1.0 BACKGROUND

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 alleged that a hospital employee, a diagnostic imaging technologist (the technologist), contravened the *Act* by inappropriately accessing her records of personal health information on six separate occasions, and that her personal health information was used and disclosed by the technologist without her consent. The complainant explained that the technologist is the former spouse of the complainant's current spouse, and alleged that the technologist accessed her electronic record of personal health information over a period of nine months, for no health related purpose.

In her complaint letter, dated October 13, 2010, and during her interview with this office, the complainant explained that when she suspected that the technologist had accessed her records of personal health information, she contacted the hospital's Privacy Officer by e-mail on July 11, 2010. The complainant reported her concerns to the Privacy Officer and requested a list of all individuals who had accessed her records of personal health information from February, 2008 to that date.

The hospital conducted an investigation into the matter and ultimately confirmed that the technologist had accessed the complainant's electronic records of personal health information. The hospital later wrote to the complainant on July 30, 2010, setting out the results of the audits that were performed during the investigation, and apologized for the incident. The hospital also stated:

> I want to assure you that this incident has been dealt with appropriately based on The Ottawa Hospital's Privacy Policy and we remain committed to protecting the privacy and confidentiality of and security of all personal health information we are entrusted with by our patients.

The complainant was not satisfied with the response that she received from the hospital and filed this complaint.

1.1 The Precedent - Order HO-002

Prior to discussing the details of this incident and the resulting investigation, it is instructive to review a previous investigation that I conducted which resulted in the issuance of Order

HO-002 on July 27, 2006. Order HO-002 also involved this hospital – the circumstances of that investigation are strikingly similar in nature to the circumstances of this complaint.

The complainant in Order HO-002 alleged that a nurse had accessed her personal health information, and that the information was used and disclosed without her consent. The complainant in that Order had informed the hospital at the time of admission that her estranged husband was an employee of the hospital and she did not wish him to know that she had been admitted. In addition, she had informed the hospital that the estranged husband's girlfriend was also an employee of the hospital.

After the complainant was discharged from the hospital, she discovered that her estranged husband had information about her treatment. She notified the hospital and an audit was conducted. The results of the audit established that the girlfriend, a nurse, had accessed the complainant's personal health information on seven occasions.

In Order HO-002, I found that the personal health information of the complainant was used and disclosed in contravention of the *Act* and that the hospital had failed to take steps that were reasonable in the circumstances to ensure the personal health information was protected against unauthorized use and disclosure in breach of section 12(1) of the *Act*.

In my order provisions, among other things, I ordered the hospital to 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. I also ordered the hospital to ensure that all employees of the hospital are appropriately informed of their duties under the *Act*.

2.0 CONCLUSION

In the discussion that follows, I conclude that although existing policies were reviewed and revised, new policies developed, and further efforts were made by the hospital to educate agents of their obligations under the *Act* following the issuance of Order HO-002, it is apparent that, as in Order HO-002, some of the hospital's own policies were not followed in the circumstances of this complaint.

I also conclude that the actions taken to prevent the unauthorized use and disclosure by employees in this hospital have not been effective and are not in compliance with section 12(1) of the *Act*. While I recognize the limits of the technological and administrative controls that are available in the complex environment of a hospital, in my view, the

circumstances set out below demonstrate that these controls must be reviewed. In addition, the order provisions speak to the cultural shift that is required in order to effect a change in attitude about patients' privacy in The Ottawa Hospital.

3.0 CONDUCT OF THE INVESTIGATION

Following the receipt of this complaint, I initiated a review and assigned the file to a Mediator/Investigator, who immediately began to gather further information from the hospital, including copies of relevant policies and procedures. The Mediator/Investigator also interviewed the following individuals:

- the hospital's Privacy Officer,
- the complainant, and
- the technologist.

During the interview of the hospital's Privacy Officer, the following details were provided about the incident.

- On July 11, 2010, the complainant e-mailed the hospital alleging that there had been a breach of her privacy.
- On July 12, 2010, the Privacy Officer ordered audits on the records of personal health information of the complainant. That same day, the Privacy Officer received the audit report and contacted the complainant to advise that the technologist had accessed the complainant's electronic records of personal health information on six separate occasions.
- The audit found that the complainant's records of personal health information had been accessed by the technologist as follows:
    - *July 22, 2008 – 20 screens;*
    - *October 6, 2008 – 21 screens;*
    - *November 6, 2008 – 18 screens;*
    - *December 20, 2008 – 20 screens (a "Sensitive Warning Flag" appeared on one of the screens viewed and the technologist did not look at that screen);*
    - *March 19, 2009 – 8 screens (a "Sensitive Warning Flag" appeared on one*

screen but the technologist chose to view that screen regardless);

- *April 7, 2009 – 9 screens.*

- According to the information provided by the Privacy Officer, the "Sensitive Warning Flag" referred to above, warns users that the field they are about to view is "highly sensitive." It is applied when a determination is made that the field to be viewed *may* contain particularly sensitive information. For example, if the "Sensitive Warning Flag" was applied to all data relating to genetic testing, or some other type of sensitive data, the flag would appear at the time any attempt is made to open a screen or field that would contain information of that nature. If an identified patient had never undergone genetic testing, then no information relating to that patient would appear once the field or screen was open. The decision to add the flag is an administrative decision of the hospital; it is not initiated by the patient.

- Unlike the "VIP Warning Flag" referred to below and contained in Order HO-002, if a user disregards the "Sensitive Warning Flag," and continues on, an audit report is *not* automatically generated and forwarded to the Privacy Officer. The Privacy Officer explained that this was because the "Sensitive Warning Flag" system is no longer in use. However, the "Sensitive Warning Flag" has not yet been deleted from all electronic records of personal health information.

- The Privacy Officer also stated that the hospital has replaced the "Sensitive Warning Flag" with the "VIP Warning Flag" in recognition of the fact that all personal health information is sensitive. The Privacy Officer was not able to provide my office with any documentation regarding the "Sensitive Warning Flag", except to state that historically it was used to "flag" particularly sensitive categories of personal health information.

- As noted above, the technologist encountered the "Sensitive Warning Flag" on two occasions. On the first occasion, she respected the warning and did not go beyond the flag. The Privacy Officer advised that despite the fact that the technologist went beyond the "Sensitive Warning Flag" on the second occasion, the screen viewed did not contain any personal health information of the complainant. Regardless, the technologist's decision to go beyond the flag was in blatant disregard of hospital policy and procedures – it is a factor that should have been taken into account by the hospital in arriving at the appropriate discipline.

- The audit also revealed that the following electronic information systems were accessed by the technologist:

PACS This is the Picture Archiving Communication System. It includes images obtained from ultrasound, MRI, X-ray and CT scans.

OACIS This is the hospital's main electronic information system which contains records of personal health information. It includes information such as blood work, visit dates, laboratory results, medications, and doctors' reports/notes.

SMS This is known as the Shared Medical System. It includes patient appointments, health numbers, contact information, and doctors' reports.

- A second audit was subsequently ordered to determine whether records of personal health information related to the complainant's spouse and son were accessed by the technologist. This audit confirmed that the technologist did not access these records. In addition, a "user audit" was conducted on the technologist, looking at the full scope of her access to electronic records dating back to 2001. No anomalies were found in this audit.

- On July 14, 2010, following the receipt of an e-mail from the complainant requesting a status update, the Privacy Officer advised the complainant that the hospital took the matter seriously, that an investigation was underway and that appropriate action would be taken. The Privacy Officer also told the complainant that a "VIP Warning Flag" would be added to the complainant's electronic records.

- The "VIP Warning Flag" is a warning that appears onscreen advising agents accessing a patient's electronic records of personal health information that the information flagged has been deemed highly sensitive by the Chief Privacy Officer. The "VIP Warning Flag" screen states that any attempt to view this 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 Warning Flag," an audit report is *automatically* generated by the Information Technology Department, and forwarded to the Privacy Officer each time the record is viewed.

- On July 14, 2010, the Director of Diagnostic Imaging, the technologist's supervisor, and Senior Advisor in Human Resources were advised of the complaint and the results of the audits.

- Between July 12, 2010 and July 27, 2010, the technologist was away from the

hospital. When she returned on July 28, 2010, a meeting was held with the Privacy Officer, the Director of Diagnostic Imaging, the Senior Advisor in Human Resources, a union representative and the technologist. During that meeting, the technologist admitted having accessed the complainant's personal health information but she denied that the information had ever been disclosed, copied or altered.

- The hospital concluded its investigation by preparing a "Privacy Breach Summary Report" which found that the technologist was not authorized to view the records. The report recommended that the technologist receive three days suspension without pay and undergo privacy retraining and counselling. Copies of this report were provided to senior management of the hospital. The disciplinary recommendations were confirmed and carried out.

- As noted above, once the hospital concluded its investigation, it issued a letter to the complainant which advised her that the investigation had concluded. The letter included an apology and set out the results of the audits. The complainant was not given any information as to whether or not the technologist was disciplined as a result of this incident.

During the interview with the complainant, she provided the following additional information to the IPC:

- The complainant stated that she wanted to have more information regarding the specific sanctions and discipline imposed on the technologist and how the hospital reached its decision.

- The complainant also wanted to know what steps have been taken to ensure that these circumstances would not be repeated in relation to both her records of personal health information, and that of other patients.

- The complainant wanted more information about the hospital's auditing practices.

The technologist was also interviewed and provided the IPC with information regarding the circumstances at issue. The information provided by the technologist did not differ in any material way from the information set out above.

Subsequently, the hospital was invited to submit representations in writing on the issues arising in this investigation. Representations were received from the hospital.

4.0 ISSUES ARISING FROM THE INVESTIGATION

I identified the following issues as arising from this review:

Are the records at issue "records" of "personal health information" as defined in sections 2 and 4 of the *Act*?

Is the hospital a "health information custodian" as defined in section 3(1) of the *Act?*

Is the technologist an "agent" as defined in section 2 of the *Act*?

Was the complainant's personal health information "used" and/or "disclosed;" if so, was it "used" and/or "disclosed" in accordance with the *Act*?

Did the hospital have information practices that comply with the requirements of the *Act* and did the health information custodian comply with these practices as required by sections 10(1) and (2) of the *Act*?

Did the hospital comply with section 12(1) of the *Act* by taking reasonable steps to ensure that personal health information was secured against theft, loss and unauthorized use or disclosure?

Did the hospital comply with section 16(1) of the *Act* by making available to the public a written statement that provides a general description of its information practices?

5.0 RESULTS OF THE INVESTIGATION

Issue A: Are the records at issue "records" of "personal health information" as defined in sections 2 and 4 of the *Act*?

Section 2 of the *Act* defines a "record" as:

> ... a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record.

Section 4(1) of the *Act* states, in part:

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, or

(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,

…

(f) is the individual's health number,

Section 4(2) of the *Act* states:

"identifying information" means 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 at issue was contained in the complainant's electronic record of personal health information and included doctors' and nurses' notes and reports, diagnostic imaging, laboratory results, the health number of the complainant, contact details for the complainant and scheduled medical appointments. I am satisfied that the information in the records was identifying information that related to the health and to the provision of health care to the complainant and to the identity of the provider of health care to the complainant, as well as the complainant's health number. On that basis, I find that the records are records of personal health information as defined in sections 2 and 4 of the *Act*. The hospital does not dispute this finding.

Issue B: Is the hospital a "health information custodian" as defined in section 3(1) of the *Act*?

Section 3(1) of the *Act* states, 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* ...

Section 2 of the *Act* defines a "person" to include a partnership, association or other entity. Section 87 of the *Legislation Act, 2006*, S.O. 2006, c. 21 further provides that a "person" includes a corporation.

Consistent with my findings in Order HO-002, I find that The Ottawa Hospital is a "person" who operates a hospital within the meaning of the *Public Hospitals Act* and that it is a health information custodian with custody or control of the personal health information at issue as defined in section 3(1)4i of the *Act*. The hospital does not dispute this finding.

Issue C: Is the technologist an "agent" as defined in section 2 of the *Act*?

Section 2 of the *Act* defines an "agent" 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;

In addition, section 17(1) of the *Act* states:

> 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,
>
> (a) the custodian is permitted or required to collect, use, disclose, retain or dispose of the information, as the case may be;
>
> (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; and

(c) the prescribed requirements, if any, are met.

While the hospital does not dispute that the technologist is employed by, and is generally authorized to act on behalf of, the hospital with respect to personal health information, it takes the position that the technologist did not access the records of the complainant in the course of her duties as an agent of the hospital.

I rejected a similar argument in Order HO-002. In that Order, I concluded that a person who, in the normal course of that person's duties, acts with the authorization of the health information custodian, and acts for or on behalf of the health information custodian in respect of personal health information, is an "agent" within the meaning of the *Act*.

In particular, I stated:

> 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.
>
> …
>
> 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.
>
> …
>
> 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.

In my view, the same rationale applies in this matter. As a result, I am satisfied that the technologist is an "agent" of the hospital, as defined in section 2 of the *Act*.

Issue D: Was the complainant's personal health information "used" and/or "disclosed" and, if so, was it "used" and/or "disclosed" in accordance with the *Act*?

Section 2 of the *Act* defines the terms "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;

That section also defines "disclose:"

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

Section 6(1) of the *Act* is also relevant. It 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...."

Was the complainant's personal health information "used" in accordance with the *Act*?

Given that I have found that the technologist is an agent of the hospital, applying section 6(1) of the *Act*, I find that her access to the complainant's personal health information was a "use." I will now turn to the question of whether her use of the complainant's personal health information was in accordance with the *Act*.

Section 17(2) states:

> 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).

Permissible uses of personal health information are set out in section 29 of the *Act*, which states 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.

There is no evidence before me to suggest that the complainant consented to the use of the personal health information by the technologist pursuant to section 29(a) of the *Act*. In fact, the opposite is the case. The technologist clearly knew that her use of the complainant's records of personal health information was occurring without the complainant's consent, and that such consent would not be provided.

With respect to 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 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;

While the hospital's representations do not directly address the question of whether the personal health information was permitted to be used by the technologist without the consent of the complainant, it states that the technologist admitted reading the information

in the records "for her own purposes."

The hospital collected the information in question for the purpose of providing health care to the complainant, however, the technologist had no involvement in the provision of such care. Nor is there any other provision in the *Act* that would provide a basis for the technologist to use the complainant's personal health information without the consent of the complainant. As a result, section 37 does not permit the technologist to use the personal information in the absence of consent.

Although the hospital's representations do not specifically address the application of section 17(2), it is apparent in the circumstances of this matter that the technologist was not using the complainant's records of personal health information with the permission of the custodian and, therefore, I also find that her use was contrary to section 17(2).

For these reasons, I find that the technologist was not entitled to use the complainant's personal health information, and her use of the information was in complete contravention of the *Act*.

Was the complainant's personal health information "disclosed" and, if so, was it "disclosed" in accordance with the *Act*?

The complainant states in her letter of complaint that she believes her personal health information was shared by the technologist with family and friends. However, when questioned about this issue, the complainant stated that she had no direct evidence to support her belief and that she had drawn inferences from information provided by her spouse.

The hospital states that the technologist denied altering, disclosing or printing the personal health information of the complainant.

Although I am sensitive to the concerns expressed by the complainant, there is insufficient evidence before me to support a finding that the technologist disclosed the complainant's personal health information. When asked directly by my staff, she strongly denied having disclosed any information from the complainant's record. I am therefore not in a position to make a finding in this regard. I will not address this issue further except to the extent that I will comment below on the steps taken by the hospital to safeguard the records of personal health information following discovery of the breach.

Issue E: Did the hospital have information practices that comply with the requirements of the *Act* and did the hospital comply with these practices

as required by sections 10(1) and (2) of the *Act*?

Section 10(1) of the *Act* states:

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

Section 10(2) states:

> A health information custodian shall comply with its information practices.

Section 2 of the *Act* defines "information practices" as:

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

During the course of this investigation, a number of documents were provided to me, including:

- *Administrative Policy and Procedure Manual – Privacy ADM II 260*;
- *Protecting Patient's Privacy* procedure,
- *Process for Investigating Privacy Breaches and/or Complaints,*
- A sample *Confidentiality Agreement*,
- A sample *Confidentiality Pledge,*
- Snapshot of VIP Warning Flag screen,
- Snapshot of Sensitive Warning Flag screen.

In the discussion that follows, I will consider whether the hospital's information practices comply with the *Act* and whether these information practices have been followed. The

existing information practices were examined in the context of this specific fact situation and, therefore, I will only comment on those portions of the information practices that relate to the issue of the unauthorized access to records of personal health information by agents of the hospital.

Administrative Policy and Procedure Manual - Privacy Policy ADM II 260

Privacy Policy ADM II 260 states, in part:

> Violation of this policy is grounds for disciplinary action up to and including dismissal. Physicians and residents breaching their duty of privacy and confidentiality as outlined in this policy may be subject to suspension or termination of privileges.
>
> …
>
> *Access to confidential information will be limited to only those employees authorized to hold, view or handle such information for their current job duties.* Access is to be determined by the employee's direct supervisor.
>
> Personal information is to be maintained in the strictest of confidence and is not to be shared with unauthorized persons. For example, employees/agents must avoid engaging in discussions about personal information in public areas such as hallways, elevators, cafeterias, etc.
>
> *Audits are conducted on the Hospital's electronic records.* Limitations are placed on users to ensure that they only have access to information they require to do their job. [Emphasis added.]

Generally, I am satisfied that the hospital's privacy policy, as written, is adequate in relation to unauthorized use. However, I also find that in practice, there are a number of issues that make it difficult for the hospital to ensure compliance with the information practices, as set out in this policy.

For example, despite the statement in the policy that "limitations are placed on users to ensure that they only have access to information they require to do their job," there are few limits in place for staff members who provide health care and, therefore, most staff who provide health care have access to all electronic records of personal health information. There are generally no technological restrictions in place at the hospital that would limit the access of a staff member to only those electronic records of personal health information relating to the individuals to whom that staff member is assisting in providing health care. Additionally, there are generally no technological restrictions relating to the fields in the

electronic records that are required by staff for the purpose of providing or assisting in providing health care. Further, where a breach has been identified by a patient, the hospital cannot take any actions to restrict further access to the complainant's records other than to place a "VIP Warning Flag" on the file or block access by a staff member to all of the electronic information systems.

I also note that, contrary to its own policy which states, "audits are conducted on the Hospital's electronic records," the hospital's "SMS" information system cannot be audited despite the fact that this system contains personal health information including patient contact details, health numbers, appointment details, and doctors' reports. I am concerned that the hospital is using certain electronic information systems that are not subject to audit.

For all of these reasons, I find that the hospital has failed to comply with its own practices contrary to section 10(2) of the *Act*.

I will address the issues of "role-based access" and audits further in my discussion relating to section 12 of the *Act*, and in the order provisions that follow.

Protecting Patient's Privacy

Protecting Patient's Privacy is an internal procedure that is not made available to patients. It sets out the rules regarding visits and calls to patients, and inquiries made about the admission status of patients. Pursuant to this procedure, and at the request of a patient, the Chief Privacy Officer and/or the Department Manager must notify the Admitting Department to change the appropriate code in the "SMS" database to reflect a patient's instructions in relation to callers and visitors.

This procedure also describes the "VIP Warning Flag." It states that, upon request, the Chief Privacy Officer will direct that a "VIP Warning Flag" be added to the OACIS information system and will request a report on all access to the patient's records of health information in that database on a daily basis. According to this procedure, the Chief Privacy Officer must investigate all incidents of access to determine whether they were authorized. In the event of unauthorized use, the *Process for Investigating Privacy Breaches and/or Complaints* will be followed.

In Order HO-002, I found that the "VIP Warning Flag" system complied with acceptable standards. However, in the circumstances of this complaint, a flag was only added to the complainant's records after the allegation of a breach was made to the hospital and, unlike the circumstances in HO-002, the agent did not continue to access the records in this

period of time. Therefore, the detailed workings of the "VIP Warning Flag" are not at issue in this complaint.

However, the hospital states that the "VIP Warning Flag" can only be used with the OACIS system. Consequently, my concern is that it is of limited value in deterring the unauthorized use of personal health information contained in **other** information systems used by the hospital including PACS and SMS, which were both accessed by the technologist in this complaint.

I am also concerned that the hospital does not appear to give any information to patients about their right to have a "VIP Warning Flag" applied to their records of personal health information. I will discuss this in more detail below in the context of a review of the hospital's obligations under section 16(1) of the *Act* to provide patients with a general description of its information practices.

Process for Investigating Privacy Breaches and/or Complaints

In Order HO-002, I had ordered the hospital to implement a protocol to ensure that, upon being notified of an actual or potential breach of an individual's privacy, reasonable and immediate steps are taken to prevent the further unauthorized use or disclosure of records of personal health information. As a result of the order, changes were made to the hospital's *Process for Investigating Privacy Breaches and/or Complaints.*

However, my investigation demonstrated that the hospital once again failed to comply with its own policy.

This process requires that reasonable and immediate steps be taken within two business days of notification of a breach. For the most part, the required steps were followed by the hospital. Most important, unlike Order HO-002, the hospital moved quickly to ensure that the technologist did not continue to have unauthorized access to the complainant's record while its investigation was taking place.

However, contrary to its own policy, the following three required steps were not carried out:

(a) The patient will be informed as to the results of the investigation and any action taken in a written report.

(b) A written report of the breach will be filed with the appropriate professional regulatory college.

(c) A review of whether policies and procedures adequately protected personal

health information will be conducted and required changes will be implemented.

In addition, contrary to the findings made in Order HO-002, the hospital has discontinued its previous practice of obtaining a non-disclosure agreement and confidentiality undertaking from the offending employee once a breach has been discovered. I will address this issue before I turn to the three steps in the process that were not complied with.

Confidentiality Undertaking and Non-Disclosure Agreement

While the nurse in Order HO-002 was required by the hospital to sign a confidentiality undertaking to confirm that she did not alter, destroy, copy or print any or all of the complainant's personal health information, the hospital advises that it no longer requires employees to sign undertakings of this nature following a breach. The Privacy Officer advised my staff that this practice was discontinued following the issuance of Order HO-002 because the hospital's human resources department advised against it. In its representations, the hospital stated that the union advised its members against signing the undertaking. However, the hospital did not provide my office with any evidence or information to suggest that there are any legal impediments relating to this practice, or the basis for the union's position. I find this completely unacceptable.

The decision to discontinue this practice is of great concern to me and, in my view, should be reinstated immediately. Where an employee demonstrates a complete disregard for hospital policies and procedures, it is unreasonable for the hospital to continue to give the employee access to the complainant's records of personal health information on the basis of a verbal undertaking that the information will not be disclosed. Without a confidentiality undertaking and non-disclosure agreement, it is difficult to provide firm assurance to a complainant that his or her information has not been disclosed and that it will not be subsequently disclosed.

In view of my findings, I will order that the requirement for a confidentiality undertaking and non-disclosure agreement be made part of the *Process for Investigating Privacy Breaches and/or Complaints.*

(a) Information Provided to Complainant

The hospital's *Process for Investigating Privacy Breaches and/or Complaints* requires that, following confirmation of a breach, a patient be informed of any actions taken by the hospital in a written report. Other than reporting to the complainant regarding the results of

the audits conducted, the complainant was provided with limited information regarding the actions taken to address this incident. In my view, the complainant has a right to this information – she was the victim of a breach of the *Act* that was confirmed and acknowledged by the hospital. The complainant has a right to receive assurances that the incident has been appropriately addressed and that steps have been taken to prevent its re-occurrence. Critical to this assurance are details of the steps taken by the hospital, including the results of its investigation and the fact that disciplinary action was taken against the employee in question. As noted above, the complainant should also receive the assurance that a confidentiality undertaking and non-disclosure agreement has been signed.

(b) Report to Professional College

The *Process for Investigating Privacy Breaches and/or Complaints* also states that "a written report of the breach will be filed with the appropriate professional regulatory college." Despite this, the hospital did not notify the technologist's professional regulatory college of the breach. In this case, the complainant notified the college and filed a complaint on her own initiative. After the Privacy Officer became aware that the complainant had taken this action, the hospital did not provide the college with a written report of the breach. When asked why the written report of the breach was not filed with the professional regulatory college, the Privacy Officer stated that the college did not ask for the hospital to comment.

In my view, the hospital's actions amount to a failure to comply with its own policies contrary to section 10(2) of the *Act*. Below, I will order that immediate steps be taken to provide the technologist's professional regulatory college with a copy of this Order and the hospital's Privacy Breach Summary Report.

(c) Review of Existing Policies and Practices

The *Process for Investigating Privacy Breaches and/or Complaints* calls for a review of existing policies and procedures following a breach, to determine if they adequately protect personal health information. In this case, following its investigation, the hospital did not conduct such a review. The hospital advised my office that policies are reviewed on an annual basis and the need for any further review was not apparent. In its representations, the hospital states that because the breach was a result of poor judgement on the technologist's part, the policies could not have prevented this unauthorized use. The hospital also states that it acknowledges that protecting personal health information and privacy are important and that it monitors and reviews its processes quarterly with reports back to the Senior Management Team and the Board Audit Committee to ensure

compliance with best practices.

In my view, consistent with existing hospital policy, this incident should have triggered a review of policies as they specifically relate to the unauthorized access of records of personal health information by employees of the hospital. The complainant should also have been advised of the existence of the review and any conclusions drawn from it. While I recognize that no single policy will be sufficient to eradicate breaches of the *Act*, hospital policies should be reviewed with a view to addressing complaints of this nature. I am also concerned that the hospital's approach to what amounts to a serious breach of privacy does not send the right message to its employees. I will therefore order, in accordance with section 10(2), that the hospital comply with its own policies regarding investigating privacy breaches by initiating a review of existing policies and practices.

Other Information Practices

My office was informed that, at the conclusion of an investigation into a privacy breach, the usual practice of the hospital's Privacy Office is to conduct privacy retraining in the department in which a breach has occurred. However, as a result of an oversight, this retraining did not take place following confirmation of the current breach. As has often been stated, comprehensive education and awareness campaigns are essential tools to protect the privacy rights of patients. I will therefore order that this training take place immediately.

Issue F: Did the hospital comply with section 12(1) of the *Act* by taking reasonable steps to ensure that personal health information was secured against theft, loss and unauthorized use or disclosure?

Section 12(1) of the *Act* outlines the obligation of health information custodians to protect 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 was used in a manner contrary to the *Act*. This raises the question of whether the hospital took steps that are reasonable in the circumstances to ensure that the complainant's personal health information was protected against unauthorized use. In this regard, the following policies

dealing with the hospital's safeguards are relevant:

- Administrative Policy and Procedure Manual- Information Systems and Technology Security ADM VII 160,
- Administrative Policy and Procedure Manual - Privacy Policy ADM II 260,
- *Protecting Patient's Privacy; Information Booklet for Employees, Students and Volunteers*,
- Password disclaimer,
- *OACIS Web Audit Process and Objectives*,
- A poster entitled *A Privacy Breach Could Ruin Your Career*,
- Training Powerpoints,
- Privacy Video.

In its representations, the hospital submits that it has implemented adequate administrative, technical and physical safeguards to ensure that the personal health information in its custody or control is protected against unauthorized use.

The hospital also explains that its privacy and security offices were merged "to support the confidentiality, integrity and availability of information" and states:

> The privacy and security program is designed to be effective and embedded into the hospital's operations, projects and culture; ensuring appropriate controls and processes are in place to mitigate risks; and maintaining compliance with PHIPA.

I will now turn to consider the safeguards that the hospital has in place.

Technical Safeguards

Role-Based Access Restrictions

Privacy Policy ADM II 260 states that "limitations are placed on users to ensure that they only have access to information that they require to do their job." Initially, staff in my office were advised that this limitation is only exercised in relation to employees, such as housekeeping and kitchen staff, who are not providing health care to patients. In its

representations, the hospital clarified that there are two levels of access within the OACIS database. In-patient nurses are limited to accessing the personal health information of patients seeking health care on their in-patient units. This restriction is based on the computer used to gain access and the user login details which only permits access to the personal health information of patients on their ward. However, all other employees who provide health care, including the technologist, have complete access to the personal health information in the OACIS information system.

The hospital also clarified that access to the PACS database is limited primarily to physicians, technologists and some nurses. It did not provide any information as to how access to the personal health information in this database is restricted except to say that although all staff who have access can view all of the personal health information in the database, there may be some restrictions on the functions that can be performed by identified groups. For example, some staff can only view the information, while others can copy and alter the information. The technologist had full, unrestricted access to PACS.

Access to the SMS database is determined by the staff member's direct management team and can be restricted based on their role. I am advised that the technologist has access to the "Radiology module" and the functions that she can carry out within the module are limited.

Although the hospital did not provide representations regarding the technologist's access to other databases containing records of personal health information, despite having been asked to do so, during the interview, the Privacy Officer stated that the technologist had full access to all other databases. Therefore, as previously noted, the technologist had wide-ranging access to most hospital electronic health information systems.

The Privacy Officer also advised my staff that the hospital does not have the technological means to restrict identified employees or groups of employees from accessing the records of personal health information of one particular patient or groups of patients, on the basis of their roles or functions, other than as set out above. I recognize that the hospital is not unique in this regard and that many hospitals have a similar inability to limit the access of staff members to only those records of personal health information that they require to perform their functions.

In Order HO-002, I noted that the clinical information systems used at the hospital are designed to provide broad access to personal health information and do not incorporate sophisticated technical features for restricting access to personal health information. I acknowledged that the rationale for not incorporating stricter access controls into the clinical information systems used in hospitals is that relevant personal health information

must be readily available in an emergency situation, otherwise, a patient's health and safety may be at risk. Having regard to all of those factors, and on the basis of the information before me at that time, I was satisfied that the clinical information systems in place at the hospital were in compliance with the *Act*.

However, section 12(1) of the *Act* requires that health information custodians revisit their safeguards from time to time to ensure that they continue to be "reasonable in the circumstances" to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal. As new technologies are developed, the "reasonable measures" standard in section 12(1) will evolve. Four years have passed since Order HO-002 was issued and the hospital has experienced another breach involving unauthorized use by an employee.

While the technical safeguards that were in place may have been reasonable when the investigation into Order HO-002 was conducted, that may no longer be the case. For example, it may now be possible to limit the access of staff to only those records of personal health information that relate to the patients to whom they are providing health care, rather than the current "all or nothing" approach. Similarly, the ability to limit a staff member's access to a specific record at the request of a patient, and/or to limit access to identified fields of personal health information, may now be reasonably achievable. In light of this incident, it is time that the hospital investigates whether technical solutions exist to achieve greater security and to better protect the privacy of patients' records of personal health information.

Under these circumstances, I have decided to recommend that the hospital conduct a review of its technological safeguards and the solutions that are currently available on the market. I will further recommend that the hospital assess whether these solutions better protect the confidentiality of personal health information and the privacy of individuals than the current technical safeguards implemented by the hospital. As part of its review and assessment, the hospital should have regard to the volume of the personal health information in its custody or control, the threats and risks associated with the personal health information, the number and nature of individuals who have access to personal health information, evolving industry standards and practices, and the technical safeguards employed by other hospitals in the province. I will also order that the hospital report back to me on the results of its review.

Login Notice

Employees are prompted to change their passwords on OACIS every sixty days. When

prompted, they receive the *Password Disclaimer* notice referred to above, which states, among other things, the following:

- employees are required to follow the policies of the hospital regarding confidentiality and to use their own passwords and ID,
- employees should not access information other than that required to carry out their duties and disclose information concerning patients and the hospital and its employees,
- a breach of confidentiality constitutes a serious offence, may result in discipline and possible termination of employment and may amount to an offence under the Criminal Code and be contrary to one or more other statutes, and
- the employee agrees to indemnify the hospital against any causes of action, costs or damages suffered by reason of breach of confidentiality.

In my view, this Password Disclaimer is a good reminder to all employees of their obligations to protect personal health information and to comply with the *Act*.

I note that there are systems in place at other hospitals that automatically display a notice when an employee logs into the electronic record. This notice provides a regular reminder that they may only access personal health information as required for their job and that failure to comply may result in termination. It also indicates that access will be tracked and audited to ensure compliance and requires the employee to select "OK" or "Cancel" in order to continue.

While the messaging is similar to the language of the "Password Disclaimer" used by the hospital, employees receive the reminder more frequently and the messaging focuses on the issue of privacy and protection of personal health information. It is also different from the "Sensitive Warning Flag" and the "VIP Warning Flag" because it can be applied to all electronic information systems.

In my view, this type of automatic notice provides employees with a helpful reminder at every login of their responsibilities under the *Act*. I also find that it qualifies as a reasonable measure to ensure that personal health information is protected against unauthorized use in accordance with section 12(1) of the *Act*. Until such time as the hospital has instituted the more comprehensive solution that I am asking it to investigate, I will order that such a login notice system be implemented on all electronic information systems that contain personal health information.

Audits

Speaking broadly, audit is a method or process to verify adherence to a policy, standard or objective. The goal of any audit process is to reduce the level of risk by having in place systems to prevent, detect and confirm breaches of policies and procedures. An audit may be carried out in a number of different ways; it may be targeted or random, real-time or after the fact. Audits are essential components of the technical safeguards for electronic health information systems because they may be used to detect who has accessed and viewed an electronic record, and can be used to maintain the integrity of the information in the record.

The *Administrative Policy and Procedure Manual - Information Systems and Technology Security ADM VII 160* states that the audit of electronic information systems is the responsibility of the Information Security and Technology department. In particular, it states that the Information Security and Technology department is responsible for ensuring audit availability of the network environment and that staff are aware of the auditing functions and capabilities. In addition, it must ensure that audit trails are implemented to provide information on who accesses what information and when.

The *OACIS Web Audit Process* policy is more specific. It specifies that audits will be run daily on files flagged with a "VIP Warning Flag" in the OACIS database. Other areas of focus for OACIS audit reports include non-hospital users (for example, at affiliate sites), patients associated with highly sensitive areas (for example, abortion clinics), as well as patients associated with routine encounters or visits, across all disciplines. The frequency of other audits range from once per month, to twice a year. All audits must be conducted in consultation with, or the approval of, the Chief Privacy Officer.

As noted, this audit policy relates to the OACIS system only. I have not been provided with any other specific policies that address the audit of the other health information systems used by the hospital.

In fact, I have been advised that, despite these policies, there are a number of electronic information systems used in the hospital that are not subject to audit because of their age. These include SMS and a number of other databases. Of greater concern is the fact that there are a number of information systems which have an audit function that has not been "turned on." This is evidenced in the last three quarterly reports by the Information Technology and Security department to Senior Management which state:

> OACIS has sophisticated and robust audit capability but *similar capability has not been turned on or is unavailable in the majority of other [hospital] systems*.

[Emphasis added.]

I also note from my review of these reports that the work necessary to ensure that the audit capability is "turned on" is "ongoing." However, this feature has yet to be activated.

In my view, the fact that audit functions are either non-existent or have not been turned on in relation to any of the electronic information systems of the hospital that contain personal health information falls short of meeting the requirements of section 12(1) of the *Act.* In view of this deficiency, I will recommend that, while conducting the review referred to earlier, the hospital explore the possibility of implementing software that would enable the hospital to audit *all* of its electronic information systems containing personal health information. In addition, I will recommend that steps be taken at the earliest opportunity to "turn on" the audit function for any databases that already have that functionality.

Administrative Safeguards

The requirement in section 12 to "take steps that are reasonable" to ensure that personal health information is protected against unauthorized use includes administrative measures such as privacy training and privacy awareness initiatives. I now turn to a review of the administrative safeguards implemented by the hospital as they relate to training and education.

Privacy Training

The hospital conducts privacy training with all new employees as part of its orientation program. All staff who were employed with the hospital at the time that the *Act* was proclaimed in force also received training, at which attendance was taken, through the privacy office. The Privacy Officer has verified that the technologist did receive this privacy training and that she did undergo additional training following the breach.

I have reviewed the training materials that have been provided to our office and I am satisfied that they set out a comprehensive education and training program relating to the hospital's obligations under the *Act*. In addition, I am satisfied that the materials include sufficient discussion around the consequences of unauthorized use of personal health information.

However, while the privacy training program aimed at management staff includes a reference to Order HO-002, no similar reference is included in the privacy training program for all other agents and employees of the hospital. In order to use this incident as a learning experience for everyone, I will order that the hospital issue a communiqué to all staff regarding Order HO-002 and the findings and order provisions set out in this Order.

Paramount in this communiqué should be a message to staff that the hospital regards breaches of this nature as serious matters, and that action will be taken to discipline agents who violate the privacy rights of patients. Further, their respective professional regulatory colleges will be provided with written reports setting out the circumstances of the breach.

In my view, all staff members should be made aware of the results of my investigation in Order HO-002 and in this Order. My order provisions relating to the communiqué to be issued to all agents will ensure that this is done. The privacy office should also include a reference to Order HO-002 and to this Order in all future privacy training sessions.

Confidentiality Pledge and Confidentiality Undertaking

A Confidentiality Pledge is distributed to all staff on an annual basis. It states that it is the expectation that all employees accept the following pledge:

- the employee will not access or use any confidential and/or personal health information that they learn of or possess, unless it is necessary for them to do so in order to perform their job responsibilities;

…

- the employee understands that alleged breaches will be investigated.

The pledge further recognizes that an employee's failure to comply with the above, or their participation in a breach of privacy, may result in disciplinary action, including the termination of employment or affiliation with the hospital, or loss of medical, dental and midwifery staff privileges, as the case may be, and may also result in legal action being taken against the individual.

A Confidentiality Agreement is signed by all new employees during orientation and it contains the same language that is in the undertaking.

I commend the hospital for instituting the Confidentiality Undertaking and Confidentiality Agreement and note that it is consistent with the hospital's obligations under section 12 of the *Act*.

Issue G: Did the hospital comply with section 16(1) of the *Act* by making available to the public a written statement that provides a general description of its information practices?

Section 16(1) of the *Act* provides, in part, as follows:

16. (1) A health information custodian shall, in a manner that is practical in the circumstances, make available to the public a written statement that,

(a) provides a general description of the custodian's information practices;

As previously noted, section 10 of the *Act* requires health information custodians to have in place, and to comply with, "information practices" that fulfil the requirements of the *Act* and the regulations. Section 16 requires that the hospital make available a written public statement that provides a general description of its information practices; that is, the policies of the hospital for actions in relation to personal health information.

Although the hospital has provided the IPC with an internal privacy policy that references the "VIP Warning Flag," it appears that the right to have a "VIP Warning Flag" added to records of personal health information is not communicated to patients unless they self-identify as having a concern about privacy. Thus, most patients would remain unaware of such a provision.

The value of the "VIP Warning Flag" system is drastically reduced if the public is unaware of its existence. For example, had the complainant known of the flag's existence, she could have requested that it be placed on her file. As noted previously, this would have generated an audit report to be forwarded to the Privacy Officer, each time that her record was accessed. Arguably, such a flag, and the resulting audit report, may have limited the technologist's access to the complainant's records and the extent of the privacy breach. I will therefore be ordering that the hospital amend its written public statement to notify individuals of the "VIP Warning Flag" system in order to fulfill its obligations under section 16(1) of the *Act*. In particular, the written public statement should describe the "VIP Warning Flag" system, how an individual may request the flag, and the employee(s) of the hospital to whom the request should be directed

6.0 ORDER

I order that The Ottawa Hospital:

Review and revise its policies, procedures and information practices relating to personal health information to ensure that they comply with the requirements of the *Act* and its regulations, taking into account the concerns expressed in this Order.

As part of the review under Order provision 1, amend its *Process for Investigating Privacy Breaches and/or Complaints* to add a provision

requiring an agent or employee who has contravened the *Act* to sign a confidentiality undertaking and non-disclosure agreement.

Immediately provide a written report of the privacy breach and a copy of this Order to the technologist's professional regulatory college.

Issue a communiqué to all agents and employees regarding Order HO-002 and the findings and order provisions contained in Order HO-010. This communiqué should include a message that the hospital views breaches of this nature seriously, that action will be taken to discipline agents who are found to have breached the *Act,* and that their professional regulatory colleges will be provided written reports setting out the circumstances of the breach.

Include a discussion of Order HO-002 and Order HO-010 in all future training programs.

Conduct privacy retraining for all agents and employees in the technologist's department, as required by the hospital's privacy policy.

Amend its written public statement to include a description of the "VIP Warning Flag" system, to indicate how an individual may request a "VIP Warning Flag" and to identify the employee(s) of the hospital to whom the request may be directed. The hospital should also take the necessary steps to ensure that the "VIP Warning Flag" may be applied in all electronic information systems that include personal health information.

Until such time as the hospital has instituted comprehensive, role-based functionality to limit access to personal health information, implement a notice that automatically displays whenever an agent or employee logs into a database containing records of personal health information and reminds them that they may only access personal health information on a need-to-know basis, that access will be tracked and audited to ensure compliance, and that the failure to comply may result in termination. The notice should also require employees to affirmatively select "Accept" or "Cancel."

Report back to my office on the implementation of these Order provisions on or before March 31, 2011.

Report back to my office on the results of the reviews and assessments referred to in the two Recommendations made below, on or before June 30, 2011.

7.0 RECOMMENDATIONS

I recommend that The Ottawa Hospital:

1. Conduct a review of existing technological safeguards and the solutions that are currently available on the market to facilitate role-based access and audit; assess whether these solutions better protect the confidentiality of personal health information and the privacy of individuals than the current technical safeguards implemented by the hospital. As part of its review and assessment, the hospital should have regard to:

    - the volume of personal health information in its custody or control;
    - the threats and risks associated with the personal health information;
    - the number and nature of individuals who have access to personal health information;
    - evolving industry standards and practices;
    - the technical safeguards employed by other hospitals in the province; and
    - the possibility of implementing software that would enable all electronic information systems containing personal health information to be audited.

2. Review the audit functionality on all systems employed at the hospital and take steps to ensure that the audit capability is "turned on." If necessary, consult with the Ontario Hospital Association on best practices in this area.

8.0 COMMISSIONER'S MESSAGE

As noted in this Order, The Ottawa Hospital conducted an investigation into the circumstances of the complaint filed by a patient. After confirming that the complainant's records of personal health information had been accessed in an unauthorized manner by a

staff member, and that a breach of the *Personal Health Information Protection Act* had occurred, disciplinary action was taken against the technologist involved, consisting of a three-day suspension without pay.

Under the *Act*, I cannot address the severity or appropriateness of the sanctions imposed against the technologist, as it 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*. However, as previously discussed, in the circumstances of this complaint, the technologist consciously chose to go beyond the "Sensitive Flag Warning" on one occasion, in blatant disregard for the privacy flag and hospital policy. In addition, while the technologist accessed the records of personal health information of the complainant on six separate occasions, the audit results revealed that on three of those occasions, the technologist viewed **over** 20 different screens of data at each access point, totaling 96 screens having been viewed over six unauthorized entries. In my view, these circumstances should be considered significant factors in determining the appropriate level of discipline imposed on individuals who violate the privacy rights of patients.

In its communications with the complainant, the hospital confirmed and apologized for the breaches, stating that the incident had been dealt with appropriately. Further details as to the disciplinary action taken against the technologist were not provided – namely, the fact of a three-day suspension. Understandably, the complainant was not happy with the vague nature of the hospital's communication and the limited amount of information provided.

During the course of this investigation, my staff had numerous conversations with staff of The Ottawa Hospital, encouraging the hospital to disclose the specific details of the discipline to the complainant. This included a telephone conversation that I personally had with the President and Chief Executive Officer of the hospital.

Despite our urging, and an initial indication that the details would be revealed, the hospital decided against this action. My staff asked the hospital to provide the reason or the specific legal impediment preventing this disclosure, however, none was provided. The hospital only provided a section of a collective agreement, which had no relevance whatsoever to the issue. I can only assume that details of the disciplinary action taken against the technologist were not provided to the complainant based on past practice rather than on any legal or collectively bargained restrictions.

Note that in Order HO-002, the discipline received by the offending employee was contained in the Order. In addition, when consulted by other hospitals in similar situations, we have advised that an individual whose file has been inappropriately accessed has the

right to know, not only the identity of the staff member who accessed their file, but the details of any disciplinary action taken, including the quantum of any penalty.

This level of transparency is important for several reasons. Accessing a patient's personal health information in an unauthorized manner is a serious violation of an individual's privacy and security of the person. In such a situation, the aggrieved individual has a right to a complete accounting of what has occurred. In many cases, the aggrieved parties will not find closure regarding the incident unless **all** the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required.

For other staff members of the hospital involved, knowing that all of the details of the disciplinary action imposed will be publicly disclosed, should serve as a strong deterrent. This is especially true if those details also become known to other employees, either through the actions of the aggrieved individual, the custodian, or both. Employees must understand that, given the seriousness of these types of breaches, their own privacy concerns will take a back seat to the legitimate needs of the victims involved to have a full accounting of the actions taken by the health information custodian. Our primary concern must lie with the aggrieved party, whose privacy was completely disregarded.