PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. PC-020007-1

Ministry of Health and Long-Term Care

December 12, 2002

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. **PC-020007-1**

MEDIATOR: **Shaun Sanderson**

INSTITUTION: **Ministry of Health and Long-Term Care**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

On March 4, 2002, the provincial New Democratic Party (NDP) Caucus Services issued a press release to advise that two NDP Members of Provincial Parliament (MPP's) had received three complaints of document mishandling by the Ministry of Health and Long-Term Care (the Ministry) in which personal information such as medical conditions, prescriptions and credit card receipts, had been sent to the wrong people. The press release indicated that two of the complaints involved the Trillium Drug Plan, while the third involved the Registration and Claims Branch. During a press conference, the NDP asked the Ontario Provincial Police (the OPP) to investigate these breaches of confidentiality, and turned over the relevant documentation to Queen's Park Security Service.

That same day, a journalist from the Queen's Park Bureau contacted the Office of the Information and Privacy Commissioner/Ontario (the IPC) to discuss this incident, and subsequently published an article in a Toronto newspaper. On March 6, 2002, the IPC initiated a formal privacy complaint under the *Freedom of Information and Protection of Privacy Act* (the *Act*).

On March 8, 2002, the IPC attended a meeting at the Ministry's Office of the Assistant Deputy Minister for Health Services. During this meeting, the following things occurred:

- The Ministry advised the IPC that it could not provide us with any details about these breaches, as it had only learned of these incidents through the press release and newspaper article. As such, it would be unable to notify affected persons and commence an internal investigation until the documents at issue were provided to them.

- The Ministry did, however, speculate that the breaches could be the result of a computer error problem, which the Trillium Drug Program (Trillium) experienced within the last year. Apparently Trillium had received phone calls from a number of clients who were

sent personal health information belonging to other recipients. The Ministry did not have further details about this issue, but indicated that the problem had been fixed. Trillium's Director agreed to look into this matter further, and to determine whether it would be possible to ascertain which individuals were affected by this problem.

- The IPC advised the Ministry that it would commence its own investigation into these matters, and accordingly agreed to contact the OPP to determine whether the documents could be retrieved.

On March 14, 2002, an OPP Detective retrieved the documents from Queen's Park Security Service, and hand-delivered them to the IPC. Copies were then provided to the Ministry's FOI Co-ordinator for review and follow-up.

Before discussing the substantive issues and results of this investigation, it should be noted that many aspects of our investigation were delayed as a result of the Ontario Public Service Employees Union (OPSEU) strike, which occurred from March 13, 2002 through May 5, 2002. However, upon completion of the OPSEU strike, this Office received full co-operation from staff at the relevant Ministry branches.

BACKGROUND TO THE INCIDENTS:

During the preliminary stages of this investigation, I interviewed a number of individuals (including the relevant MPP's and two of the complainants) to clarify the circumstances surrounding each incident. The following is a background to these incidents:

I) Drug Programs Branch (Trillium Drug Program) – Incidents 1, 2 & 3

The Trillium Drug Program unit administers the program for people who have high drug costs in relation to their income by assessing applications and processing receipts. The program has an annual deductible that is based on income. Each year starting August l, recipients must pay for their drug cost up to their deductible level before they are eligible for drug coverage. The deductible is paid in quarterly instalments. Once the deductible is paid in each quarter, eligible people receive drug coverage until the start of the next quarter.

Incident #1

In February 2002, an MPP's office received a telephone call from a constituent who was concerned that she had received another individual's personal health information relating to the Trillium Drug Program. The staff person advised the constituent to return the information to the Ministry, but did not record further details about the incident, nor the constituent's name. The constituent did not follow-up with the MPP's office, nor did she contact or return the information to the Ministry.

Incident #2

On or about February 27, 2002, Person A (a Trillium client) received a letter from the Ministry, which included another individual's credit card slips and drug receipts. The letter stated that the receipts were being returned as invalid, as they did not contain an Rx number indicating that the product was dispensed by prescription. Person A explained that, upon notifying the Ministry of this error, he was advised by a Trillium staff member to return the documents to the Ministry and to not contact an MPP or the person named on the receipts. Person A then contacted his MPP to advise her of this incident. The complaint was forwarded to the Health Critic MPP as well as the Justice Critic MPP. On March 3, 2002, all three MPP's attended the home of Person A to examine, verify and seal the relevant documents. After the press conference on March 4, 2002, the sealed package was handed over to Queen's Park Security Service.

Incident #3

On April 26, 2002, the FOI Co-ordinator contacted this office to advise that, during the course of this investigation, the Ministry became aware of a new incident. While investigating incident #2, a Trillium manager found a memo dated March 7, 2002, indicating that a woman (Person B) had called to advise them that she had received another individual's health information. Coincidentally, the information pertained to Person A. The Ministry employee had asked Person B to either destroy the information, or to send it back to them. As of April 26, 2002, the Ministry had not followed up to verify whether this had occurred, nor had anyone contacted Person A to advise him of the incident.

II) Registration and Claims Branch/Provider Services Branch – Incident #4

The Registration and Claims Branch is responsible for delivering a number of programs, including the registration of eligible health care providers, the payment of medical and hospital claims to Ontario health care providers and the payment of medical and hospital claims for Ontario residents visiting other provinces and countries.

The Provider Services Branch is responsible for the Fee-for-Service Payment Program under the *Health Insurance Act* for the following fee-for-service providers: physicians, chiropractors, physiotherapy facilities, optometrists, podiatrists, and dentists. Medical consultants working for Provider Services Branch are located in several of the Registration and Claims Branch district/regional offices and work directly with Registration and Claims Branch staff.

Incident #4

In early Fall 2001, Person C's physician submitted an application for out-of-province medical coverage on her behalf. In October 2001, Person C received another individual's denial letter from the Ministry. The letter contained the individual's name, physician, medical condition and Health Number. Upon twice notifying the Ministry of this error, Person C was offered an apology and advised to destroy the information. However, Person C did not destroy the information, as she was concerned there may have been a mix-up with her own application. On November 5, 2001, while attending a meeting at her MPP's constituency office, Person C

advised the staff person of this incident. However, the MPP was not made aware of this until February 28, 2002, following incident #2. On March 1st the MPP contacted Person C to discuss the matter further, and on March 4th, Person C brought the letter to her MPP's office. The document was subsequently provided to Queen's Park Security Service.

ISSUES ARISING FROM THE IPC INVESTIGATION:

The following issues were identified as arising from the investigation:

(A) Was the information in question "personal information" as defined in section 2(1) of the *Act*? If yes,

(B) Was the disclosure of the personal information in accordance with section 42 of the *Act*?

RESULTS OF THE INVESTIGATION:

Issue A: Was the information in question "personal information" as defined in section 2(1) of the *Act*?

Section 2(1) of the *Act* states, in part:

> "personal information" means recorded information about an identifiable individual, including,
>
> …
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> …
>
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
>
> (g) the views or opinions of another individual about the individual, and

> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Incident #1

Further to discussions with the MPP, I was unable to obtain any further details regarding the type of information that was allegedly sent to her constituent by the Ministry. In discussions with the FOI Co-ordinator, I was advised that the Ministry had no knowledge of such an incident occurring. It is my view that, if the constituent did receive correspondence from the Ministry relating to another individual, it would have likely contained personal information as defined in section 2(1) of the *Act*. However, in the absence of any specific details regarding this incident, and based on the limited information provided, I am unable to conclude whether the information at issue was personal information as defined in section 2(1) of the *Act*. Accordingly, I will not be referring to this incident further in this report.

Incident #2

I have reviewed the relevant documents relating to incident #2 and note that the information at issue consists of three pharmacy receipts. The receipts contain the name and address of the pharmacy, a slip number, the sale amount, a credit card number, expiry date and an authorization number. Although the press release had indicated that the receipts also contained the signature and name of the affected person, I have found this not to be the case. During our investigation, it was learned that the signature line on the receipt contained the word "Del", which indicates that the medication was delivered to the affected person. I must therefore determine whether, in the absence of a name or signature, the receipts contain personal information as contemplated in section 2(1) of the *Act*.

In Order P-230, former Commissioner Tom Wright commented on the approach to be taken in determining whether information qualifies as personal information within the meaning of section 2(1) of the *Act*:

> I believe that provisions of the Act relating to protection of personal privacy should not be read in a restrictive manner. If there is a reasonable expectation that the individual can be identified from the information, then such information qualifies under subsection 2(1) as personal information.

Based on the above, and the circumstances of this case, I believe that it is reasonable to expect that the individual in question could be identified from the information that appears on the three pharmacy receipts. I also find that the receipts contain both information about financial transactions in which the individual was involved, as well as an identifying number assigned to the individual, contemplated in paragraphs (b) and (c) of the definition of personal information in section 2(1) of the *Act*.

The Ministry does not dispute this finding.

Incident #3

As noted earlier, the Ministry was made aware of incident #3 when Person B contacted them on March 7, 2002. The Ministry advised the IPC that Person B had received a letter from Trillium, which was addressed to Person A. Upon notifying the Ministry of this incident, Person B was advised to either destroy the information, or return it to the Ministry. Since the Ministry had not followed up with Person B, nor received the relevant documentation by April 26, 2002, I contacted Person B to obtain further details. During our telephone discussion, Person B advised me of the following:

- She received a package from the Ministry, which contained correspondence pertaining to her, as well as approximately three pages pertaining to another individual. To the best of her recollection, the three pages consisted of two form letters and one sheet that resembled an invoice/record of prescriptions. The documents were sent from Trillium, and included information such as Person A's name, address, file number and prescription information. She said the three pages were stapled to her own correspondence in error.

- She could not remember the exact date that she received the information; however, she believes it was sometime in late February 2002. She telephoned the Ministry as soon as she received the package, and was told to dispose of the information. After her initial phone call to the Ministry, she did not receive any follow-up calls.

Although I am unable to review the documentation, based on my discussions with Person B, I am satisfied that the information at issue contained personal information as contemplated in one or more of paragraphs (b), (c), (d), (f), (g) and (h) of the definition of personal information in section 2(1) of the *Act*.

The Ministry does not dispute this finding.

Incident #4

I have reviewed the relevant documents relating to incident #4 and note that the information at issue consists of a two-page letter relating to another individual other than Person C. The letter is addressed to a physician, and advises that the affected person's application for payment of health services outside Canada has been denied. The letter also contains the affected person's name, Health Card Number and refers to a specialist consultation requested. It is my view that the information at issue contains personal information as contemplated by one or more of paragraphs (b), (c), (f), (g) and (h) of the definition of personal information in section 2(1) of the *Act*.

The Ministry does not dispute this finding.

Conclusion: The information relating to incidents 2, 3 and 4 was personal information as defined in section 2(1) of the *Act*.

Issue B: Was the disclosure of the personal information in accordance with section 42 of the *Act*?

Section 42 of the *Act* sets out the rules for disclosure of personal information other than to the individual to whom the information relates. This section provides that an institution shall not disclose personal information in its custody or under its control, except in the circumstances listed in section 42(a) through (n). Having reviewed these provisions, I find that none of these circumstances were present in any of incidents 2, 3 or 4. Accordingly, I find that the disclosures of personal information by the Ministry were not in compliance with the *Act*.

The Ministry does not dispute this finding.

Conclusion: The disclosures of personal information relating to incidents 2, 3 and 4 were not in compliance with section 42 of the *Act*.

OTHER MATTERS:

The first two priorities for an institution faced with a potential disclosure of personal information are: firstly, to identify the scope of the disclosure and take steps to contain it; and secondly, to identify those individuals whose personal information may have been disclosed and, barring exceptional circumstances, to notify those individuals accordingly. In order to do this, the institution must arrange for the safe return of the disclosed information to ensure it is properly contained and that the recipient has not retained any copies, nor passed along the information to any other individuals. Retrieving the documents will not only assist the institution in trying to determine how the error occurred and whether corrective measures are required, but will also assist in providing proper notice to the individuals whose privacy has been compromised.

Containment:

Incident #2

As noted earlier, on March 3, 2002, all three MPP's involved in this complaint attended the home of Person A to examine, verify and seal the relevant documents, which were then turned over to the Queen's Park Security Service. During this investigation I contacted all three MPP's to confirm that no additional copies of this information have been retained. I also contacted Person A, who confirmed that he has not retained any copies of the documents at issue, nor passed them along to any other individuals.

Incident #3

Upon learning of this new incident, I contacted Person B to discuss details about the information she had received. During our discussion, she told me that she was advised by the Ministry to destroy the information. Accordingly, she advised me that she ripped up the pages into dozens of pieces and, as a safety precaution, disposed of the pieces in three different garbage bags. She confirmed that she has not kept any of this information, nor passed it along to any other individuals.

Incident #4

During this investigation, I contacted the MPP who was involved in this complaint to confirm that neither her, nor her staff, had retained any copies of the documents at issue. I also contacted person C, who advised me that she has not retained any copies of the documents, nor passed them along to any other individuals.

Based upon my discussions as noted above, I am satisfied that all the improperly disclosed information has been contained, and that the recipients of this information have neither retained any copies, nor passed along the information to any other individuals.

Notice to affected persons:

Incident #2

The Ministry contends that, due to the OPSEU strike, they were unable to immediately notify the affected person whose personal information was improperly disclosed. The Ministry also indicated that it had difficulty identifying the affected person in this case, but, as noted earlier, was able to eventually do so. Although this incident occurred on or about February 27, 2002, the affected person was not notified about the breach of her personal privacy until May 9, 2002, by way of a telephone call. The Ministry advised that the affected person was satisfied with the explanation provided, and accepted its apology for the error.

Incident #3

A Ministry employee was advised of this incident on March 7, 2002, but did not notify the FOI Co-ordinator. She became aware of this incident during the course of this investigation, and subsequently advised the IPC on April 26, 2002. The affected person was notified about the breach of his personal privacy on May 3, 2002, by way of a telephone call. He was also advised that an investigation into this matter was underway. The Ministry advised the IPC that the client understood what had transpired and accepted Trillium's expressed regrets.

Incident #4

On April 3, 2002, the Ministry notified the affected person by telephone to advise her about the breach of her personal privacy and the circumstances surrounding this incident. She was also told that a formal letter would be forthcoming from the Director of Provider Services, and that the IPC was investigating the matter. The Ministry advised the IPC that she was appreciative of the call and the steps planned to prevent future incidents from occurring. On April 10, 2002 the Director of Provider Services sent a letter to the affected person, expressing her regret for this incident. The letter also outlined details of the incident and advised her that they are investigating this matter to determine whether corrective measures in the office procedures will be required. On June 11, 2002, the Director sent a follow-up letter to the affected person, again expressing the Ministry's regrets, and advising her about the steps that had been initiated to avoid similar occurrences in the future.

Summary of Trillium's investigation and steps taken in response:

I attended a meeting at the Ministry's main offices on June 27, 2002 to discuss Trillium's investigation and findings. During this meeting, I was advised that Trillium had concluded its own internal investigation into these matters, and was provided with a verbal overview of its findings. In particular, I was advised that Trillium's recent incidents were unrelated to the computer error problem that it experienced last year. Trillium agreed to provide the IPC with a written report outlining these findings. I also scheduled a follow-up meeting to review the relevant policies and procedures.

I subsequently attended Trillium's offices on July 16, 2002 to review the office procedures, as well as to obtain copies of all relevant policies. The IPC then received Trillium's written report on August 20, 2002. The report outlined the privacy issues as follows:

Incidents 2 and 3

Trillium determined that these incidents resulted from human error in the mailing procedure. When advised about incident #2 on February 26, 2002, a client information clerk asked Person A to return the information he received in error. The Manager then held a staff meeting to remind them of the importance of adhering to the mailing procedures for the protection of document confidentiality. When advised about incident #3 on March 7, 2002, a client information clerk asked Person B to either destroy or return the information she received in error. On March 9, 2002, the Associate Director of Trillium held a unit staff meeting to stress the importance of protecting client's confidentiality, and also discussed ways to improve the process for mailing confidential documents.

In its report, Trillium stated the following:

> The mailing of TDP [Trillium Drug Program] confidential information to applicants and potential applicants is taken very seriously by the program as the information that is handled on a day-to-day basis is highly confidential. All staff is certainly aware of what can happen if we are not extremely careful. The program mails out approx. 300 receipt summaries, in addition to other documents, per day so it is important that everything is done to ensure confidentiality.
>
> Once this breach was discovered the manager immediately had a staff meeting and reminded staff about the importance of confidentiality and how important it is to make sure that documents are going to the right applicant.
>
> Since this incident we have revisited the way we handle documents and have implemented a plan to improve the process for mailing.

Trillium has provided the IPC with a copy of its "Updated Mailroom Procedures" which were altered to reduce the potential for errors and to enforce accountability. Prior to this, any documents that needed to be returned to clients were forwarded with the file to the mailroom.

The documents were then sent out by a staff member from that unit. The new procedure allows for the processing staff to handle the return of documents right from the source. Each processing staff is now responsible for returning documents to clients. The processing staff must now gather, assemble and mail all documents that need to be returned.

Computer Error Problem

Trillium uses a software program called RAM (Receipt Adjudication and Management) to adjudicate prescription drug receipts and print out receipt summary reports. A defect in RAM's print engine occurred when printing summaries of merged information for different Trillium applicants. The error involved an addressee being matched to the incorrect summary report. Subsequently, a small number of Trillium clients were sent information belonging to other recipients. Trillium staff was unaware of the problem at the time. In April 2001, Trillium received calls from recipients advising that their receipt summary reports contained information relating to other individuals. The recipients were asked to destroy the documents or return them to Trillium. Based on the calls, Trillium immediately initiated an investigation to determine the cause of the problem.

Following an investigation, the RAM print engine problem was discovered. The manager opened a "high priority technical Problem Log" for an immediate fix, and assigned it to the technical staff. In the interim, Trillium instituted a process to ensure that all mailings were manually checked before leaving the office to prevent further mailing mistakes. A memo outlining a description of the problem, as well as the temporary workaround to the problem was distributed to all staff on May 16, 2001. On May 17, 2001, the "code for the fix" was sent to Trillium's current software provider, who is under contract to provide technical support and maintain the Health Network Systems. The corrected software was installed in Trillium's computers on May 29, 2001. Trillium has provided the IPC with the supporting documentation referred to above.

As noted earlier, during our initial meeting with the Ministry on March 8, 2002, Trillium's Director agreed to look into this matter further and to determine whether it would be possible to ascertain which individuals were affected by this problem for the purposes of notification. Trillium's report indicates that Ministry technical staff, as well as software provider staff, attempted to extract this information but were unsuccessful.

Summary of Provider Services' investigation and steps taken in response:

During this investigation, it was determined that the Ministry's Provider Services Branch, rather than the Registration and Claims Branch, would lead responsibility for the error which resulted in incident #4. As such, I attended a meeting at the Ministry's office of the Assistant Deputy Minister for Health Services to discuss Provider Services' investigation and findings, as well as to obtain copies of all relevant documents referred to below.

At this meeting, I was provided with Provider Services' final written report, which contains its investigation and findings in relation to this matter, as well as the steps that have been

implemented to prevent a similar situation from reoccurring. The report provided the following background to this situation, which was also explained during the meeting.

The Provider Services Branch has Medical Consultants located in several district offices across the province. As part of their duties, Medical Consultants review applications for prior approval for full payment of insured out-of-country health services. The Ministry receives and responds to approximately 2000 applications per year. These applications are adjudicated in accordance with the *Health Insurance Act* of Ontario. The patient and the Ontario physician are advised of the Ministry's decision. Support staff from the Registration and Claims Branch produces denial letters with specific paragraphs provided by the Medical Consultant. These letters are sent from district offices that have Medical Consultants in place, while head office in Kingston produces denial letters for districts that do not. Letters of approval are all sent through head office.

In this case, the Ottawa district Medical Consultant received an application for out-of-country medical treatment from an Ontario physician for one of his patients in September 2001. The Consultant adjudicated the application and denied the request, as the requirements for funding had not been met. Ottawa district office support staff produced a specific denial letter under the direction of the Consultant. The letter was properly addressed, and sent to the patient and attending physician. However, a copy of the letter was also mistakenly sent to Person C.

During its investigation, a Medical Consultant responsible for the Out-of-Country Prior Approval Program reviewed the files pertaining to both the affected person and Person C. It was determined that an error likely occurred with the affected person's copy of the denial letter being placed in an envelope addressed to Person C. As noted earlier, the affected person was notified of this mistake and provided with two letters of explanation and apology.

The Provider Services Branch reviewed its policies and procedures and subsequently implemented the following changes to avoid a similar error from reoccurring:

- Window envelopes will be used to prevent improper labelling or typing of envelopes.
- All out-of-country approval letters will continue to be produced, tracked and mailed from the Kingston head office.
- All out-of-country denial letters will now be produced, tracked and mailed from the Kingston head office, rather than from the district offices as done previously.
- As there is no legislative or other requirement to send patients a copy of the decision letter, this practice has now been stopped. Decision letters will continue to be sent directly to the attending physician, as required.

The Director also advised that all Ministry and government guidelines for the protection of privacy would continue to be followed.

DISCUSSION:

With the exception of Trillium's computer error problem, it appears that the breaches of personal information by both Branches of the Ministry occurred as a result of human error. As noted above, each Branch has now reviewed its existing policies, particularly with respect to mailing-

out procedures for documents containing confidential information. I am satisfied that necessary steps have been implemented to ensure the protection of personal information in the future and to prevent similar incidents from reoccurring. The Director of Provider Services and the Manager of Trillium should both be commended for taking the initiative to revise their office policies in this regard.

However, a matter that concerned me greatly during my investigation into these incidents was the way in which Ministry staff, at varying levels, initially responded to these privacy breaches. For reasons discussed below, I believe the responses were inadequate, and indicate a need for Ministry staff to become educated about how to properly respond to a privacy breach.

Learning of a Privacy Breach

Once an institution learns that a possible privacy breach has occurred, immediate actions should be taken. In a publication entitled "*A Privacy Breach Has Occurred – What Happens Next?*" the IPC has suggested the following actions to assist in controlling a privacy breach:

- Identify the scope of the breach and take steps to contain the damage (for example, this may involve retrieving hard copies of personal information that have been disclosed, determining whether the privacy breach would allow unauthorized access to an electronic information system, changing file identification numbers);

- Ensure that appropriate institution staff is immediately notified of the breach, including the FOI Coordinator, the head and/or delegate;

- Immediately inform the IPC of the breach;

- Notify individuals whose personal information has been disclosed;

- Conduct an internal investigation into the matter, report on the findings and quickly implement any recommendations. The objectives of this investigation should include a review of the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal information;

- Address the situation on a systemic basis. In some cases, program-wide or institution-wide procedures may warrant review, such as in the case of a misguided fax transmission. Ensure that policies, procedures and staff training are adequate across the board.

It is clear that in *all* of the above privacy breaches, Ministry staff initially overlooked most of these necessary steps. In incident #2, the documents were not retrieved from the recipient, nor was there any follow-up to ensure they had been properly contained. The affected person was not notified of this incident until well over two months later, and only after direction from the IPC. In addition, neither the FOI Co-ordinator, nor the IPC were advised of this incident, and there was no internal investigation or review of the program's policies until after an investigation was initiated by the IPC.

In incident #3, the documents were not retrieved from the recipient and no follow-up was done to ensure they had been properly contained. The affected person was not notified until two months later, and only after direction from the IPC. Although a meeting was held to remind staff about the importance of confidentiality, neither the FOI Co-ordinator nor the IPC were immediately notified of this incident.

In incident #4, the documents were not retrieved from the recipient and, again, no follow-up was done to ensure they had been properly contained. The affected person was not notified until approximately six months later, and only after direction from the IPC. In addition, neither the FOI Co-ordinator nor the IPC were advised of this incident, and there was no internal investigation or review of the program's policies until after an investigation was initiated by the IPC. The Ministry also points out that neither the Director, Manager or the Medical Consultant responsible for the Out-of-Country Prior Approval Program were aware of the privacy breach until the incident was revealed approximately six months after the breach occurred. It has not been determined who the recipient initially contacted in the Ministry, nor have the details of any conversation been determined. It should be noted that once the Director, Manager and Medical Consultant were made aware of the privacy breach, they made immediate and extensive efforts to contain the breach and notify affected parties.

With respect to Trillium's computer error problem, it is evident that the Ministry took steps to conduct an investigation and to initiate both interim and permanent corrective measures to the problem. However, it appears that the documents were not retrieved from the recipients who contacted the program, nor were all of the affected persons made aware of this incident. Furthermore, the FOI Co-ordinator and the IPC were not notified about this problem until a year later, as a result of the IPC's investigation into other incidents.

CONCLUSIONS:

I have reached the following conclusions based on the results of my investigations:

1. The information relating to incidents 2, 3 and 4 was personal information as defined in section 2(1) of the *Act*.

2. The disclosure of the personal information was not in compliance with section 42 of the *Act*.

3. The disclosures were inadvertent, through human error. The Ministry has taken appropriate measures to ensure the protection of personal information in the future and to prevent similar incidents from reoccurring.

4. The Ministry's initial responses to the disclosures were inadequate, and I will therefore recommend changes to the Ministry's policies and procedures to address this issue.

RECOMMENDATIONS:

1. I recommend that the Ministry create a policy outlining the procedures that should be followed when a privacy breach occurs.

2. I further recommend that the Ministry take appropriate actions to ensure that all staff are notified and educated about these procedures.

By **March 12, 2003**, the institution should provide the IPC with proof of compliance with the above recommendation.

December 12, 2002

Shaun Sanderson
Mediator