital's Privacy Officer by telephone, seeking restrictions on the use of her records by hospital caregivers. The details of this conversation are not entirely clear. The complainant states that she had not heard of the term "lock-box" at this time, but she told the Privacy Officer she sought to have records relating to mental health treatment earlier in that year to be "made inaccessible to anyone." Handwritten notes of the Privacy Officer from this time confirm that the hospital was aware that the complainant wished to withdraw consent to the use of her personal health information. The notes do not provide more detail about the scope of the request, and do not refer to mental health records. They indicate that the Privacy Officer agreed to provide the complainant with the hospital's lock-box request form.

[18] The letter to the complainant from the hospital's Privacy Officer following this conversation explained that, while the hospital was not capable of "locking" her electronic health record (EHR), it could add a "warning flag" and contact her treating physicians to notify them of her withdrawal of consent. The Privacy Officer also provided the complainant with the hospital's lock-box request form. This form states, among other things, that the hospital is "currently capable of locking the paper health records and is not capable of locking the electronic health record." The implementation of the lock-box for paper records is not at issue in this complaint.

[19] Despite the statement that the hospital was "not capable of locking the electronic health record", the hospital's Patient Privacy Policy states that patients are entitled to withdraw consent to the use and disclosure of personal health information stored in the hospital's electronic health record system, by applying a consent directive. Further, the hospital has a Corporate Standard Operating Procedure governing consent directives, which sets out the procedures for implementing a directive. That Procedure states, among other things, that a request to apply a consent directive to the electronic health record must be made through completion of the lock-box request form.

[20] From the above, I infer that the statement by the Privacy Officer and on the form, that the hospital was "not capable of locking" the electronic health record, was not meant to suggest that the hospital could not implement a patient's consent directive with respect to electronic records. Rather, it was meant to convey that it could not apply a technological barrier against access to that record.

[21] While the hospital agrees that the complainant made a verbal request which it interpreted as a lock-box request, it states that it sought a clear direction from her as to the restrictions sought and, pending that direction, placed a "privacy warning flag" on her EHR. Following the conversation between the complainant and the Privacy Officer, the hospital placed a warning flag on the complainant's EHR, which stated:

> *You are attempting to access personal health information which has been deemed highly sensitive by TOH Chief Privacy Officer. Please ensure you have patient consent or are part of the patients circle of care prior to proceeding.*
>
> *All access beyond the Flag is closely monitored by the Privacy Office for potential violations of patient privacy. The monitor will only be triggered if you proceed beyond this point.*
>
> *Do you wish to continue? YES or NO*

[22] The complainant did not return the lock-box request form at this time. Several years passed and, in 2016, she contacted the hospital again, at which time she requested and received an audit of her electronic health record. Through the results of this audit, the complainant discovered that agents of the hospital providing care to her had accessed her mental health records, despite her belief that she had withdrawn her consent to the use of those records.

[23] On October 6, 2016, the hospital received a completed lock-box form from the complainant. This form stated that the complainant wished to place conditions on any further use or disclosure of her PHI by the hospital and "any doctor/health practitioner. "The date range specified for her direction is "from beginning to present and future." The complainant completed the form stating that the direction applied to her entire health record, and to her entire health care team. The complainant also sent a letter on November 29, 2016 in which she repeated her withdrawal of consent.

[24] As before, the form also contained the statement: "The Ottawa Hospital is currently capable of locking the paper health record and is not capable of locking the electronic health record." Following the hospital's receipt of the form, the above-noted warning flag remained on her EHR. I have no evidence about any other steps taken by the hospital to implement the complainant's directions.

[25] The complainant filed a complaint with the IPC in February 2017, which became file HC17-13. In the complaint, she alleges, among other things, that hospital agents had accessed her mental health records despite her effort to lock those records in 2013, and that the hospital did not have the capability to implement her direction.

[26] In June of 2017, the hospital implemented a new flag (which it calls the "consent directive flag") on the complainant's EHR, which stated:

> *Please ensure that any access beyond this flag is with* ***explicit patient or substitute decision maker consent*** *to do so or is for a specific authorized purpose.* [emphasis in original]

[27] The technical restrictions were the same for both the warning flag and the consent directive flag. The flags appeared as warnings and if users selected "yes" to continue, they could access the complainant's personal health information in the EHR.

[28] In August of 2018, the hospital became aware of a gap in the implementation of this consent directive flag. The flag appeared when a user searched for records by the patient's name or medical record number. However, it did not appear if a user accessed a patient's electronic health record through a roster list of patients. At the time, the hospital explained that this was a deficiency which would be addressed by its new electronic medical record, EPIC, which it anticipated implementing in June 2019.

[29] On January 17, 2019, the hospital implemented a newly worded consent directive flag. The new flag stated:

> The patient has directed The Ottawa Hospital to only allow access to their personal health information with their express consent. Please ensure that any access beyond this flag is with express consent by the patient or substitute decision maker, or is for a purpose authorized without consent, which would only apply in narrow and specific circumstances (e.g. error or risk management, a risk of serious bodily harm to any person, billing, etc.). Please document the consent and/or the specific authorized purpose in the patient's record. If you need further clarification, contact the Information and Privacy Office (IPO) before proceeding.
>
> Any access beyond this flag is closely monitored by the IPO for potential violations of patient privacy.
>
> Do you wish to proceed? YES or NO.

[30] On June 1, 2019, the hospital implemented the EPIC system, which replaced its previous electronic medical record. This system also introduced a new tool to enable implementation of consent directives, which the hospital has called "Break the Glass." I will describe this tool in more detail below.

**The complaints to the IPC**

[31] As indicated above, the complainant filed her first complaint with the IPC in February 2017, which was assigned to an analyst to attempt informal resolution. She filed a second complaint in June of 2018, which became HC18-60. The files were assigned to a mediator to explore resolution and gather additional facts. Despite many discussions and communications between the mediator and the parties, no resolution was possible and the complaints were referred to adjudication. On June 10, 2019, I began my review of the complaints by issuing a Notice of Review.

[32] The complainant and the hospital have made submissions and been given the opportunity to respond to each other's submissions, except as described below. Before I set those out, I will address certain issues arising out of the complainant's submissions.

[33] The complainant provided submissions in response to those of the hospital on August, 29, 2019, and supplemented those with numerous additional submissions. I have before me correspondence from the complainant dated September 11, September 18, October 2, October 25, November 4, November 28, December 10, December 17, 2019, January 6, January 17, June 22, and October 28, 2020 (the last being submissions in response to the hospital's Supplementary Representations). In her submissions, the complainant raises numerous issues beyond those covered in the Notice of Review, including allegations against legal counsel for the hospital, additional allegations of unauthorized accesses to her health records, additional allegations of violations of section 30(2) of the *Act*, allegations of falsehoods by hospital staff, unauthorized modification of a health record, denial of access rights, cover-up of wrongdoing, and inadequacies in the EPIC system.

[34] I have reviewed and considered all of the complainant's submissions but do not address in this decision every issue she has raised. I have not expanded the scope of my review to consider certain additional issues raised by the complainant where I find no reasonable purpose or reasonable grounds to do so, the issues are not within the scope of my authority, or were raised at a late stage of the process. I also do not address issues which the complainant has raised in other complaints to this office.

[35] To be clear, I find no useful purpose in reviewing whether the hospital's previous electronic medical record system was deficient, as alleged by the complainant, because it did not log when users printed copies of records. Below, I conclude that there were shortcomings in the hospital's previous processes for implementing consent directives, which it has remedied. I find that a consideration of this particular issue is unnecessary, as any finding on it would not lead to any remedy. Further, there is no evidence that any agent accessing the complainant's records ever made printed copies of them.

[36] The complainant alleges that the hospital has violated section 11 by failing to ensure her records are up-to-date. The facts she relies on relate to her assertion that hospital caregivers used records that were not reasonably necessary to her current health care. I find section 11 inapplicable to these facts, which are more appropriately considered under section 30, below.

[37] In her submissions, the complainant also alleges that the hospital's legal counsel is in violation of section 70 of the *Act*, by interfering with her medical care, and engaging in bullying and unlawful harassment. She submits that the hospital unlawfully disclosed her health information to this counsel, and that he unlawfully collected it. I will not address these allegations as the complainant has raised those in another complaint to this office. However, to the extent this correspondence is relevant to some of the issues in this complaint, I refer to it below.

[38] Beyond the lock-box issues, the complainant has raised a number of allegations with respect to a particular consultation with a rehabilitation consultant. Those allegations form part of another file before this office, HA19-00091, and I will not deal with them here.

[39] The complainant also submits that the hospital's privacy officer has attempted to mislead the IPC through the hospital's submissions, provided falsehoods, and engaged in personally insulting attacks on the complainant's character. I find no reasonable basis for these allegations. I find no evidence of attempts to deceive the IPC. Nor do I construe anything in the hospital's submissions to constitute personally insulting attacks on the complainant's character. The complainant also submits, without evidence, that the hospital has contravened section 70, prohibiting retaliation, for which I find no basis.

[40] The complainant has submitted that it is unfair to ask her whether the changes implemented through the hospital's new electronic medical record have addressed the issues raised by her complaints. She states that this seems like a "trick question" in that it is a complicated and technical matter, in addition to which the hospital has refused to answer certain questions she has put to it about this system on the basis that her letter is "harassing and vexatious." She states that she cannot be expected to make comments on the additional capabilities of the new system when neither she nor the adjudicator know what they are. She also submits that the new system is irrelevant to the issues raised in her complaint.

[41] I find no unfairness in asking the complainant to address the adequacy of the hospital's new means of implementing consent directives. She has made thorough and knowledgeable submissions regarding the deficiencies in the hospital's processes, and been provided with the hospital's submissions regarding its past and current processes. As to the relevance of the current processes, the adequacies of the new system are relevant to any potential orders that I may make, if I uphold portions of these complaints.

**Representations**

[42] The hospital submits that it applied a reasonable lock-box at the earliest possible opportunity. It states that, on August 16, 2013, pending receipt of clear directions from the complainant as to the conditions she wished to place on access to her records, the hospital placed a privacy warning flag on the complainant's EHR, based on her oral request. It also provided her with the lock-box request form to complete.

[43] The hospital stated that it made clear to the complainant that it was not capable of "locking" the EHR, except through the addition of a warning flag. It submits that this is consistent with its obligations under the *Act*.

[44] The hospital states that the *Act* does not permit, much less require, health information custodians to implement complete locks on records of personal health information pursuant to a patient's consent directive. It submits that although the *Act* allows an individual to withdraw their consent to the collection, use or disclosure of PHI for the purposes of providing health care, this withdrawal of consent is not unlimited. One limitation is found in section 19(2), which allows agents to comply with legislative or professional obligations to record, for example, assessments of a patient's condition, despite a consent directive. The *Act* also specifies circumstances where collection, use and disclosure of a patient's personal health information is permitted despite a consent directive, such as for risk management.

[45] Although the hospital asserts that it implemented a reasonable lock-box at the earliest opportunity, it states that the consent directive functionality within the new EPIC system ("Break the Glass") is "even better". Its submissions with respect to the new system will be outlined in more detail below.

[46] In her submissions, the complainant disputes the hospital's contention that it implemented a "reasonable consent directive." Among other things, she submits that any system that allows access to records under a consent directive – unless consent is not required – does not comply with sections 10 and 20(2) of the *Act*.

[47] The complainant submits that the hospital has failed to ensure that its agents are appropriately informed of their duties under the *Act*. She relies on the intent of the legislators for support of her claim that her consent directives are absolute rights guaranteed under the *Act* and not to be considered as optional according to a custodian. She submits that the *Act* requires more than the taking of some ineffective steps that do not ensure the inaccessibility of health records that a patient does not want used. Any steps that do not result in preventing access do not comply with the intentions of the legislators.

[48] The complainant submits that staff do not understand the meaning of section 30 of the *Act* (discussed below). She submits that the hospital's privacy officers do not have the medical training to understand when review of records is necessary for particular care, that the current privacy officer is misguided as to how section 30 applies

to the reality of clinical practice in hospitals and is in turn providing bad guidance to health professionals.

[49] She also states that it is "obvious considering the amount of unlawful and unacknowledged accesses" to her personal health information that the rules in the *Act* are misunderstood or that the hospital holds them in "arrogant disregard." She submits it is obvious that privacy education is lacking or insufficient at the hospital. The complainant submits that the hospital's account of its security measure reads well but in reality "its staff access whatever patient records they want and nothing happens."

[50] The complainant states that the intent of the lock-box provision was to "absolutely prevent use, disclosure or collection for health care purposes by requiring those consent directed records to be rendered inaccessible for those purposes and not just flagged with a warning…"

[51] The complainant submits that the hospital is "in denial of all its privacy transgressions and inadequacies", has attempted to mislead the IPC, has not treated her with integrity and, through its counsel, is now threatening her. She states that the hospital's agents have acted wilfully and are unrepentant for their unlawful actions.

[52] She states that she has the right to require that each and every record that a hospital agent accesses has her explicit and written consent.

## Did the hospital adequately implement the complainant's lock-box requests?

[53] I will consider the complaints in two parts. The first considers whether the hospital took reasonable steps between August 16, 2013 and June 2019 to implement the complainant's lock-box requests. This part also considers the complainant's allegations of widespread unauthorized accesses to her PHI during this period by the hospital's agents. The second part considers whether the hospital's new processes, introduced with its adoption of the EPIC system in June 2019, meet its obligations under the *Act* to take reasonable steps in the circumstances to implement the complainant's lock-box request.

### *August 2013 to June 2019*

*Did the complainant make an effective lock-box request in August 2013?*

[54] In determining whether the hospital complied with its obligation to implement the complainant's consent directive, I must decide what she asked for, and when. There is no dispute that the complainant had a conversation with the hospital's Privacy Officer in August 2013, in which she indicated her wish to withdraw consent to the use of her personal health information. The complainant and the hospital differ in their accounts of this conversation. The complainant views this conversation to be an unequivocal withdrawal of consent to the use of her mental health records, triggering the hospital's obligation to take steps to ensure that its agents cease using those records for the

purpose of her health care. In her view, any use of this information by hospital caregivers following the date of this conversation was thus unauthorized.

[55] However, it appears that the hospital did not view this conversation the same way. Although it recognized that the complainant was seeking a lock-box, it asked the complainant to complete a written lock-box request form to provide it with clear direction on the nature and scope of her request. Pending receipt of this form, it placed a warning flag on the complainant's EHR.

[56] I pause to note here that nothing in the *Act* prevents a health information custodian from acting on an oral withdrawal of consent. Despite its policy requiring that consent directives be in writing, the hospital's submissions do not suggest that it would not have given effect to a clear oral consent directive from the complainant. In this case, however, it appears that the hospital requested that the complainant complete its lock- box request form in order to ensure clarity about her directions, and did not treat the conversation as amounting to withdrawal of consent. The complainant did not return the form, and did not communicate further with the hospital about her lock-box request, until October 2016.

[57] Thus, although the complainant believed that the conversation of August 2013 was sufficient to communicate the terms of her consent directive, the hospital had a different understanding. Given the differences in their accounts, I prefer to rely on the documentary evidence as an indication of the intent of the parties at the time of this conversation. Based on that, I am unable to find that the conversation of August 2013 amounted to a consent directive to which the hospital was required to give effect.

[58] As described above, with the submission of the written lock-box request form in October 2016, the complainant gave the hospital the clear direction it was waiting for. Upon receipt of this direction, the hospital had an obligation to implement the complainant's lock-box request. Despite this, the original "warning flag" on the complainant's EHR remained in place, until June 2017.

[59] I have no information about what, if any, other direction the hospital gave to the complainant's health care providers following her lock-box request in October 2016, and I infer that the warning flag was the primary means by which the terms of her lock-box request was communicated to the hospital's agents. Unfortunately, this "warning flag" was not adequate to ensure compliance with the lock-box request, and with the *Act*. As set out above, the flag told users that they were attempting to access highly sensitive personal health information. It further told users to "ensure you have patient consent or are part of the patient's circle of care prior to proceeding." Thus, it explicitly invites health care providers in the complainant's circle of care, who normally rely on assumed implied consent to provide health care to her, to continue doing so when the complainant's request was precisely that they stop doing that. In giving incorrect information to caregivers about their obligations under the *Act*, the flag was not a reasonable measure to implement the complainant's lock-box request.

[60] I acknowledge that in another decision under the *Act*, HO-002 this office found that a similar flag employed by this hospital was part of a good privacy protection program. However, the circumstances of that case related to measures taken to prevent deliberate snooping by a nurse, the girlfriend of the patient's estranged husband. It did not involve the implementation of a lock-box request.

[61] In June 2017, this flag was replaced by one requesting users to "ensure that any access beyond this flag is with **explicit patient or substitute decision maker consent** to do so or is for a specific authorized purpose." [emphasis in original]

[62] The hospital described this flag as a "consent directive flag". However, as the vehicle to implement a consent directive, it was also insufficient. The flag did not alert users to the existence of a consent directive on the specific patient's health record. Hospital caregivers acting in the course of their normal duties could reasonably assume they were accessing records for an "authorized purpose." Caregivers who routinely provide health care assuming the implied consent of their patients to the use of their personal health information would likely not, on the basis of this flag alone, question whether they may continue to proceed as before.

[63] It is also worth noting that the flag was not implemented for more than half a year after the complainant submitted the lock-box request form. Further, as I describe above, the flag did not appear on a patient's record when the record was accessed from a roster of patients. It only appeared when patient's records were searched by medical record number or name. Thus, following the implementation of this new flag, at least one agent of the hospital accessed the complainant's records through a roster list for the purpose of providing health care, without being prompted to obtain her consent. The hospital was not aware of this gap until the complainant raised questions about certain accesses shown on audit reports, and it investigated her complaints about those accesses.

[64] In view of the inadequate language of the consent directive flag and the hospital's delay in discovering its limited coverage, I find that during this time, the hospital failed in its duty to take reasonable steps to implement the complainant's consent directive. As stated above, the hospital did not provide information about any other steps taken to implement the directive.

[65] Also as stated above, the hospital further amended the flag in January 2019 to be more specific and detailed. I find the wording of this third flag (set out above at para. 29) adequately communicated to users the effect of a lock-box request, in that it explained that accesses to the patient's EHR required express consent or were for purposes authorized without consent, and explained the meaning and provided examples of such authorized purposes. However, until the hospital implemented the new EHR in June 2019, the deficiency with respect to the incomplete coverage of the flag to patients on a roster persisted. I will discus the new EHR in more detail below.

### *Allegations of unauthorized uses or disclosures between August 2013 and October 2016*

[66] Apart from the above, I have also considered the complainant's allegation that, during a consultation with a psychiatrist in August 2016, she withdrew consent for that psychiatrist to use her 2013 mental health records for the purpose of providing her with care. I have reviewed the evidence in support of this allegation, consisting of part of the psychiatrist's clinical note of the consultation. The complainant redacted all of the note apart from two lines. I do not place much weight on two disconnected lines taken out of context from the rest of the document, and in themselves, I find that these lines do not establish a withdrawal of consent.

[67] It follows from my finding above that between August 2013 and October 2016, there was no consent directive in place. This disposes of the allegations that agents of the hospital who were collecting, using or disclosing the complainant's health information for the purpose of providing health care or assisting in providing health care to her during the period from August 2013 to October 2016, were not authorized to do so on the basis of assumed implied consent.

### *Allegations of unauthorized uses or disclosures after October 2016*

[68] As described above, in October 2016, the complainant submitted a written lock-box request form. Through this form, the complainant withdrew consent to further use or disclosure of any of her records of personal health information. Also as described above, the hospital's procedures for ensuring compliance with this direction remained flawed. Even after the hospital replaced the first warning flag, the new "consent directive flag" gave unclear direction, and did not appear when users accessed records through a roster list of patients.

[69] As a result, caregivers providing health care to the complainant accessed her health records without her consent, following October 2016. The hospital does not assert that these uses were permitted without consent. I find the failure to respect the complainant's lock-box request was attributable to a systemic failure to put in place reasonable measures to implement consent directives. Whether the complainant's EHR showed the first flag (which was in place until June 2017), or the hospital's "consent directive flag" which followed it, I have found that neither gave clear direction to the hospital's caregivers about the implications of her consent directive. Given this general finding, it is unnecessary for me to review each of these allegations individually.

[70] In these circumstances, it does not appear that the hospital's agents knew that, in providing health care to the complainant, they could not rely upon her assumed implied consent to perform tasks such as reviewing her records in preparation for consultations. While such a review was unauthorized due to the withdrawal of consent, I have no reason to conclude, as submitted by the complainant, that they were knowing and wilful violations of her privacy. Rather, as I state above, I find it more likely they were the result of the systemic failures in the hospital's processes for implementing

consent directives.

**Limitation principle**

[71] Having made the above findings, it is not strictly necessary to consider other arguments made by the complainant in support of her contention that uses of her records were unauthorized under the *Act*. However, in view of the ongoing issues between the complainant and the hospital, and her continuing relationship with hospital caregivers, I will provide my comments on some of these additional arguments.

[72] In addition to her contention that the hospital's agents unlawfully used her health information, contrary to her consent directive, the complainant also asserts that many of these accesses involved uses of her information beyond what was reasonably necessary to provide her with health care.

[73] Section 30(2) of the *Act* sets out a "limitation principle" on the collection, use or disclosure of personal health information:

> A health information custodian shall not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure, as the case may be.

[74] In this case, the complainant questions, for instance, whether accesses to her mental health records were reasonably necessary to an assessment of her need for rehabilitation following a physical injury, or as part of a social work assessment during discharge planning. She argues that mental health records cannot lawfully be used for medical care apart from mental health care.

[75] The complainant asserts that, because none of the agents named in her complaints were providing psychiatric care[9], and were not even licensed to do so, accesses to psychiatric records that were years out-of-date could not have been "reasonably necessary" for the purpose of treatment of her physical health (which included breast cancer surgery, radiation, bone density management, and a fractured pelvic bone). She also submits that none of the caregivers accessing those records included the contents of the mental health records in their medical reports, and this demonstrates that those records could not have been necessary to the care they provided. In the case of one caregiver, she states that it is a "classic case of snooping since no information was entered from the records accessed to prove they were necessary for the care."

[76] The complainant submits that other hospital caregivers involved with her care did

---

[9] This is taken from the complainant's submission but I note that one of the hospital's agents named in her complaints and involved in her care was a psychiatrist.

not use her mental health records, thus proving her contention that they were unnecessary to her care in these instances. In short, the complainant submits that no reasonable person would conclude that the provision of health care by these providers would require review of psychiatric records. The complainant submits that "necessary means necessary", and these caregivers were snooping into her records.

[77] The hospital provided evidence from some of its agents explaining their rationale for reviewing the records at issue. One physician, a radiation oncologist, stated that a patient's physical, psychological and emotional well-being are integral parts of a treatment plan, and that she would be negligent in her role as physician if she did not take all of these aspects into account. Another physician, involved in an assessment for osteoporosis, states that such an assessment includes a review of medication, and that some commonly used in psychiatry can cause bone loss. Thus, as an endocrinologist, she would look at psychiatric records in a patient's EHR for such information.

[78] The rehabilitation consultant documents on a form that she reviewed the complainant's records related to cancer treatment and psychiatric care, in arriving at an informed decision about her ability to participate in a structured rehabilitation program following her fracture.

[79] In general, the hospital states that when physicians and staff assess any new patient, they review previous dictations, consultations, imaging and pathology reports. The hospital refers to the World Health Organization's definition of health as "a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity." It states that to satisfy their professional obligations, its staff are required to review all relevant information for patients who are referred to them, and that a patient's physical, psychological and emotional well-being are an integral part of a treatment plan.

[80] I find no violation of section 30(2) in the circumstances of this case. The requirement in section 30(2) is based on "reasonable" necessity, which is a more expansive concept than the complainant's formulation of "necessary means necessary".

[81] The agents who reviewed the complainant's mental health records were involved in the provision of health care to her and were reviewing her medical history in preparation for consultations with her. I find convincing the explanations from the hospital about the health care rationale for review of the complainant's medical history for the purpose of those consultations including, in some instances, her mental health records. The age of the mental health records does not point to indiscriminate browsing through irrelevant and outdated records, as the complainant suggests. None of these records was created more than four years before these events.

[82] One of the allegations in file HC17-13 concerns review of the complainant's breast imaging records, not her mental health records, by an endocrinologist in 2015. In this instance, the complainant alleges that this specialist had no valid reason to review breast imaging records for the purpose of bone density health care. The

complainant provided no basis for her allegation and without any evidence to suggest that care provided to her for a previous issue could not reasonably have implications in relation to other health issues, I would not uphold such an assertion. In this case, in any event, the hospital explained the physician's rationale for this review stating, among other things, that hormonal therapies used to treat breast cancer have significant effects on bone density so a diagnosis of breast cancer often alters decision-making in terms of treatment for bone health. For the same reasons as above, I find no violation of section 30(2).

[83] Although the complainant asserts that mental health records can only be reasonably necessary to mental health care and not other medical care, there is no evidence to support this assertion. While the complainant strongly disagrees with the hospital's submission that the uses of her mental records were "reasonably necessary" to provide health care to her, I find no persuasive evidence to support her allegation that these uses were unauthorized under section 30(2). Her views, vehement as they are, are not reasonably supported or convincing in the face of the hospital's submissions on this point.

[84] In arriving at these findings I do not mean to suggest that caregivers have unlimited scope to use a patient's health records in providing them with care. In this case, the complainant has made broad and unsupported assertions that what is reasonably necessary to provide health care is limited only to information about the specific medical issue which is the subject of a health care consultation, which I do not find to be reasonable or factually supported.

### *Allegation that some health care providers were not in the circle of care*

[85] I have also considered the complainant's submission that some agents who accessed her records were not providing health care to her at the time of their actions, and for that reason, regardless of any consent directive, their actions were not authorized because they could not have relied on assumed implied consent. In one instance, the hospital states that a caregiver reviewed the complainant's records, including her mental health records, in anticipation of providing care to the complainant. However, the complainant did not ultimately meet with this caregiver. In the circumstances described, I am satisfied that the review of these records, but for the consent directive, would be authorized as a use for the purpose of providing health care.

[86] In another instance, the complainant alleges that an access to her records (in this case, not her mental health records) a month after a consultation was not within the circle of care. She alleges that she ceased to be a patient of the physician in question on the date of that consultation (in June 2016). The hospital made unsuccessful efforts to contact this physician, who had retired by the time this allegation was brought to its attention. In the circumstances, and in light of my above finding in relation to the hospital's broader failures to implement the complainant's consent directive during the period of time during which this access occurred, I decline

to make any findings on this specific instance.

### *Other allegations of unauthorized uses or disclosures*

[87] One of the complainant's allegations relates to a social work consultation in June 2017.

[88] As background, I found above that, following the complainant's submission of a written lock-box request in October 2016, caregivers providing health care to the complainant accessed her health records without her consent. I also found it unnecessary to review the allegations against each of these caregivers individually, as I found the failure to respect the complainant's lock-box request was attributable to a systemic failure to put in place reasonable measures to implement consent directives.

[89] As describe above, both the first flag, which was in place until June 2017 and the hospital's "consent directive flag" which followed it had deficiencies, in that neither gave clear direction to the hospital's caregivers about the implications of her consent directive.

[90] In the circumstances, I had no reason to conclude, as submitted by the complainant, that they were knowing and wilful violations of her privacy. Rather, I find it more likely they were the result of the systemic failures in the hospital's processes for implementing consent directives.

[91] In the case of the consultation with a social worker in 2017, and regardless of the above background, the complainant alleges that she gave oral instructions to the social worker with respect to the use of her personal health information, which instructions were violated. The evidence in support of her assertion is the social worker's report of the consultation which states that the complainant gave the social worker "permission to look up information on OACIS[10] which pertains to her current admission." The complainant also relies on audit reports showing accesses to her records by this social worker on June 23 and 26, 2017, the latter being the date of the consultation.

[92] The complainant alleges that before and after the consultation on June 26, 2017, the social worker reviewed a social work assessment from 2016 and a psychiatric record from 2013, in violation of her consent directive. She alleges that the social worker knowingly and wilfully disrespected the complainant and her privacy, and betrayed her trust. The hospital's position is that accesses to the complainant's records by this social worker were with her consent, referring to the documentation of consent in the report.

[93] As above, I find that accesses to the complainant's records before the

[10] OACIS refers to the electronic health records system used by the hospital at this time.

consultation of June 26, 2017 were not authorized, as the complainant had withdrawn consent to such accesses by her written lock-box request of October 2016. However, as before, I find the failure to respect the complainant's lock-box request was attributable to a systemic failure to put in place reasonable measures to implement consent directives, and not to any deliberate or wilful violation of the complainant's health privacy. I have no evidence as to which of the two flags discussed, the first warning flag or the consent directive flag, was in place at this time but, in any event, I have found both to be deficient. In addition, I have no evidence as to whether the social worker accessed the complainant's records prior to the consultation through a roster list (in which case no flag appeared). In these circumstances, I find that a caregiver such as the social worker could reasonably assume that she could rely on assumed implied consent to perform tasks such as reviewing the complainant's records in preparation for a consultation.

[94] In arriving at this conclusion, I reject the complainant's submission that the social worker's report shows that the social worker knew that she did not have permission to review the complainant's records before the meeting. The part of the report the complainant refers to does not provide a basis for any inferences about the social worker's knowledge or statement of mind before the meeting.

[95] I turn now to the allegation that the social worker accessed the complainant's records following the meeting, contrary to an explicit oral consent directive given during the meeting. For the reasons below, I do not uphold this allegation.

[96] The evidence to support this allegation is limited. I have referred to the statement in the report that the complainant gave the social worker permission to review information "which pertains to her current admission." I also have before me an audit report which appears to show accesses to 2016 social work records and a 2013 psychiatric note, on the date of the consultation. I have no evidence as to the time of the meeting, from either the complainant or the hospital. The complainant alleges that these accesses occurred after the meeting. In the following discussion I will assume, without finding, this was the case.

[97] The complainant alleges that the 2016 social work records and 2013 psychiatric note did not "pertain to her current admission." In her view, the phrase "current admission" refers only to those records generated during the period of June 20-29, 2017, when she was admitted to the hospital because of a fractured pelvis.

[98] The report states that the social worker explained her role. The social worker explained that an assessment would help in determining the complainant's home situation. It notes that the complainant had "limited supports and lives alone." The report also states that the complainant expressed worries about her ability to manage at home.

[99] The phrase "pertain to her current admission" is ambiguous. It could be understood to mean, as the complainant alleges, that the social worker was given

consent to only review information relating to the complainant's pelvic fracture and associated treatment. Or, it could be understood as consent to review records reasonably necessary for the purposes of providing discharge planning as part of health care needs following the complainant's treatment for the pelvic fracture.

[100] In the whole context, I find that the social worker might have reasonably understood that a previous social work assessment and records relating to the complainant's mental health "pertained" to her "current admission." These records could be viewed as relevant to planning to meet the complainant's needs following her discharge from the hospital. Certainly, it would be reasonable to view social work records arising out of a similar assessment in 2016 to be relevant to the social worker's assessment in 2017. I also find that a mental health record from 2013 could reasonably relate to an assessment of the complainant's ability to manage on her own following her discharge for a significant injury, a question which the complainant raised with the social worker.

[101] In sum, I find that the direction given by the complainant during the consultation of June 26, 2017 authorized a review of records relevant to discharge planning arising out of the complainant's admission to hospital on that occasion, which could reasonably encompass social work records from 2016 and a mental record from 2013. In the circumstances, I dismiss the allegation that such a review following the consultation (assuming it occurred following the consultation) was not authorized.

[102] Further, I have no reason to view these actions as deliberate and wilful violations of the complainant's privacy, as alleged by the complainant. In this respect, I note that despite the complainant's lengthy medical history with this hospital, the only records the social worker reviewed for the purpose of this consultation were those related to previous social work involvement and a psychiatry clinical note.

[103] Two of the complainant's allegations are about the hospital's disclosure to other parties. One concerned the disclosure of the complainant's information to the College of Physicians and Surgeons of Ontario (the "CPSO"). The hospital states that it received a request from the CPSO for certain records for the purposes of an investigation initiated by a complaint from the complainant regarding her care and treatment. The CPSO provided the hospital with a consent signed by the complainant specifying that only certain records created in 2016 could be released. The hospital states that it disclosed only records covered by that consent and there is no evidence to suggest otherwise. As the disclosure was with the complainant's express consent, I find it was authorized under the *Act*.

[104] Even without consent, section 43(1)(b) permits disclosure of personal health information to this type of college for the purpose of investigations under the *Regulated*

*Health Professions Act. 1991*.

[105] Another allegation in complaint HC17-13 concerns the hospital's provision to eHealth Ontario of her consent directive information.[11] The complainant alleges that this is a disclosure done without her consent, in violation of her rights under the *Act*.

[106] The hospital acknowledges that it sent eHealth Ontario the complainant's consent directive, and indicates that this was done in keeping with its obligation to "convey any known restrictions on access to a patient's phi prior to the flow of that phi from the hospital to eHealth Ontario for purposes of the Clinical Viewer and other eHealth Ontario electronic health record systems."

[107] At the time of these events, section 6.2(1) of Ontario Regulation 329/04, made under the *Act*, stated that the provision of personal health information from a health information custodian to eHealth Ontario is not considered a disclosure, in specified circumstances:

> Where a health information custodian provides personal health information to eHealth Ontario for the purpose of eHealth Ontario creating or maintaining one or more electronic health records, and eHealth Ontario satisfies the requirements listed in subsection (2),
>
> > (a) the health information custodian shall not be considered in so providing the personal health information to be making it available or to be releasing it to eHealth Ontario for the purposes of those expressions as used in the definition of "disclose" in section 2 of the Act;[12]
> >
> > …

[108] Subsection (2), referred to in the above, set out the requirements eHealth must follow in creating or maintaining electronic health records. The hospital states that it sent information about the complainant's consent directive to eHealth Ontario as part of a bulk upload of patients' directives.

[109] The complainant has provided no evidence to establish that the hospital violated the *Act* in providing eHealth Ontario with her consent directive. In her submissions, she questions whether this action was lawful, and submits that such a disclosure is not required by law and her explicit wishes should have been taken into account by the

---

[11] eHealth is now part of Ontario Health.

[12] Since the time of these events, this regulation has been revoked, and a new Part V.1 to PHIPA enacted to create a privacy framework for the provincial electronic health record. Compliance with Part V.1 and its regulations is not atissue in these complaints.

hospital. I find no merit in this submission. The provision of this information to eHealth is not considered a "disclosure" for the purposes of the *Act* in the circumstances described in section 6.2(1) and I see no basis to view it as a contravention of the *Act*. Indeed the provision of this information to eHealth was for the purpose of protecting the complainant's privacy in relation to her health information.

[110] The complainant submits that there is no evidence that eHealth has satisfied the requirements of subsection 6.2(2) of the Regulation and questions whether a finding about whether the provision of her consent directive information to eHealth can be made without such evidence. I also find no merit in this submission. The complainant has offered no basis to question compliance with the Regulation by eHealth. Without any grounds to believe it has not complied, I have no reason to engage in a review of eHealth's information practices.

[111] I therefore dismiss the allegation that the provision of the complainant's consent directive to eHealth contravened the *Act*.

[112] Some of the accesses covered by the complainant's allegations were not for the purpose of providing health care. The complainant alleges that accesses by members of the hospital's Health Records Department violated the *Act*. The hospital provided her with an explanation of those accesses in a letter to her in September 2018, after she questioned them. It stated that one access was made in order to fulfill a request from the complainant for copies of her health records. Another was made to verify that the complainant's request had been fulfilled after the complainant raised a question with staff in that Department about the adequacy of the release of records to her. Based on the hospital's explanations, which are not contradicted, I am satisfied that these accesses were permitted without consent under section 37(1)(c) of the *Act* (permitting uses "for planning or delivering programs or services"). They are uses made in the provision of services arising out of the complainant's request for access to her health records.

[113] The complainant also complains about an access by a member of the hospital's Patient Relations staff during this period. The hospital states that this individual accessed the complainant's Discharge Summary to investigate the complainant's contention (made during a phone call) that she was being released from the hospital too soon. The complainant agrees that she discussed this matter with this individual but still maintains that the access was unlawful, in that there is no proof of a written complaint file.

[114] I accept the hospital's submission that access to the complainant's Discharge Summary for the purpose of reviewing the complainant's expressed concerns was permitted under section 37(1)(d) of the *Act*, which permits uses without consent for the purposes of risk management or error management. The absence of a formal complaint file does not cast doubt on the hospital's account of this conversation, nor does it mean these uses were not authorized for those purposes.

[115] In general, the complainant has described the actions of the hospital's agents as wilful, deliberate, unprofessional uses of her information, which they did knowingly and expecting to go undetected, and which the hospital went to lengths to conceal. I have no reason to view any of the accesses as deliberate "snooping" events, as the complainant alleges. The hospital's agents were either involved in providing health care to the complainant or acting in the course of their duties with the hospital. While some of the accesses to the complainant's EHR by these agents were contrary to the complainant's consent directive, and were not based on a provision of the *Act* permitting access without consent, they were not the result of any wilful, deliberate act. Rather, these actions are attributable to a systemic failure by the hospital to take steps that were reasonable in the circumstances to implement the consent directive by communicating the restrictions placed by the complainant.

**Does the hospital's current process for implementing the lock-box comply with the *Act*?**

[116] There remains the question of whether the current process by which the hospital implements consent directives is a reasonable measure to implement the lock-box.

[117] A key component of this current process is a privacy tool contained in the hospital's new EPIC system, called "Break the Glass" (or BTG). According to the hospital, this tool starts with a window which appears when staff attempt to access a record. The tool can be applied at the request of the patient to records arising out of a single encounter, in relation to a specific user, or to the entire EHR for that patient.

[118] The hospital provided a screen shot of the window and message that appears when staff attempt to access the complainant's file. The new wording is similar to that set out above from the January 17, 2019 consent directive flag. It states:

> The patient has directed one or more of the Atlas Alliance hospitals to only allow access to their personal health information with their express consent. Please ensure that any access beyond this flag is with express consent by the patient or substitute decision maker, or is for a purpose authorized without consent, which would only apply in narrow and specific circumstances (e.g. error or risk management; a risk of serious bodily harm to any person; billing; etc.). Before you click Accept, please document the consent or the specific authorized purpose by clicking on one of the Reasons, by typing in the Further explanation box, and by typing your password. If you need further clarification, click Cancel and contact the privacy office at an Atlas Alliance hospital before proceeding.

[119] A second box states:

> You need to Break-the-Glass for the following reasons. Any access beyond this flag is closely monitored by a privacy office at an Atlas Alliance hospital for potential violations of patient privacy. Do you wish to proceed:

[120] The messages provides a list of 9 reasons to choose from:

- Billing
- Direct patient care
- IT Team/Tech
- Research
- Unspecified
- Coding Review
- Incident Investigation
- Quality Review
- Scheduling

[121] The message provides spaces to request help, as well as to provide a further explanation for the access. It is mandatory to select a reason, as well as to input a password. The user may then click "accept" or "cancel".

[122] The hospital states that each time a user proceeds past this warning screen, and even if they see the warning screen and do not access the record, such actions are recorded and the log data monitored by the hospital's privacy office.

[123] The hospital states that it published an article in its newsletters of June 13 and 20, 2019, describing this new consent directive privacy tool, which it provided with its submissions. Among other things, this article states:

> What should staff do when they encounter a Break-the-Glass pop-up?
>
> • Ask for the patient's consent, then, in the "**Further explanation**" box, document whether the consent was verbal or written, and whether it was given by the patient or their substitute-decision maker.
>
> • Select the appropriate **Reason** (e.g. direct patient care, scheduling, etc.).
>
> • Enter password.
>
> • Click "**Accept**".
>
> Only specific situations (i.e. error or risk management, a risk of serious bodily harm to any person, billing, etc.) allow for access without patient consent.

[124] The hospital also states it is revising its operating procedure for Consent Directives accordingly.

[125] In this case, the complainant submits that the hospital's process for implementing the lock-box is deficient because it permits a user to access records to which the lock- box relates, as long as the user claims that the patient has given consent. In her submission, the tool is "not designed to prevent users from accessing individual patient records without consent when a consent directive is in place", because "patient records in the EPIC system are not locked."

[126] With respect to the hospital's auditing practices, the complainant submits that retroactive identification of unauthorized use does not provide what the *Act* requires to respect consent directives. She states that "only EHR systems that prevent access to records to which directives apply without authorization or lawful purpose do that". She submits that audits can be fabricated and questionable accesses can be removed and, therefore, audits and post-access monitoring do not provide her lock-box privacy rights.

[127] The complainant asserts that the hospital "cannot monitor the hundreds of patient record accesses that are performed daily at the hospital and for them to claim they will is deception." She submits that the bottom line is that this new system is "not designed to prevent users from accessing individual patient records without consent when a consent directive is in place." She states that patient records are not locked and that a user can access any of them unlawfully after gaining entry. She submits that the legislators did not contemplate halfway measures like the EPIC system.

[128] The hospital submits that the *Act* does not permit, much less require, health information custodians to implement "complete locks" on personal health information pursuant to a patient's consent directive. Its "Break the Glass" tool complies with the *Act*. The hospital states that the purpose of the *Act* is to create rules for the collection, use and disclosure of health information about an individual, while facilitating and balancing the effective provision of health care to those individuals. It submits that its privacy tool strikes that balance, and that completely eliminating the ability of an agent to gain access to an individual's medical record is neither technically possible nor legally required. In the hospital's submission, it would impair the ability of medical and nursing staff to provide either emergent or timely medical care to an individual in need, or who wished to modify or remove their consent directive.

[129] After providing her initial submissions in these complaints, the complainant sent numerous additional letters, in which she enclosed copies of audit reports from the hospital showing activity by hospital agents during the period June 1, 2019 to September 19, 2019. She provided these audit reports as evidence to support her position that the new consent directive tool does not provide the lock-box as intended by the *Act*, and is not a reasonable implementation of her consent directive.

[130] The complainant submits that the audit reports show that half of the health care providers involved in her care accessed her records without her consent despite the

new "Break the Glass" tool. These individuals include nurses and physicians in the emergency department, admitting and other clerks, and others.

[131] In a further submission, the complainant submits that the hospital's auditing capabilities are deficient and, because of this, the hospital would be unable to determine whether or not an access by a user was in accordance with a consent directive. She also states that the hospital has advised her that once a user gains access to a patient's records through the "Break the Glass" tool, they are permitted access for up to seven days without having to complete the information in the tool again. She submits that this is a failure to ensure effective implementation and monitoring of consent directives.

[132] I invited the hospital to respond to some of the new evidence, as well as certain other submissions from the complainant. I did not seek its response on other submissions that came at a late stage. As described earlier, the complainant made multiple submissions and even when only invited to respond to the hospital's submissions, added new allegations.

[133] The hospital disputes the complainant's assertions that the audit reports are evidence of unauthorized accesses by the hospital's agents. Among other things, the hospital refers to an event during which the complainant was brought to the hospital's emergency department by paramedics. The audit report records access to the complainant's EHR by the triage nurse who assessed the complainant. The hospital submits that the complainant was present in the hospital, seeking care, and providing her personal health information to this nurse. In the hospital's submission, relying on section 19(2), the nurse had a legal and professional obligation to record the findings of this assessment in the EHR.

[134] The hospital makes the same submission with respect to individuals performing diagnostic imaging and testing who recorded information in the complainant's EHR.

[135] Generally, in the hospital's submission, the audit report records events on dates in which the complainant agreed to receive medical care. It submits that her consent to obtain care must be interpreted as a modification or suspension of the previously issued consent directive as care cannot be provided without the collection and use of personal health information. It submits that the complainant cannot expect that a health care provider who has collected information directly from her will subsequently conclude that they have no right to use the information obtained to provide treatment. This, in the hospital's submission, would put the hospital and its agents in an untenable if not absurd position.

[136] With respect to its auditing capabilities, the hospital submits that EPIC, the EHR used by the Hospital, has a sophisticated audit logging system, allowing it to identify each screen accessed by an individual logged into a patient's chart. The audit log records all accesses, views, changes, coding, and background system processes, assigning a code to each field, page, or encounter accessed by a user. In total, there

are over 3,000 different event-logging codes that identify the specific action and part of the record accessed by a user.

[137] The hospital states that these audit logs enable it to investigate user access, identify what health information was accessed and used and allow it to determine whether these accesses and uses were authorized. It states that the complainant's assertions regarding the functionality of the EPIC audit logs are inaccurate and based on incomplete information.

[138] The hospital submits that it configured the BTG warning to be consistent with the objectives of *PHIPA*: to strike the appropriate balance between ensuring patients receive timely and effective care from health professionals, with a patient's consent directive to restrict access to their health information. In this context, it states, the goal of the BTG warning is to prevent users from accidentally looking at or clicking into a record that they did not intend to access, and to deter users from accessing records out of curiosity. The hospital submits that its staff are trained about the requirement to obtain express patient consent before accessing a file when a BTG warning appears.

[139] The hospital did not dispute the complainant's contention that users who gain access to a patient's records through the BTG tool are given access for seven days without repeating that process. It states that the seven-day period was expressly selected because it approximates the average length of stay for a patient admitted to the hospital. The seven-day period ensures that patients are not required to provide their consent each time the EHR or encounter needs to be accessed during their stay. It allows care providers to more efficiently provide care to the patient during that patient's episode of care.

[140] The hospital clarifies that where a user accesses a specific encounter that is subject to a lock-box, such as where it was accessed to provide care to a patient with their consent, that particular user will not be asked to "break the glass" again to access that specific encounter for seven days. The user, however, would be presented with a BTG warning if they attempted to access a different protected encounter.

[141] Further, it states that a patient who provides consent to a user to break the glass to provide them with care is responsible for advising the user if they intend to provide only a limited consent. For example, it states, the patient must inform the user if the consent given is limited to viewing only a particular portion of the EHR or to only a particular record and only on that one occasion, even if the user will continue to provide care to the patient.

[142] The hospital also states that, in contrast to situations in which a patient provided consent to receive care, users engaged in administrative tasks such as coding or billing, which do not require a patient's consent, are presented with the BTG each time they seek to access either a protected encounter or protected patient record. These users must provide the reason why they accessed the patient's record.

[143] The hospital also states that each time a user accesses records beyond the BTG, such actions are recorded, and log data are monitored and audited by its privacy office on a daily basis. Individuals who have inappropriately indicated that they require access to provide care will not have continued access for the seven-day period.

[144] In sum, the hospital submits that its approach to implementation of lock-box requests is thoughtful, evidence-based and reasonably balances a patient's privacy rights with the hospital's mission of providing health care.

[145] In her last set of submissions, the complainant submitted additional audit reports and raised additional issues. She alleges that when she gave consent to hospital agents to access her records for a specific purpose (in one example, to a booking clerk to make a booking), the consent was not effective since she was unaware of the seven-day extension of access. She states that she was deceived by the hospital when she gave consent in July and August 2019 for a single specific purpose, without being advised that her consent would be valid for that user for seven days.

[146] The complainant submits that the BTG instructions indicate that access can be gained with consent or an authorized purpose and provides some examples of such purposes. She states that a user could be confused by this instruction and consider providing patient care or scheduling, for examples, as circumstances that do not require consent and then go ahead with the access. She states that this may have been the case with some of the accesses shown in the audit reports, which she submits are unauthorized. In the complainant's submission, a better way to avoid confusion and inadvertent access without consent is to prevent a user from proceeding beyond the prompts unless the response to the prompts permits use.

[147] The complainant also objected to the notion that custodians need to strike a "balance". She submits that the objective of the *Act* is to protect of the privacy of patients while they receive health care from health professionals. It provides custodians with rules that are immutable. In her submission, the right to withdraw consent is an absolute right, resulting in consultation for express consent for each and every use of records involved in a directive. The hospital, according to the complainant, has designed its new EPIC system to compromise the privacy and consent rights of its patients. Its very representations demonstrate its commitment to non-compliance with the lock-box provisions of the *Act*. The complainant states that "nothing is locked or blocked in the Epic EHR although patients might be given the false impression it is".

### ***Analysis***

[148] As the key element in its implementation of the lock-box, the hospital has chosen a "consent directive flag" that advises users seeking to access records that they must have either the express consent of the patient, or be acting for a purpose authorized without consent. The flag further requires the user to document the consent, the authorized purpose, and then enter their password. The flag can be applied to records relating to a single encounter (which was the complainant's original concern), a specific

user, or the entire record. In addition, users are told that accesses beyond the flag are monitored by the hospital's privacy office.

[149] I find that the hospital's "consent directive flag" is part of reasonable steps taken by the hospital to implement the complainant's consent directive. I take into consideration the flexibility of the flag, which enables the hospital to apply it to records of a specific visit, to specified users, or to a patient's entire EHR. I also take into consideration the elements that users have to complete and agree to before they can access information subject to the flag. The article which the hospital distributed with the introduction of the BTG provides clear guidance to the hospital's agents on the use of this privacy tool. It clearly tells staff that consent is required, and that only specific situations (giving, as examples, error or risk management, a risk of serious bodily harm to any person, or billing) allow for access without patient consent.

[150] I accept the hospital's evidence as to the rationale for the implementation of a seven-day "window" following consent to access a patient's records to which the BTG privacy tool has been applied. I find persuasive its submission that when patients are in the hospital or at an appointment, and have consented to access as part of receiving care from a caregiver, requiring that caregiver to "break the glass" each time they access the patient's chart or a particular encounter would unnecessarily delay care to a patient who has already consented to the use of their health information for this purpose. I find that this feature of BTG does not detract from the reasonableness of the steps the hospital has implemented to comply with lock-box requirements.

[151] I am, however, sympathetic to the complainant's submission that the BTG tool contains an ambiguity which could undermine its effectiveness. As set out above, the instructions to users are clear that either patient consent, or a specific authorized purpose for which consent is not required, is needed in order to access the record to which the BTG tool has been applied. It also reminds users that authorized purposes are narrowly prescribed. However, in prompting users to choose a reason for access, the BTG tool combines a list of purposes which require consent, with those which do not. Thus, "direct patient care" (which requires consent) is listed alongside "billing" (which does not require consent).

[152] The newsletter containing instructions to staff, which the hospital circulated when the BTG tool was introduced, was clear. However, the above potential ambiguity in the BTG tool itself may undercut the clarity of the hospital's message to its staff and lead to confusion. I will thus recommend that the hospital amend the BTG instructions to ensure that there is clarity about which listed reasons permit access to records without consent, and which require consent.

[153] I make no finding on the complainant's submission that the consent she gave during a time when "Break the Glass" was placed on her EHR, but she was unaware of the seven-day window, was ineffective because it was obtained by deception. As I have stated, this submission was made in her very last submission, to which I did not seek a further response from the hospital. Rather than prolonging my inquiry to address this as

a separate complaint of unauthorized uses, I found it appropriate instead to consider whether this practice is, in itself, reasonable.

[154] The logging and auditing of user accesses are also important components of the hospital's process for implementing consent directives. To the extent that users understand that their accesses will be logged, this promotes front-end compliance with their responsibilities. Further, the hospital can audit accesses and investigate as necessary to determine whether those accesses are authorized. As indicated above, the complainant alleged that these reports fail to identify the specific records accessed by a user and the hospital cannot, therefore, determine from its audit whether or not an access was in keeping with a consent directive. However, she has provided no basis to contradict the hospital's evidence that it logs each screen accessed by an individual logged into a patient's chart, and all accesses, views, changes, coding, and background system processes.

[155] In arriving at my conclusions, I have considered the complainant's submission that only a complete technological barrier against access to her records will suffice as a reasonable measure to ensure compliance with her consent directives. I agree with the hospital that the *Act* does not require it to ensure compliance with a patient's lock-box request through imposition of a technological barrier to access in its EHR. That is certainly one way to implement a lock-box but, as illustrated in the IPC's Lock-box Fact Sheet, there are many ways in which a lock-box can be achieved. Each of the various ways in which consent directives can be implemented has advantages and disadvantages. It is not hard to imagine some of the disadvantages of imposing a barrier against access in a hospital environment where efficient and timely access to information is imperative. Further, under section 12(1), the standard of compliance is not perfection, but whether the means chosen by the hospital are reasonable in the circumstances.

[156] I have also considered the complainant's description of the lock-box as an "absolute" right under the *Act*. As I state at the outset of this decision, it has been observed elsewhere that the term "lock-box" is prone to misinterpretation as it suggests a control more absolute than what the *Act* provides. Not only does the *Act* provide for circumstances in which health information can be used without consent, it also does not prescribe the means by which the lock-box must be implemented. Further, the obligation on the hospital to take "reasonable steps" to implement the lock-box does not require that it grant patients absolute control over the use of their information.

[157] As described above, the complainant asserted that the audit reports she received from the hospital demonstrate that the hospital's agents continue to access her records without her express consent or other authority.

[158] Considering the late stage at which these allegations arose, I did not ask the hospital to address individual accesses shown in the audits. The complainant continued to add additional allegations of unauthorized uses, including in her last submissions of October 28, 2020 in response to the hospital's supplementary submissions. Rather, I

requested that the hospital respond generally to the complainant's position that the audit logs provide evidence that the hospital's new privacy tool does not bring the hospital into compliance with the lock-box provisions of the *Act*.

[159] In those later submissions, the complainant pointed to instances such as review of her chart in preparation for an appointment, or for the purpose of scheduling an appointment, which she alleges occurred without (or before) she gave consent. As I indicated, the hospital was not asked to address each of these new allegations. However, even if I assume that certain hospital caregivers accessed the complainant's records without her prior consent for the purpose of providing health care, this does not detract from my general findings.

[160] I have found that overall, after June 2019, the hospital remedied the shortcomings in notifying its agents of the complainant's consent directive. As I state above, the requirement to take "reasonable steps" does not impose a standard of perfection. Despite the BTG tool, there may be times when the hospital's caregivers gain access to a patient's records without the required consent or other authorization. Even if this occurs (and results in an unauthorized access within the meaning of the *Act*), it does not, by itself mean that the hospital has failed in its responsibilities to take reasonable steps under section 12(1). The *Act* does not require it to provide absolute guarantees.

[161] I also provide the following comments on some of the issues the complainant has raised, for future guidance.

[162] Some of the allegations made in the complainant's submissions relate to occasions when she was receiving direct care from the hospital's agents, such as a time when she was brought to the emergency department by paramedics, or underwent diagnostic procedures. The hospital describes the example of a triage nurse who has an obligation to assess the complainant on her arrival in the emergency department. It submits that, under section 19(2), that nurse has a legal and professional obligation to record the findings of the assessment in the patient's EHR, and that the presence of the consent directive does not change that.

[163] I agree with the hospital's submission that on these occasions, the complainant's pre-existing consent directive cannot reasonably be understood to prohibit its agents from using the very personal health information provided by her in these circumstances, for the purpose of giving the very health care she seeks. It would lead to absurd results if lock-boxes operate to prevent those caregivers from dealing with information a patient is providing them in the context of a health care encounter. Recalling that one of the purposes of the *Act* is to establish rules for protecting the privacy of individuals in relation to personal health information *while facilitating the effective provision of health*

*care*[13], the lock-box provisions of the *Act* should not be read to require unworkable and contorted interactions between caregivers and patients during the provision of health care.

[164] Of course, depending on the circumstances, the collection, use or disclosure of a patient's information in a hospital context may also be authorized without consent under other parts of the *Act*.

**The complainant's right of autonomy**

[165] Despite my comments above, there is no doubt that the complainant's consent directive will have an impact on the authority of hospital agents to access her records at some point during their provision of care to her. It will require them to adapt their customary practices, in order to give effect to her directive. I have referred above to the requirement that hospital caregivers obtain consent from the complainant to review her records in advance of consultations, unless permitted under the *Act* to do so without consent.

[166] It is evident from the material before me that the complainant wishes to apply her lock-box rights to direct which records can be consulted by given hospital agents at each step of her health care. It is evident from her submissions that she has strong views as to the relevance of care provided for one health issue, to any other health issue.

[167] The impact of this approach is demonstrated in correspondence sent by the hospital's lawyer to the complainant in August 2019 (attached to the complainant's submissions). In the letter, the hospital's lawyer states that the complainant has refused consent to a step in the process of booking an MRI, which is a review of the referral by a radiologist for the purpose of determining what priority level should be assigned to the scheduling of the MRI appointment. The lawyer states that if this is the case, the hospital will not be able to schedule the appointment. The lawyer also advises the complainant that requiring that each agent obtain her express consent to access each and every record required for follow up, result, or consultation may result in delays, difficulties, and/or an inability to access and receive medical care at the hospital.

[168] The complainant characterizes this letter as threatening, intimidating, and believes it is "punishable under section 70".[14] As I read the letter, the hospital is expressing a concern, among other things, that the complainant's expansive and inflexible view of her consent directive rights may affect the provision of health care to her. It is not hard to imagine that the complainant's lock-box imposes an additional

---

[13] See section 1(a).

[14] Section 70 of the *Act* contains protection for whistleblowers, among others. As indicated above the complainant hasfiled a separate complaint regarding this matter. This complaint has been dismissed.

procedural step for the hospital in providing healthcare to her, and that the effect of this step is that her health care may be delayed in cases where the *Act* does not permit collections, uses and disclosures to occur without consent (and contrary to express instructions). I do not view the expression of that opinion to be threatening or intimidating.

[169] Another example illustrating the impact of the complainant's consent directive on her health care is found in the hospital's submissions. The hospital submitted a statement from a specialist describing his involvement with the complainant's health care. In this statement, this specialist refers to being unable to edit a clinic note in order to report to the complainant's family doctor, due to lack of permission to access the complainant's records.

[170] As demonstrated in this decision, the relationship between the complainant and the hospital has become strained. The complainant, as described above, is quick to ascribe malicious motives to many hospital caregivers. She calls, I have found unjustifiably, for their denunciation and prosecution. She also accuses the hospital's privacy officer of deception and cover-up. The hospital, for its part, has come to view the complainant as a vexatious litigant. It states that she has written over 50 letters of complaint to various hospital staff and departments, and made 9 overlapping complaints to the IPC. It states that in several of her complaints, she persists in raising new issues, resulting in delay. It appears that the hospital has discussed with its agents the importance of thoroughly documenting their every action in relation to the complainant's records, a step it does not take with all patients.

[171] In the hospital's last submission in these complaints, it states that the complainant's unfounded complaints and allegations over the years have resulted in a significant expenditure of time and resources and requests that I dismiss them in the exercise of my jurisdiction under section 57(4)(e). This section gives me authority to decline to review a complaint if I find it to be frivolous, vexatious or made in bad faith. It does not apply to the circumstances of this case. First, I made a determination to conduct a review and this decision represents my decision on the issues encompassed in that review. Second, having conducted my review, I have found merit in some of the complainant's allegations. In this sense, her complaints are neither frivolous nor vexatious. I also find they have not been made in bad faith. Bad faith generally implies some improper motive or ill-will.[15] I have no reason to believe that the complainant is motivated by bad faith in her dealings with the hospital.

[172] That is not to diminish the hospital's efforts to address her complaints, all the while continuing to provide health care to her. It does not underestimate the effort of

---

[15] See orders made by this office under the *Freedom of Information and Protection of Privacy Act* which interpret this phrase, such as Order M-850.

providing health care in the face of a consent directive which has been interpreted by a patient to provide a right to direct every flow of information pertaining to her care.

[173] Although the hospital describes the complainant as a vexatious litigant, it is also still providing health care to her and, in that capacity, implicit in some of its submissions may be an underlying concern that the complainant may be interfering with her care by adopting an expansive approach to her lock-box rights. Through the *Act*, the Legislature has granted patients the means to exercise their autonomy to make choices about the use of their personal health information by their caregivers. In exercising the right to withhold or revoke consent, a patient may at times act in a way that a caregiver believes is not in the patient's best interests. Apart from specific and narrow circumstances, the *Act* gives patients the right to make those decisions, and requires health information custodians to respect those choices.

[174] Similar principles, and tensions, exist when patients exercise their right to refuse unwanted treatment. In discussing the role of the Consent and Capacity Board under the *Health Care Consent Act, 1996* to determine whether a patient had the capacity to refuse unwanted treatment, the Supreme Court of Canada stated that

> "[t]he right to refuse unwanted medical treatment is fundamental to a person's dignity and autonomy. ….
>
> The legislative mandate of the Board is to adjudicate solely upon a patient's capacity. The Board's conception of the patient's best interests is irrelevant to that determination. As the reviewing judge observed, "[a] competent patient has the absolute entitlement to make decisions that any reasonable person would deem foolish" (para. 13). This point was aptly stated by Quinn J. in *Koch (Re)* (1997), 1997 CanLII 12138 (ON SC), 33 O.R. (3d) 485 (Gen. Div.), at p. 521:
>
> > The right knowingly to be foolish is not unimportant; the right to voluntarily assume risks is to be respected. The State has no business meddling with either. The dignity of the individual is at stake.
>
> In this case, the only issue before the Board was whether Professor Starson was capable of making a decision on the suggested medical treatment. The wisdom of his decision has no bearing on this determination.[16]

[175] Obviously, the entitlement to make decisions about treatment is more absolute (and any exceptions to it will generally have more significant consequences for an

---

[16] *Starson v. Swayze*, 2003 SCC 32 (CanLII), [2003] 1 SCR 722 at paras. 75-76

individual) than the entitlement to make decisions about one's own personal health information. However, I would note that both rights can involve the same tension between perceptions of an individual's best interests and the right to make capable choices. Similarly, while a hospital may question the wisdom of a patient's right to refuse or withhold consent to the use of their health records in the delivery of care to them, ultimately, it must, subject any exceptions in the *Act*, respect the patient's right to make that choice.

## RECOMMENDATION

1. For the foregoing reasons, I recommend that the hospital amend the direction in the "Break the Glass" tool so that it clearly distinguishes between those reasons for which consent of the individual is required, and those for which consent is not required.

Original Signed by: April 20, 2021

Sherry Liang
Assistant Commissioner