Information and Privacy Commissioner/ Ontario

ORDER HO-002

Ann Cavoukian, Ph.D.
Commissioner
July 2006

NATURE OF THE COMPLAINT:

The Office of the Information and Privacy Commissioner/Ontario (IPC) received a complaint under the *Personal Health Information Protection Act, 2004* (the *Act*) involving The Ottawa Hospital (the hospital) in Ottawa, Ontario.

The complainant, through her legal counsel, made a complaint to the IPC that during and after her treatment at the hospital as an in-patient, her personal health information was illegally accessed on ten known occasions, and some of that information was used and disclosed without her consent, and for an illegal purpose. For ease of reference, I will refer to communications and positions of the complainant's counsel as those of "the complainant."

According to the complainant, her personal health information had been accessed by a registered practical nurse (the nurse) employed at the hospital. This individual did not provide health care to the complainant at any time. The complainant also indicated that the nurse was her estranged husband's girlfriend. The estranged husband, with whom the complainant is involved in divorce proceedings, is also employed at the hospital in a capacity that has no direct involvement in providing health care. The complainant states that the nurse accessed her electronic health records, in an unauthorized manner, during and after the complainant's stay at the hospital, over a six week period.

In her complaint letter, the complainant explains that she had specifically raised her privacy concerns at the time of admission:

> … given that her estranged husband works at the [hospital] and that his girlfriend is a nurse at the same [h]ospital complex, [she] took measured steps to inform and caution the [hospital] about her concerns over her privacy on admission…. She explained to the attending medical staff the rationale for her concerns, in particular, that she and her estranged husband … were undergoing rancorous divorce proceedings and a custody battle for the children. Having made the [hospital] aware of her concerns, she expected that extra care would be taken to monitor access to her personal health information.

The complainant also states that she had advised staff in the emergency department, as well as in the hospital's Heart Institute, where she was later transferred, that she had a restraining order against her estranged husband.

Following her discharge from the hospital, the complainant became aware that there had been a potential breach of her privacy because her estranged husband had phoned her and, "…without prompting of any kind, raised the issue of her chronic heart condition in a manner which indicated he was aware of her current treatment." The complainant indicates that, at that point, she warned her ex-husband that she would make a complaint. She then contacted the privacy office at the hospital, by telephone, to lodge a complaint.

Upon receiving the complainant's call, the privacy office placed a "VIP flag" on the complainant's electronic health record that advised staff accessing her record that the patient's information

had been deemed highly sensitive by the Chief Privacy Officer. The VIP flag also indicates that any attempt to view highly sensitive patient information "is closely monitored for potential invasions of patient privacy." It then prompts the user to choose whether or not they still wish to view the record. As a result of the VIP flag, an audit report would automatically be sent to the Chief Privacy Officer each time the complainant's record was viewed. The Chief Privacy Officer also ordered an audit on the electronic health record. According to the investigation report completed by the hospital's Chief Privacy Officer, referred to in more detail below, the audit found that "… there was an individual who had accessed the file without cause or justification." The report confirms that the individual in question was the nurse.

Because the audit indicated that unauthorized access had occurred, the hospital's privacy office undertook an investigation to determine what had taken place. Once it concluded the investigation, the hospital issued a report on the matter to the complainant. The hospital also forwarded copies of the report to the College of Nurses of Ontario and the IPC. The report outlined the steps that the hospital took as part of its investigation and "confirmed that there was in fact a breach." The report also referred to the nurse's previously unblemished 24 years of service and the estranged husband's essentially clean record through 21 years of employment with the hospital. The report went on to indicate that an internal disciplinary action was taken with respect to both employees. The nurse was suspended without pay for four weeks and the estranged husband for ten days.

Upon reviewing the hospital's report, the complainant filed a complaint with the IPC. The IPC opened a complaint file and assigned the matter to a mediator in order to seek resolution of the matter. Staff from my office conducted the following interviews to obtain further information:

- the hospital's privacy office
- the hospital's labour relations officer
- the nurse
- the nurse's manager
- the estranged husband
- the estranged husband's manager
- the complainant and her counsel.

As the complaint was not resolved by way of mediation, it proceeded to the adjudication stage, in which I conducted a review under the *Act*. I wrote to the complainant and the hospital, outlining the factual background and the issues to be addressed in the complaint, and asked them to provide representations. In response, both the complainant and the hospital provided written representations.

ISSUES ARISING FROM THE REVIEW:

In this order, I will consider the following issues:

Is the information referred to in the complaint "personal health information"?

Is the hospital a "health information custodian"?

Was the nurse an "agent" of the hospital?

Was the complainant's personal health information "used" by the nurse, and was this use in accordance with the *Act*?

Was the complainant's personal health information "disclosed," and was this disclosure in accordance with the *Act*?

Did the hospital comply with section 12(1) of the *Act*?

PRELIMINARY MATTERS:

Section 7 provides that the *Act* applies to the collection, use or disclosure of personal health information by "health information custodians," or in some instances that are not applicable in this case, by persons who are not health information custodians. It is therefore necessary to determine whether the complainant's information qualifies as "personal health information," and whether the hospital is a "health information custodian," as those terms are defined in the *Act*.

In addition, the review canvassed the issue of whether the nurse was an "agent" of the hospital in relation to the circumstances of this complaint. Section 17(1) of the *Act* addresses the collection, use, disclosure, retention and disposal of personal health information by agents of a health information custodian. As a result, it is also necessary to determine whether the nurse was an "agent" as that term is defined in section 2 of the *Act*.

PERSONAL HEALTH INFORMATION

Personal health information is defined in section 4(1) of the *Act*, which reads in part as follows:

> 4(1) In this Act,
>
> "personal health information", subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information,
>
> (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,

(b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual, …

Section 4(2) of the *Act* defines "identifying information" as "information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual."

The information accessed by the nurse was the complainant's electronic health record. It included the following information: her name and address, her location in the hospital, the name of the physician who provided health care to her, as well as her diagnosis and prescribed medications.

The complainant submits that this was "identifying information," and that it comprises her personal health information. The hospital does not dispute this. Given the nature of the information, I find that it is the complainant's personal health information, as defined in section 4 of the *Act*.

HEALTH INFORMATION CUSTODIAN

The term "health information custodian" is defined in section 3(1) of the *Act*. In this case, clause 4 i of section 3(1) is relevant. These parts of section 3(1) state, in part:

> "health information custodian", subject to subsections (3) to (11), means a person or organization described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph, if any:
>
> 4. A person who operates one of the following facilities, programs or services:
>
> i. A hospital within the meaning of the *Public Hospitals Act*, …

The complainant submits that the hospital is a public hospital within the meaning of the *Public Hospitals Act*, and accordingly, a health information custodian under section 3(1)4 i of the *Act*. The hospital does not dispute this.

I have reviewed the results of the Corporation Profile Report which clearly states that The Ottawa Hospital is the corporation that operates the hospital. I agree with the complainant's submission on this point and I find that the hospital is a "health information custodian" under 3(1)4 i of the *Act*.

WAS THE NURSE AN AGENT OF THE HOSPITAL?

The term "agent" is defined in section 2 of the *Act* as follows:

> "agent", in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of

> personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated.

The Notice of Review raised the question of whether the nurse was an agent in the circumstances of this complaint. In the complainant's representations, she submits that "a 'nurse' is an 'agent' in relation to a health information custodian.…" The hospital does not comment on this issue in its representations.

A cursory reading of the definition of "agent" in the circumstances of this complaint might suggest that, because in this instance the nurse did not have the hospital's authorization to use or disclose the health information in question, and was in fact doing so for her own purposes, she was not an "agent." That is not my view. For the reasons that follow, I have concluded that this interpretation is not sustainable, and that the nurse was in fact an agent.

A careful reading of the definition, particularly when viewed in the context of the *Act* as a whole, makes it clear that the Legislature intended that the phrase, "acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian" should be read as a reference to the person's *usual* duties and activities, as opposed to an action taken in the particular circumstances of a complaint. In this case, it is clear that, in her usual role as an employee of the hospital, the nurse does precisely this. It is also important that the definition of "agent" expressly contemplates the inclusion of employees in this category.

The whole idea of "agency" is included in the *Act* to ensure that employees and others whose responsibilities involve access to personal health information are expressly covered by the restrictions and potential sanctions in the *Act* with respect to improper collection, use or disclosure. Broadly speaking, section 7(1) provides that the *Act* applies to the collection, use and disclosure of personal health information "*by a health information custodian*." In respect of public hospitals (and a number of other kinds of health care provider), section 3(1)4 defines "health information custodian" as a "*person who operates*" the facility (in this case, the corporation known as The Ottawa Hospital, rather than its employees or agents).

As well, section 17 of the *Act* clearly contemplates the possibility of improper collection, use or disclosure by agents, which would be impossible if their status as agents ended when they ceased acting for the custodian's purposes and began acting for their own. Sections 17(1)(b) and 17(2) state:

> A health information custodian is responsible for personal health information in the custody or control of the health information custodian and *may permit the custodian's agents* to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if,
>
> (b) the collection, use, disclosure, retention or disposition of the information, as the case may be, is in the course of the agent's duties and not contrary to the limits imposed by the custodian, this Act or another law;

(2) Except as permitted or required by law and subject to the exceptions and additional requirements, if any, that are prescribed, *an agent* of a health information custodian shall not collect, use, disclose, retain or dispose of personal health information on the custodian's behalf unless the custodian permits the agent to do so in accordance with subsection (1). [Emphases added.]

As they apply to agents, these provisions would be rendered meaningless if a person who would usually be an agent is converted to a non-agent in the event that they act improperly. The Legislature could not possibly have intended this result. Accordingly, because the nurse, in the normal course of her duties, acts with the hospital's authorization, and on its behalf, in respect of personal health information, and does so for the hospital's purposes, I find that she is an agent of the hospital under the *Act*.

DISCUSSION:

WAS THE COMPLAINANT'S PERSONAL HEALTH INFORMATION "USED" BY THE NURSE, AND WAS THIS USE IN ACCORDANCE WITH THE *ACT*?

Section 2 of the *Act* defines the term, "use" as follows:

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

Section 6(1) of the *Act* states, in part, that "the providing of personal health information between a health information custodian and an agent of the health information custodian is a use by the custodian, and not a disclosure by the person providing the information…." I have found, above, that the nurse was an agent of the hospital, so section 6(1) establishes that her access to the complainant's personal health information was a "use". Because the nurse is an agent of the hospital who "handled" the information, I am satisfied that her access to the information was a "use", and I will address the question of whether her use of the complainant's personal health information was in accordance with the *Act*.

Permissible uses of personal health information are set out in section 29 of the *Act,* which reads as follows:

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

(b) the collection, use or disclosure, as the case may be, is permitted or required by this *Act*.

The hospital did not provide any representations on the question of whether the nurse's use of the complainant's personal health information was in accordance with the *Act*. The complainant provided detailed representations on this issue.

Under subsection (a), consent is a primary requirement, and the collection, use or disclosure must also be necessary for a lawful purpose. It is clear that the complainant did not consent to the nurse using her information for any purpose. As already discussed, the complainant expressed concerns about her estranged husband or his girlfriend, the nurse, even knowing that she was a patient in the hospital.

The complainant addresses this further in her representations. She states:

> Faced with the stresses associated with an impending divorce and risks of losing custody of her children, [the complainant] took extraordinary measures to both hide her identity and protect her privacy once informed that her health demanded her urgent hospitalization. Why? Because, her estranged husband and his girlfriend worked at the [hospital] and she feared that, if they learned of her medical condition and hospitalization, this information could be used against her with a detrimental adverse effect on her custody battle with her estranged husband.
>
> Apprehending illegal access, use and disclosure of her personal health information, [the complainant], at the time of her admission, took highly unusual precautions to alert, in clear and unequivocal terms, the hospital, the treating physician and the nursing staff both at the [hospital] and the Heart Institute. In a nutshell, she emphasized the need to the medical staff to exercise additional caution and vigilance in protecting her privacy and personal health information.
>
> …
>
> Prior to her admission to the [hospital's] Emergency Ward, [the complainant] informed the emergency nurse of her concerns by noting that her estranged husband and his girlfriend were both employees at the [hospital];
>
> [The complainant] also alerted her treating physician about her apprehension of a possible breach of her privacy. [Her] warnings were duly recorded in the following documents prepared by the [hospital's] medical staff;
>
> a. Patient History and Nursing Assessment dated August 15, 2005;
>
> b. Cardiology Patient Care Plan dated August 15, 2005.
>
> When she was relocated to the Heart Institute … [the complainant] reiterated her apprehension about a breach to her privacy to the medical staff;

> At admission, [the complainant] registered at the [hospital] under her maiden name in order to make sure that she could not be easily identified.

According to the complainant, the information recorded in the records marked "a" and "b", above, reflected a desire not to see her ex-husband, and my review of the evidence supports this view. On this basis, it is obvious that she did not consent to the nurse using her personal health information pursuant to section 29(a) of the *Act*, and accordingly, this section provides no basis for the nurse having the access that she did.

With respect to section 29(b) and the question of whether the use was permitted or required under the *Act*, section 37 of the *Act* sets out those circumstances where personal health information may be used without the consent of the individual to whom the personal health information relates. The only parts of section 37(1) that have possible relevance in the circumstances of this complaint are sections 37(1)(a) and (b). These sections state:

> 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;
>
> (b) for a purpose for which this *Act*, another *Act* or an *Act* of Canada permits or requires a person to disclose it to the custodian;

In my view, the hospital collected the information for the purpose of providing health care services to the complainant. As discussed previously, the nurse had no involvement in providing health care to her. Nor is there any other provision in the *Act* that would provide a basis for the nurse to use the complainant's personal health information.

I find that the nurse was not entitled to use the complainant's personal health information, and her use of the information was in clear contravention of the *Act*.

WAS THE COMPLAINANT'S PERSONAL HEALTH INFORMATION "DISCLOSED" AND WAS THIS DISCLOSURE IN ACCORDANCE WITH THE *ACT*?

Section 2 of the *Act* defines "disclose" in relation to personal health information in the custody or under the control of a health information custodian or a person, as "to make the information available or to release it to another health information custodian or to another person, but does not include to use the information, and 'disclosure' has a corresponding meaning."

As already discussed, the complainant's estranged husband's employment responsibilities did not directly relate to the provision of health care. In my view, he was not an "agent" of the hospital with respect to personal health information, as his employment responsibilities did not involve any form of authorized access to personal health information of the complainant

or anyone else. There is also no evidence that he directly accessed the complainant's personal health information. Based on the evidence, any access he had to the complainant's information would have had to be provided by the nurse. In my view, such access, if it occurred, would properly be characterized as a "disclosure" rather than a "use".

On that point, the investigation report prepared by the hospital indicates that both the nurse and the complainant's estranged husband claimed that he had not been given access to the complainant's information. When he was interviewed by my office in connection with the complaint, however, the estranged husband acknowledged that the nurse had disclosed the complainant's personal health information to him on one occasion.

With regard to information being provided to her estranged husband, by the nurse, the complainant states:

> [The estranged husband] phoned [the complainant] … and raised the issue of her chronic heart condition. This indicated that he had the information about [the complainant]'s health condition even though she had <u>never</u> previously divulged her health condition or her hospitalization to him.

I also observe that the hospital's notes of the complainant's call to the privacy unit, to alert them of her concern that her records had been improperly accessed, document the complainant's allegation that her estranged husband was aware that she had tests at the heart unit, and the precise nature of those tests. The complainant questioned how her estranged husband could have had access to such detailed information.

As noted, despite his initial denial during the hospital's investigation, the estranged husband has acknowledged that the nurse did provide the complainant's personal health information to him. I therefore find that this information was "made available" to him, and based on the definition in section 2, I also find that the information was "disclosed" to him within the meaning of the *Act*. This disclosure was effected by the nurse, whom I have found to be an "agent" of the hospital. Section 7(1)(b)(ii) provides that the *Act* applies to "a person who is not a health information custodian and to whom a health information custodian disclosed the information," which would clearly include disclosure by an agent. For this reason, the restrictions and potential sanctions in the *Act* also apply to the husband with respect to his dealings with the complainant's personal health information.

I now turn to the question of whether the disclosure by the nurse was in accordance with the *Act*. Permitted disclosures of personal health information are discussed in section 29 of the *Act*, which is reproduced in the discussion of "use", above.

Section 29(a), in addition to permitting personal health information to be "used" on the basis of the patient's consent and where it is necessary for a lawful purpose, also permits the information to be "disclosed" on that basis. For the same reasons given above, it is abundantly clear that the complainant did not consent to her estranged husband obtaining disclosure of her information. Given the steps she took to avoid any contact with her estranged husband, or even allowing him

to know that she was a patient in the hospital, I find that she did not consent to the disclosure of her personal health information to him.

Section 29(b) allows for disclosure where it is "permitted or required" under the *Act*. In that regard, sections 38 through 49 enumerate a variety of circumstances in which personal health information may be disclosed without consent. In my view, none of these provisions have any possible application in this complaint.

I therefore find that the disclosure of the complainant's personal health information to her estranged husband was in contravention of the *Act*.

DID THE HOSPITAL COMPLY WITH SECTION 12(1) OF THE *ACT*?

Section 12(1) of the *Act* outlines the obligation of health information custodians to safeguard personal health information. It states:

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

I have already found that the complainant's personal health information, specifically her electronic health records, were both used and disclosed in breach of the *Act*.

Steps taken at Admission and during the Complainant's stay in the Hospital

As mentioned above, the complainant's representations go into considerable detail about her efforts to ensure that her privacy was protected during her admission to the hospital. These efforts began prior to her admission, and as outlined previously, she alerted the hospital, the treating physician and the nursing staff of her concerns, specifically emphasizing "the need for the medical staff to exercise additional caution and vigilance in protecting her privacy and personal health information." The complainant also indicated that she notified hospital staff, at the time of her admission, that she had a restraining order against her estranged husband.

In addition, as already discussed, the complainant took the additional step of registering at the hospital under her maiden name.

I have reviewed a copy of the complainant's Patient History and Nursing Assessment. From this review, it is clear that hospital staff noted in her chart that the complainant's estranged husband works at the hospital and was not to be permitted to see the complainant. In addition the complainant's Cardiology Care Plan shows that a physician at the hospital made a similar note in her chart.

Regardless of whether the complainant made a specific request to have her personal health information protected, the chart notes made by hospital staff make it abundantly clear that the complainant had informed them that her estranged husband was an employee of the hospital and she did not wish him to know that she was in the hospital. It is also significant that she informed the hospital prior to her emergency ward admission that the nurse, her estranged husband's girlfriend, was also an employee at the hospital.

In its representations, the hospital advised the IPC that:

> The [hospital] responded adequately to ensure that the patient's ex-husband would not be aware that she was a patient of the hospital by notifying the Manager of [department of the estranged husband] to ensure that her estranged husband did not work in the area that week.

I do not agree that the hospital responded adequately. The estranged husband was relocated for the duration of the complainant's stay in the hospital, but in my view, while this may have been a starting point for addressing the complainant's concerns, it was by no means a complete response.

In effect, the complainant's concerns were processed by staff as a "physical security" issue and not as a "privacy" matter. No attempts to protect the complainant's personal health information were made. As a result, the privacy office was not contacted at any point by the staff involved. The first notice the privacy office received of the potential breach of privacy was when the complainant later contacted the office, following her discharge from the hospital and upon learning that her estranged husband had obtained information pertaining to her condition.

The inadequacy of this response is highlighted by several policies and procedures of general application that were intended to safeguard personal health information at the time of the complainant's admission, including:

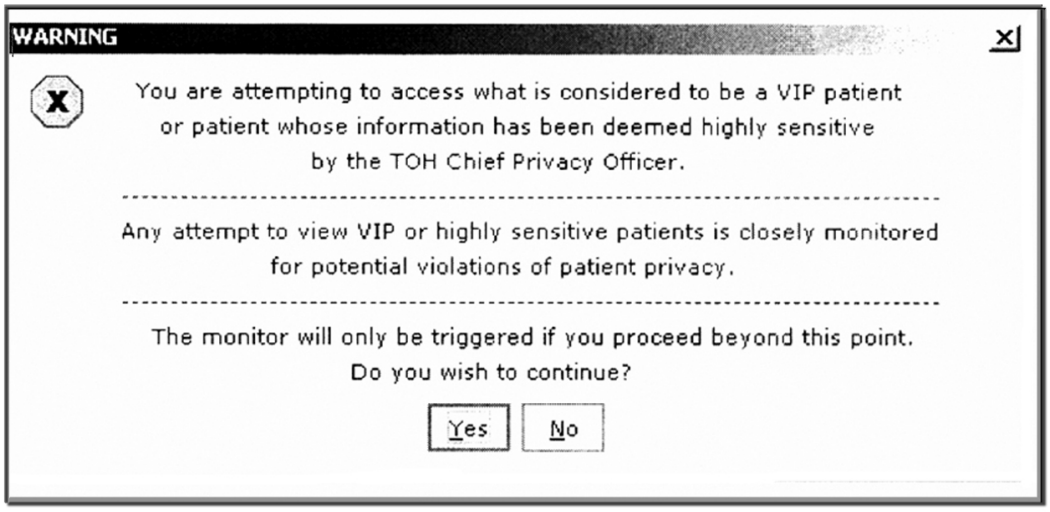
- Protecting Patient's Privacy protocol;
- Responding to Complaints about Privacy Breaches Decision Tree;
- Process for Investigating Privacy Breaches and/or Complaints;
- Patient Concerns Management policy; and
- Ottawa Hospital Privacy policy.

In particular, the "Protecting Patient's Privacy" procedure clearly lays out the process an employee is expected to follow, "When a patient makes a request that they do not want an employee or physician knowing they are in the hospital." In such a situation, the Department Manager is to be notified, and is required to take a number of steps. During my review of this complaint, it became evident that the Supervisor of the estranged husband's department received this notification, rather than the Department Manager. It is not clear whether this caused the

breakdown that occurred in following the "Protecting Patient's Privacy" procedure, which I will now outline.

Under the procedure, the Department Manager is required to notify the employee's manager, who must assign other personnel, if required. The Department Manager is also required to enter the appropriate code in the hospital's Shared Medical System (or "SMS"), one of whose purposes is to set out appropriate rules for visits to the patient.

In addition, however, the Department Manager is required to inform Patient Relations and the Chief Privacy Officer. Upon receipt of the notification, the Chief Privacy Officer is to request that a "VIP Flag" be added to the hospital's electronic patient records system (OACIS) to ensure patient confidentiality. Once the flag is in place, a warning appears onscreen when anyone tries to access the patient's electronic health record, advising that all access to that file is "closely monitored." The person accessing the record is then required to indicate whether they wish to continue by clicking "yes" or "no", as seen below.



Where a patient has indicated they do not want an employee to know they are in the hospital, the "Protecting Patient's Privacy" procedure also requires the Chief Privacy Officer to request a report of all access to the patient's health information, on a daily basis. If the Chief Privacy Officer determines there has been inappropriate access to the patient's health information, the Privacy Breach Process will then be followed.

In this case, except for the requirement to address physical security, it is clear that this policy was not followed. Because of the lack of notice to the Chief Privacy Officer, no VIP flag was added to the complainant's electronic health record at the time of her admission or during the entire length of her stay in the hospital, and for a considerable time afterwards. Nor was any monitoring of access carried out during that period. It was only after the complainant contacted the hospital's privacy office following her conversation with her estranged husband, in which he displayed knowledge of her health situation (that could only have come from her electronic health record), that an audit was performed and a protective flag added to her file. By that

time, as indicated in the hospital's report, the nurse had improperly accessed the complainant's personal health information on seven occasions.

In my view, therefore, the hospital's response to the complainant's extensive attempts to protect the privacy of her personal health information was inadequate. Specifically, the hospital did not "take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against … unauthorized use or disclosure," as required by section 12(1). While the hospital had a good "Protecting Patient's Privacy" procedure in place, the fact that it was not followed in this case underlines the importance of fully integrating all policies and procedures into the fabric of the institution. Even the most rigorous privacy policy will be ineffective if it does not become an accepted part of the institutional culture and its day-to-day operations.

I find that the hospital's limited response to the complainant's expressed concerns at the time of her admission and during her stay in the hospital, up to the time of her contacting the privacy office, was in breach of section 12(1) of the *Act*.

Steps taken following the Complainant's Notification to the Hospital

Unfortunately, there were further problems with the safeguarding of the complainant's health information. Following notification by the complainant of the potential breach, the hospital's Chief Privacy Officer immediately took the following actions: placed a VIP flag on the complainant's electronic record of personal health information, ordered an audit of the electronic record, implemented the privacy office's Privacy Breach Process, and began conducting an internal investigation.

In her complaint letter, the complainant raised the concern that, following notification of the potential breach of the privacy of her personal health information, the "illegal access to [the complainant]'s personal health information continued unabated…," for an additional three weeks, despite the privacy office having been informed of the breach. The hospital advised that during the course of its investigation, the nurse did indeed ignore the VIP flag and accessed the complainant's electronic health record on three further occasions, after the privacy office had been notified of the possible breach by the complainant.

The complainant's letter expressly questions the adequacy of the VIP flag as a means of preventing unauthorized access, concluding that "[o]bviously, a better solution is now urgently required." In my view, the problems that led to the additional instances of unauthorized access can be traced to the hospital's policies, as outlined in greater detail below. The privacy-protection features that are built into the clinical information system used at the Ottawa Hospital are similar to those commonly found in clinical information systems used in other hospitals throughout the province. In general, these systems are designed to provide broad access to personal health information and do not incorporate sophisticated technical features for restricting access to health information. For example, most clinical information systems depend on role-based access privileges (the role of a nurse is permitted broad access); location-based access privileges (i.e., where a system is shared across multiple health care settings); graded levels of access based on

role; confidentiality or privacy flags to indicate patients with sensitivities relating to privacy (e.g., VIPs; patients with sensitive procedures or conditions such as abortions or HIV/AIDS, etc.) and/or retrospective audits to control access to personal health information.

In addition, some clinical information systems, such as that which is in use at the Ottawa Hospital, incorporate somewhat more sophisticated technical features for restricting access to information, namely "on-the-spot" warnings. If a confidentiality or privacy flag has been placed on a record, there may be on-the-spot warnings issued directly to the privacy office upon access to the record. This helps to ensure that any privacy breaches can be quickly identified so that steps may be taken immediately to prevent further breaches. On-the-spot warnings are particularly helpful in cases where patients have identified one or more specific individuals who pose a threat to their privacy, as in the present case. The rationale for not incorporating stricter access controls into clinical information systems that are typically used in hospitals is that if relevant information is not readily available in an emergency situation, this could pose a risk to a patient's health and safety. As a result, I am satisfied that the VIP flag system employed by the hospital meets accepted standards.

In this case, the steps that should have been taken to ensure that no further unauthorized access occurred were apparently hampered by the hospital's Privacy Breach Process and Human Resources protocols. The Privacy Breach Process outlines the steps to be taken by the Chief Privacy Officer, including;

- Requesting an audit of the hospital's information system;
- Contacting Labour Relations for breaches involving staff;
- Investigating the breach, including interviewing the individual who may have accessed the file;
- Notifying the appropriate Manager;
- Disciplinary action for confirmed violations;
- Informing the patient of the results of the audit and any action taken;
- Reporting the breach to the appropriate Professional Regulatory College;
- Reviewing relevant policies and procedures; and
- Contacting the Information and Privacy Commissioner of Ontario, if necessary.

The hospital advised the IPC that the Human Resources protocol for investigations requires meetings with the relevant employee's manager, a representative of the Human Resources department, and in this instance, the union representative, before speaking with the employee. This protocol engendered a time delay of more than three weeks, during which time the nurse in question continued to access the complainant's personal health information on three further occasions. This delay is particularly disturbing.

Given the events that had already transpired, the hospital's reliance on requirements to report to the nurse's Manager, the Human Resources department, and a union representative, to justify the delay in dealing with this continuing breach of privacy is untenable. I appreciate the need for the hospital to have a clear and deliberate protocol for investigating employee actions that may lead to disciplinary action. However, the protection of patient privacy is the paramount consideration in this situation, and must not be impeded by rules about management-employee relations. To the extent that the hospital's policies do not reflect this set of priorities, they are inconsistent with section 12(1) of the *Act*, and must be amended. Under no circumstances should the nurse have been allowed to continue to access the complainant's electronic record of personal health information once the privacy office became aware of the potential unauthorized use by the nurse.

As an example of a different approach, in Report HI-050013, where a hospital employee had inappropriately accessed a patient's chart, the hospital immediately removed the access rights of that employee pending further investigation, and suspended the employee with pay (and later dismissed her). In that instance, the record was not in electronic form. It would be extremely helpful if software developers could explore ways in which health care institutions could block access by a staff member to a particular patient's records, as may be suitable in the circumstances, once an egregious incident such as this one has taken place.

In any event, the chain of events in this case makes it abundantly clear that the hospital's policies, and particularly the Privacy Breach and Human Resources protocols, were not sufficient to protect the complainant's personal health information from further unauthorized access by the nurse.

Having already breached section 12(1) by not taking steps that were reasonable in the circumstances to protect the complainant's personal health information from unauthorized use or disclosure at the time of her admission and during her stay in the hospital, I find that the hospital committed a further breach of section 12(1) of the *Act*. The hospital failed to prevent continued access to the complainant's personal health information by the nurse, despite the fact that the complainant had alerted the Chief Privacy Officer that a breach had likely occurred, and despite the fact that the privacy audit confirmed that breaches had, in fact, already taken place.

Steps taken concerning the Hospital Employees

In addition, having determined that unauthorized access had occurred, the hospital undertook disciplinary action with the employees and entered into agreements with them. In my view, the adequacy of these arrangements must also be reviewed to determine whether they represent "steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal."

As part of the internal investigation, the hospital conducted interviews with representatives from human resources, the managers of the two employees, the union representatives for the two employees and the two employees involved. Appreciating the seriousness of the breach,

the hospital issued disciplinary letters to the nurse and the estranged husband and suspended them without pay for four weeks and ten days, respectively.

The hospital also entered into confidentiality agreements with the nurse and the estranged husband. The terms of the agreements confirmed that the two employees did not alter, destroy, copy or print any or all of the complainant's personal health information.

The complainant's initial complaint and her representations to the IPC expressed a number of concerns about the actions taken in relation to the employees:

- the nurse's initial access lasted for about thirty minutes, which would have allowed her sufficient time to download the entire file;
- it is not known what use the estranged husband may have made of the information that was disclosed to him;
- the sanctions against the employees were inadequate.

Under the *Act*, my focus cannot be with the severity or appropriateness of the sanctions against the employees, which is not part of the Commissioner's identified role. Rather, the issue I must address is whether the actions taken provided adequate safeguards in accordance with section 12(1) of the *Act*.

Upon review of the confidentiality agreements, I find that they do not sufficiently address the issue of unauthorized disclosure. Given that the complainant's concern was that access to her personal health information could have, "a detrimental adverse effect on her custody battle with her estranged husband," I would have expected that the agreements would include a non-disclosure covenant, in addition to the assurances that the nurse and the estranged husband would not alter, destroy, copy or print any or all of the complainant's personal health information. As such, I find the agreements to be insufficient.

In my view, the hospital ought to have taken further steps to prevent any further dissemination of information obtained by the nurse and the complainant's estranged husband. I find that its failure to do so is a further breach of section 12(1).

In addition to the disciplinary action and the confidentiality agreements undertaken, the hospital embarked on a communication initiative to further educate its employees and agents about privacy issues, the role of the Privacy Office, and the *Act* itself. I applaud the hospital and the Chief Privacy Officer for taking these steps.

Following the completion of its investigation, the hospital forwarded a copy of its investigation report, which I have outlined above, to the complainant, the College of Nurses of Ontario and my office.

The complainant maintains that despite the above actions, at no time did the hospital extend to her an apology for the incident. The hospital advised that it did not issue a formal apology to the complainant but rather, that it was their usual practice to apologize upon initially speaking to

the complainant, something the Privacy Coordinator believes she would have done in this case. The hospital was instructed to deal directly with the complainant's legal counsel throughout the investigation; the Chief Privacy Officer advised that she was unable to recall conclusively if at any time a verbal apology had been expressed.

SUMMARY OF FINDINGS:

I have made following findings in this review:

1. The information at issue in the complaint is "personal health information" as defined in section 4 of the *Act*.
2. The hospital is a "health information custodian" as defined in section 3(1)4i of the *Act*.
3. The nurse is an "agent" of the hospital as defined in section 2 of the *Act* in relation to the use and disclosure of personal health information referred to in this complaint.
4. The complainant's personal health information was "used," as defined in section 2 of the *Act*, by the nurse.
5. This use of the complainant's personal health information was in contravention of the *Act*.
6. The complainant's personal health information was "disclosed," as defined in section 2 of the *Act*, to the complainant's estranged husband.
7. This disclosure of the complainant's personal health information was in contravention of the *Act*.
8. The hospital did not comply with section 12(1) of the *Act* in that it did not take steps that were reasonable in the circumstances to ensure that the personal health information in its custody or control was protected against theft, loss and unauthorized use or disclosure, and to ensure that the records containing the personal health information were protected against unauthorized copying, modification or disposal.
9. Staff of the hospital failed to follow internal policies that specifically related to the protection of patients' privacy, and in so doing, failed to ensure the fullest protection of the complainant's privacy and her personal health information.
10. The hospital failed to take immediate action to prevent any further unauthorized use of the complainant's personal health information, once notified by the complainant of the possible breach of her privacy.

ORDER:

1. I order the hospital to review and revise its practices, procedures and protocols relating to patient health information and privacy, and those relating to human resources, to ensure that they comply with the requirements of the *Act* and its regulations, taking into account the concerns expressed in this order about the paramount importance of protecting patients' personal health information.

2. As part of the review under order provision 1, I order that the hospital implement a protocol to ensure that reasonable and immediate steps are taken, upon being notified of an actual or potential breach of an individual's privacy, to ensure that no further unauthorized use or disclosure of records of personal health information is permitted.

3. Following the review, I order the hospital to ensure that all employees and/or agents of the hospital are appropriately informed of:

   (a) their duties under the *Act* pursuant to section 15(3)(b) of the *Act*;

   (b) their obligations to comply with the revised information practices of the hospital pursuant to section 10(2) of the *Act*;

4. While I cannot order the hospital to issue a formal apology to the complainant, I strongly urge the hospital to do so.

5. In order to verify compliance with this order, I require that the hospital provide me with proof of compliance by October 27, 2006.

POSTSCRIPT:

This was a truly regrettable situation in which a patient who was admitted to a hospital, made a specific request to prohibit her estranged husband and his girlfriend, a nurse at the hospital, from having any information regarding her hospitalization, only to learn that the exact opposite had occurred.

Despite having alerted the hospital to the possibility of harm, the harm nonetheless occurred. While the hospital had policies in place to safeguard health information, they were not followed completely, nor were they sufficient to prevent a breach of this nature from occurring. In addition, the fact that the nurse chose to disregard not only the hospital's policies but her ethical obligations as a registered nurse, and continued to surreptitiously access a patient's electronic health record, disregarding three warnings alerting her to the seriousness of her unauthorized access, is especially troubling. Protections against such blatant disregard for a patient's privacy by an employee of a hospital must be built into the policies and practices of a health institution.

This speaks broadly to the culture of privacy that must be created in healthcare institutions across the province. Unless policies are inter-woven into the fabric of a hospital's day-to-day

operations, they will not work. Hospitals must ensure that they not only educate their staff about the *Act* and information policies and practices implemented by the hospital, but must also ensure that privacy becomes embedded into their institutional culture. As one of the largest academic health sciences centres in Canada, the Ottawa Hospital had properly developed a number of policies and procedures; but yet, they were insufficient to prevent members of its staff from deliberately undermining them.

Health information custodians are responsible for ensuring compliance with the *Act* and are responsible for the actions of their employees and agents. I am taking this opportunity to remind all custodians of the importance of ensuring that their employees and agents are made fully aware and properly trained with respect to their obligations under the *Act*, as well as the need to create environments in which privacy issues are not only understood, but form an integral part of the culture of their institution. Despite the stellar efforts of this hospital's Chief Privacy Officer, the hospital's failure to follow through on its privacy policies at the time of the complainant's admission, followed by priority being given to a Human Resources Protocol over preventing further instances of unauthorized access to the patient's records, contributed in large part to the breaches reported. The ultimate responsibility, of course, lies in the actions of the two offending parties.

I strongly encourage all health information custodians, especially larger institutions such as hospitals, to take the need to protect patient privacy to heart. Upholding compliance with the Act is not simply a matter of following the provisions of an enacted law, but ensuring that the use and disclosure of sensitive personal information such as health information is strongly monitored, and access controlled to those who truly need it in the performance of their duties. Predicating access on a "need to know" basis could perhaps be no more important than in a healthcare setting, where so much is at stake. The negative consequences flowing from the unauthorized access and use of a patient's health information are extensive and far-ranging. Patients have enough to deal with – any additional stress arising from an unauthorized party peering into their health records is completely unacceptable.

July 27, 2006

Ann Cavoukian, Ph.D.
Commissioner