OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report PH-2012-001

April 30, 2012

Summary: A Complainant filed a Privacy Complaint with this Office against a massage therapist as a Custodian under the *Personal Health Information Act* ("*PHIA*"). The Complaint alleged that the Custodian lost a file containing the Complainant's personal health information. The Commissioner found that the Custodian breached sections 13, 15, 19 and 20 of *PHIA*, as she failed to meet the obligations set out in *PHIA* for the protection of personal health information and has no policies and procedures in place regarding her collection, use and disclosure of personal health information, nor any of the required notice materials. The Commissioner recommended that the Custodian take immediate steps to safeguard the personal health information in her possession, develop and implement the proper policies and procedures and post or provide notice materials as required by *PHIA*. The Commissioner also recommended that the Custodian complete the *PHIA* Online Education Course offered by the Department of Health and Community Services.

Statutes Cited: *Personal Health Information Act*, S.N.L. 2008, c. P-7.01, sections13, 15, 19 and 20.

File # 0185-060-11-001

I BACKGROUND

[1] On July 15, 2011 this Office received a Privacy Complaint under the *Personal Health Information Act* ("*PHIA*") with respect to an independent massage therapist, who is a custodian as defined in *PHIA*. Section 66(3) of *PHIA* states as follows:

> *66(3) Where an individual believes on reasonable grounds that a custodian has contravened or is about to contravene a provision of this Act or the regulations in respect of his or her personal health information or the personal health information of another, he or she may file a complaint with the commissioner.*

[2] The Complainant alleged that her personal health information had not been adequately protected, as a file containing her personal health information had been lost by the massage therapist (the "Custodian"). While this Office has always named public bodies in reports issued under the *Access to Information and Protection of Information Act* (*ATIPPA*"), I have decided not to do so in this particular case for several reasons. First of all, this is the first complaint we have received under *PHIA* and at the time the complaint was made, the legislation had been in force for less than three months. Secondly, the enactment of *PHIA* meant that for the first time, private businesses and individuals (as custodians) were subject to provincial health privacy legislation. So, given that the legislation was new and that this complaint is against an individual custodian who was not previously bound by provincial privacy legislation, I am not naming the Custodian. I reserve the right to reverse that decision by reporting the name of the Custodian in my 2012-2013 Annual Report if the Custodian has not adequately responded to my recommendations. However, *PHIA* has now been in force for a year, and all custodians have now had ample opportunity to familiarize themselves with its provisions and take appropriate measures to ensure they are compliant. In future reports, custodians will normally be named, whether they are an individual, a business or a public institution.

[3] On July 25, 2011 this Office wrote to the Custodian and formally advised her of the complaint. An investigator from this Office spoke with the Custodian briefly by telephone and explained the investigative process. On August 25, 2011, another letter was sent to the Custodian requesting information with respect to the Custodian's information handling and storage practices and any policies and procedures relating to information management. Unfortunately, there was no response to the second letter, despite several unsuccessful attempts to contact the Custodian by telephone and

letters sent (by courier) in November 2011 and January 2012. Finally, in early February 2012, this Office prepared and served a Summons to Witness on the Custodian and on February 13, 2012, the Custodian attended at our Office and provided the information necessary for us to proceed with our investigation and Review.

IV DISCUSSION

[4] The Custodian admitted that a portion of the file containing the Complainant's personal health information had been lost, and she was unsure how or when the information was lost. In terms of her filing and information storage practices she informed us that she has a locked filing cabinet at home where she stores patient files. Patient files consist of paper records, and the only electronic files she has consist of reports that she would prepare if required to do so by a client. These reports are prepared on her personal computer, which is password protected. On a daily basis, the Custodian retrieves treatment notes for all her patients for that day and brings them to her place of work. At the end of the day, she brings the treatment notes back home. She uses a messenger bag/briefcase to transport the files.

[5] The Custodian informed us that there is no space for a filing cabinet in her treatment room at her place of work. However, outside of her treatment room, she has a drawer and a wall mounted folder that are located in an area that is shared with the other practitioners who work at this clinic. During the day, the Custodian's treatment notes are either kept in this drawer which is unlocked, or in the wall mounted holder in the common area. The Custodian stated that when she uses the wall holder she places files so that the names on the files face the wall.

[6] The purpose of *PHIA* is set out in Section 3 as follows:

> *3. The purposes of this Act are*
>
> *(a) to establish rules for the collection, use and disclosure of personal health information that protect the confidentiality of that information and the privacy of individuals with respect to that information;*
>
> *(b) to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in this Act;*

> *(c) to provide individuals with a right to require the correction or amendment of personal health information about themselves, subject to limited and specific exceptions set out in this Act;*
>
> ***(d) to establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control;***
>
> *(e) to provide for an independent review of decisions and resolution of complaints with respect to personal health information in the custody or control of custodians; and*
>
> *(f) to establish measures to promote the compliance with this Act by persons having the custody or control of personal health information.*
>
> [Emphasis added]

[7] The mechanisms referred to in section 3(d) are set out in sections 13 to 22 and also in sections 37 and 48 of *PHIA* and can be briefly summarized as follows (please note that this list is neither exclusive nor exhaustive):

- Where the custodian is not a natural person, a contact person must be designated to respond to requests from the public and facilitate the organizations' compliance with *PHIA*. A Custodian that is a natural person can either perform these functions him/herself or may designate another person as the contact person (s. 18).
- Oaths of confidentiality must be taken by all employees, agents, contractors and volunteers, and they must be made aware of and comply with the obligations set out in *PHIA* as well as the custodian's policies and procedures (s. 14).
- Information managers (as defined in s. 2(1)(l) of *PHIA*) must enter into written agreements with custodians and must be compliant with *PHIA*. Employees of information managers must also agree in writing to comply with *PHIA* and the agreement entered into by the custodian and information manager (s. 22).
- Detailed privacy and security policies and procedures must be developed and implemented by the custodian to protect the confidentiality of the information, restrict access to personal health information to only those who have a need to know, and ensure reasonable steps are taken to protect the information against theft, loss and unauthorized access, use or disclosure (s. 13, s. 15).

- The custodian must ensure employees, agents, contractors and volunteers are aware of their obligations under *PHIA* and the policies and procedures of the custodian (s. 14).
- The custodian must make available to the public a written statement regarding its information handling practices, including how to access one's own personal health information and how to make a complaint to this Office(s.19).
- The custodian must provide to clients or post in a conspicuous area notice of the purposes for which personal health information is collected, used and disclosed (this ensures that consent is knowledgeable) (s. 20).
- The custodian must keep records/logs of disclosures (s. 48).
- The custodian must implement a process for managing limited consent requests (s. 37).
- The custodian must have a plan in place to deal with privacy breaches (s. 13 and 15).

[8] In the circumstances of this case, not all of the above are relevant. Here the custodian is a natural person, and there are no employees, agents, contractors or volunteers; nor is there an information manager. Therefore, the agreements noted above as well as the privacy training sessions are not necessary. However, the Custodian does have an obligation to educate herself about her obligations and take the necessary steps to become complaint with *PHIA*. Unfortunately, it appears that she has not done so.

[9] First of all, the Custodian informed us that she has no privacy and security policies as required by section 13. This is the first step in turning one's mind to the protection of the personal health information that one holds. The Department of Health and Community Services has created resources to assist custodians of personal health information to meet their obligations under *PHIA*, one of which is a "Policy Development Manual". This can be found at http://www.health.gov.nl.ca/health/phia/index.html#policy. This manual takes the legal obligations set out in *PHIA* and transforms them into a policy framework. It also provides sample language to assist custodians in developing and implementing their own policies and procedures.

[10] Similarly, the Custodian has no notice materials posted as per sections 19 and 20 of *PHIA*. Notice materials are meant to inform the public about the custodians' reasons for collecting, using and disclosing personal health information. Sample notice materials are also available on the above

noted website, and consist of a poster-type document and a brochure, which contains more detailed information than the poster. Both of these resources could be easily adapted by custodians to meet the requirements of *PHIA*.

[11] Further, the Custodian has inadequate security arrangements in place to protect the personal health information in her possession against theft, loss or unauthorized disclosure. While the files stored at her home are kept in a locked filing cabinet, this is not the case at her place of work. The Custodian's place of work is comprised of a shared office space and a private treatment room. Records containing personal health information are not stored at her workplace but are carried back and forth from her home to her place of work in a simple zippered messenger bag. Records brought to her place of work are stored, for the day, in a wall folder or in an unlocked desk drawer. I would again refer the Custodian to the website noted above, which also contains a *PHIA* "Risk Management Toolkit". The Toolkit comprises a series of self assessment tools designed to help custodians to understand the requirements set out in *PHIA* with respect to safeguarding personal health information, and help custodians evaluate their level of compliance by looking at the different types of safeguards they currently use and identifying areas for improvement. It contains an information security management overview, a privacy checklist, privacy breach guidelines, a privacy breach reporting form and other resources. These are all excellent tools to help custodians become *PHIA* compliant.

[12] In terms of safeguarding personal health information in this particular case, the best case scenario would be to keep all the personal health information at the place of work, in a locked filing cabinet. That way, information would not need to be continuously transported back and forth, thus minimizing the chance of loss. However, when or if paper records must be carried back and forth, a briefcase with a lock is a better option, as this offers some extra protection at a very low cost, and is in keeping with the "reasonable" security measures required by the legislation. Records must also never be left unattended in public places. Many instances of stolen patient records have occurred through a vehicle break-in. If electronic records are to be transported by custodians, the device used to do so must be encrypted.

[13] As noted above, a locked filing cabinet in the place of work is essential as a reasonable security measure. Recognizing that many small or independent custodians will share office space, having a locked filing cabinet for each custodian in which they can place their own files offers much better protection than a wall folder or an unlocked drawer, and again, this measure is inexpensive and easy to avail of. Files could then be removed from the cabinet as needed and returned immediately after the treatment session. Further, if the Custodian is going to be working on client files at home, on her home computer, this information should be stored separately in an encrypted folder so that only the Custodian (and not family members or houseguests, etc.) can access it.

[14] *PHIA* compliance need not be costly or complicated. Independent and smaller custodians, with the help of the materials on the Department of Health and Community Services website, can largely accomplish this alone, with little or no outside assistance. Colleges, boards, and associations representing health professionals may also choose to assist their members in developing resources. Larger custodians with more complicated business lines may require legal assistance to draft agreements and contracts with third parties or to develop specialized policies and procedures. However, large or small, custodians must turn their minds to their obligations as set out in *PHIA* and ensure they are taking appropriate steps to safeguard the personal health information they hold. In the present case, the most basic of security measures are absent, and this simply is not good enough.

V CONCLUSION

[15] The Custodian has clearly failed to meet the obligations set out in *PHIA* for the protection of personal health information. Further, she has no policies and procedures in place regarding her collection, use and disclosure of personal health information, and she has none of the required notice materials. As such, it is my finding that the Custodian has breached sections 13, 15, 19 and 20 of *PHIA*.

[16] Finally, the Custodian's initial non-cooperation with this Office was troubling, and we had to avail of alternative legal options to secure her participation in this investigation. Custodians are advised that this Office will not hesitate to use all the legal options at our disposal to ensure that Custodians will not be able to unduly delay an investigation.

VI RECOMMENDATIONS

[17] In light of the foregoing, under the authority of section 72(2) of *PHIA*, it is my recommendation that the Custodian take immediate steps to:

1. develop and implement detailed privacy and security policies and procedures to protect the confidentiality of the personal health information in accordance with section 13 of *PHIA*;
2. implement appropriate measures to safeguard the personal health information in her possession in accordance with section 15 of *PHIA*, such as storing files in a locked filing cabinet both at home and in the workplace; keeping files at the workplace and only transporting them when absolutely necessary using a locked briefcase or an encrypted mobile device;
3. develop and post/provide the proper notice materials regarding information handling practices, including how to access one's own personal health information and how to make a complaint to this Office, and the purposes for which personal health information is collected, used and disclosed in accordance with sections 19 and 20 of *PHIA*.

[18] It is also my recommendation that the Custodian undertake the *PHIA* Online Education Course offered by the Department of Health and Community Services, which can be found at http://nlchi.lms.saiglobal.com/default.ashx .

[19] The Custodian should endeavor to have these tasks completed within 60 days of receiving this Report, and this Office will initiate follow-up with the Custodian to ensure these obligations are fulfilled.

[20] Under the authority of section 74(1) of *PHIA*, I direct the Custodian to write to this Office and the Complainant within 15 days of receiving this Report to advise of her decision regarding the recommendations in this Report.

[21] Dated at St. John's, in the Province of Newfoundland and Labrador, this 30th day of April 2012.

E. P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador