REPORT OF THE COMMISSIONER'S FINDINGS

Personal Health Information Privacy and Access Act

Breach Notification Matter: 2011-423-H-136
Complaint Matters: 2011-491-H-151, 2011-492-H-152, 2011-494-H-153, 2011-495-H-154, 2011-497-H-156, 2011-502-H-157, 2011-508-H-158, 2011-516-H-161, 2011-522-H-164, 2011-569-H-182, 2011-591-H-190

Date: February 9, 2012
Office of the Access to Information and Privacy Commissioner of New Brunswick

Privacy Breach Incident

Doctor S. Sanderson is a Pediatric Endocrinologist and a member of the Pediatric Department at the Out Patient Clinic of the Saint John Regional Hospital ("the Hospital"). She is a salaried physician employed by Horizon Health Network. In November 2010, Dr. Sanderson's Administrative Assistant realized that a USB key used to store back-up patient health information was missing.

As a foreground to this case, some 5 to 6 years ago, Dr. Sanderson's office created a patient information database. The database includes personal health information of children who Dr. Sanderson has treated over the last 15 to 16 years. There were approximately 1600 patients in this database. This database was stored on Dr. Sanderson's main desk computer, a computer integrated into the Hospital's information technology system.

In order to serve her patients, Dr. Sanderson's office had to retrieve information from the database. Specific administrative tasks such as organizing visits, appointments, testing and follow-up with her patients required a computer program supporting those needs. In other words, Dr. Sanderson's office needed a data management program. The information technology services offered by the Hospital, however, did not support the use of a data management software program. In fact, it was common practice at the Hospital to employ the computer program Excel to manage data for physicians' particular needs in serving their patients. Dr. Sanderson's office opted to use the Excel program to create this patient information management database. The database was used by Dr. Sanderson's Administrative Assistant as a work plan for booking patient appointments and follow-up tests.

Excel was found not to be the most efficient program for the maintenance of a patient database, and this led Dr. Sanderson's staff to proceed with a back-up the medical data on a secondary source. A flash drive was chosen for that purpose. The USB key flash drive ("flash drive") was used only as a back-up secondary source.

A second reason the patient health information was backed up on the flash drive was to retrieve the information during times when the Hospital's secure system (i.e., that of Horizon Health Network) could not be accessed. Dr. Sanderson and other physicians stored data on their office computers and it was backed up regularly on the Hospital's main server. Dr. Sanderson's staff could continue to work on the Excel program during these downtimes only by accessing the flash drive's data.

It was believed that the flash drive in this case stored data from approximately 900 patients, and included the patient's name, name of patient's parents, address, phone number, date of birth, Medicare number, diagnosis, appointment dates and follow-up testing. It was not possible to ascertain which 900 of the total number of patients were affected.

According to Dr. Sanderson's Administrative Assistant, a back-up of the Excel work plan containing patient information was regularly performed every 1 to 2 months on the flash drive. The last back-up is believed to have been done in August of 2010 and the next back-up would have been performed in October. The Administrative Assistant reported only having had an opportunity to do so around the Remembrance Day holiday in November of 2010 and this is when she could not locate the flash drive and realized it was missing. Accordingly, it is unclear when exactly the flash drive went missing.

Commissioner's Investigation

Why the delay?

When Dr. Sanderson's Administrative Assistant realized that the flash drive was missing in November 2010, she notified Dr. Sanderson. Dr. Sanderson does not recall this first notification but she trusts that she was notified. During this investigation, Dr. Sanderson did admit to not having paid attention to this notice and as a result, she did not act on the matter in November of 2010.

Meanwhile, Dr. Sanderson's staff, along with three other staff members from other physicians' offices in the Pediatric Unit, assisted in trying to locate the missing flash drive in the room. This collaborative effort remained unsuccessful. It was not until nine months later in August of 2011 that the Administrative Assistant reminded Dr. Sanderson that the missing flash drive could not be found. This is when Dr. Sanderson took notice and immediate action.

Further efforts were undertaken to find the missing mobile device, but to this date the flash drive has never been located.

Why did the breach occur?

Upon being notified in August of 2011 that the flash drive was still missing, Dr. Sanderson informed the Hospital's Nurse Manager of the incident who in turn contacted the Chief Privacy Officer for Horizon Health Network. The next day, the Hospital's Executive Management Team, the Chief Privacy Officer for the Department of Health, and the Access to Information and

Privacy Commissioner's Office were notified. The Chief Privacy Officer met with Dr. Sanderson and the Nurse Manager to undertake their investigation.

The Commissioner met with the Hospital's Executive Management Team, Dr. Sanderson and her Administrative Assistant, and Horizon Health Network's Chief Privacy Officer to gather the facts of the incident. Discussion took place regarding why and how the privacy breach occurred. The Commissioner also visited the office and general area where the flash drive went missing.

At the time of the incident, Dr. Sanderson's office was separate from that of her Administrative Assistant. The latter was located off a main corridor of the Hospital in a room with three administrative assistants of other physicians. This room had two doors: the main door which was opened during working hours; and, a second door at the opposite end which remained closed. Neither of these doors were not locked during the day, even when staff were not present. The staff's desks were situated behind open-concept cubicles and therefore were easily accessible to anyone who entered. This shared office area was used by patients who signed in for their appointments, and staff members who accessed a printer (designated as a central location to pick up any printed materials). In addition, this same room served as a common area for staff with access to a refrigerator and coffee.

According to facts obtained, the two doors to this room were normally closed when staff left at the end of their shift (at 4 pm); however, from 4 pm until approximately 8 pm during the week, the room remained unlocked with no staff present. Security personnel making regular rounds on the unit where the room was located would verify that both doors were locked during evenings, nights, weekends, and holidays.

The flash drive in question was kept in the Administrative Assistant's desk in an unlocked drawer. The information stored on said flash drive was neither password protected nor encrypted.

Notification to affected patients

The Commissioner provided assistance to Dr. Sanderson and Horizon Health Network in ensuring that all patients affected by the privacy breach were notified as quickly as possible. In that regard, Dr. Sanderson's office identified the current list of patients whose personal health information was contained in the database. There were 1513 patients.

Notification to all these patients was carried out in early September of 2011. The notification letters advised of the right to file a complaint with the Commissioner under the *Personal Health Information Privacy and Access Act* ("the *Act*"). Of the several hundred notified, we know that a number contacted Dr. Sanderson and Horizon Health Network directly. We received inquiries, complaints and concerns from 25 individuals. Among those who contacted our Office, 11 individuals filed formal complaints under the *Act*. The complaints are described below.

Complaints of affected individuals

When a person is concerned that his or her personal health information may have been compromised, that person has the right to file a complaint with the Commissioner under subsection 68(2) of the *Act*. The Commissioner has 90 days within which to conduct her investigation and file a report on findings.

Our Office received complaints from parents whose children's personal health information had been lost as a result of this incident. Most of the complaints were filed in late September, and some in November of 2011. In the present case, the 90-day deadline was extended to the date of the present Report of Findings. This was necessary in order for us to complete a thorough review of the circumstances surrounding the privacy breach incident.

In the main, the complaints raised these questions:

a) What were the reasons for the serious delay in being notified of the privacy breach?
b) Why was medical information stored on a memory stick that was neither password protected nor encrypted?
c) What actions are being taken to correct the breach and to prevent similar future incidents?
d) Could loss of personal information, including that of a child, lead to identity theft and affect one's financial history?
e) Is there a need to obtain a new Medicare number?

These questions are dealt with in turn in our findings below.

Serious delay in notification

The answer to the first question was elaborated at the beginning of this Report. The significant delay in notification of this privacy breach incident, i.e., between November of 2010 and August of 2011, was solely the result of Dr. Sanderson not having paid attention to staff when being advised that a flash drive containing patients' personal health information had gone missing.

Section 49 of the *Act* provides when notification of a privacy breach must be made:

> 49(1) A custodian shall...
> (c) notify the individual to whom the information relates and the Commissioner in the manner prescribed by the regulations at the first reasonable opportunity if personal health information is
> (i) stolen,
> (ii) lost,
> (iii) disposed of, except as permitted by this Act, or
> (iv) disclosed to or accessed by an unauthorized person…

The *Act* obligates custodians to protect personal health information and given the highly sensitive nature of personal health information, individuals have the right to know when their personal information has been compromised. Consequently, the privacy breach notification rules found in section 49 are mandatory and notification can only be disregarded in specific limited circumstances (as set out in subsection 49(2)). Those exceptions were not applicable in this case.

As per section 49, notification must be made as soon as possible. The notification process is designed to keep custodians accountable when a breach has occurred and to provide assistance to individuals whose information has been compromised by reducing the harm which may come to them as a result of the breach.

In this case, the loss of the flash drive which was neither password protected nor encrypted clearly gave rise to the obligation to notify at the first reasonable opportunity. That opportunity was November of 2010, but notification did not take place at that time. Accordingly, Dr. Sanderson failed in her duty to notify the affected individuals and the Commissioner as required by section 49 of the *Act.*

Having said this, when Dr. Sanderson was reminded in August of 2011 that the flash drive was still missing, she took notice and immediate action to notify all her patients.

Storage of patient medical information on a flash drive

This matter relates to the general rule regarding the protection of personal health information which is found in section 50 of the *Act* entitled *Security Safeguards*:

> **50**(1) In accordance with any requirements prescribed by the regulations, a custodian shall protect personal health information by adopting information practices that include

> reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.
>
> **50**(2) The information practices referred to in subsection (1) shall be based on nationally or jurisdictionally recognized information technology security standards and processes, appropriate for the level of sensitivity of the personal health information to be protected.
> (…)
> (*e*) ensure agents of the custodian adhere to the safeguards.
>
> **50**(4) A custodian who maintains personal health information in electronic form shall implement any additional safeguards for the security and protection of the information required by the regulations.

A *custodian* is a health care provider, and can be a physician, a nurse, a hospital, and so on. Both Dr. Sanderson and Horizon Health Network are custodians and both have a duty to protect personal health information as imposed upon them by section 50.

Section 50 emphasizes the importance of protecting personal health information at all times through safeguards, which must keep the information confidential, integral, accurate, and as in the present case, secure. More precisely, section 50 demonstrates a pragmatic way to implement safeguards by referring to two standards: that of reasonableness and level of sensitivity of the information.

The first standard calls for safeguard measures to be reasonable, which means to keep the information secure using safeguards that are reasonable from an objective viewpoint and not according to personal choices. Reasonableness does not mean that security safeguards have to be perfect but should be reasonable in the circumstances. For instance, a file containing patient medical records (in paper format) rests on top of a desk and it is open as the custodian reviews its contents. The custodian leaves the office for lunch, but does not put away the file as her staff remains present. During the lunch hour, a person accesses the office to repair the custodian's printer and to do regular maintenance of that machine. The patient's personal information is clearly visible. The custodian believes that the patient file is secure within her office, where the public does not enter, and safe because staff were present. Therefore, from the custodian's subjective viewpoint, the patient file was safe. From an objective viewpoint, however, it is clear that the patient file was not safe as it can be viewed and accessed by the repair technician. This measure was not reasonable. A visit by the repair technician should

have prompted the custodian or her staff to put away the file before the repair technician was able to enter the office. This measure would be reasonable.

It serves to mention that reasonable security measures can also be derived from common sense. Locked doors and drawers are in many cases effective security safeguards. Regrettably, it is often the lack of attention to practices used every day in our workplaces which present the greatest security concerns.

The second standard calls for safeguards to be determined in conjunction with the level of sensitivity of the information. The higher the level of sensitivity of the information, the higher the level of security required. Again, circumstances will determine which level of security measures are reasonably needed to protect personal health information in each case. For example, a list containing just the names of individuals who are participating in a health survey will not demand the same level of security as a list containing medical diagnoses of the same individuals.

Furthermore, whenever electronic devices are used to store personal health information, the *Act* requires a heightened degree of caution and obligates custodians to adopt additional security measures. These are found in section 20 of the *Act*'s *Regulation 2010-112*. Section 20 also includes other physical, technical and administrative security safeguard measures:

> **20**(1) A custodian shall establish and comply with a written policy and procedures with respect to information practices for the protection of personal health information containing the following requirements:
> (*a*) measures to protect the security of personal health information during its collection, use, disclosure, storage and destruction;
> (*b*) measures, for example by the use of passwords and encryption, to ensure that removable media used to record, transport or transfer personal health information is appropriately protected when in use;
> (*c*) measures to ensure that removable media used to record personal health information is stored securely when not in use;
> (*d*) measures to ensure that personal health information is maintained in a designated area and is subject to appropriate security safeguards;
> (*e*) measures that limit physical access to designated areas containing personal health information to authorized persons;

> (*f*) procedures that provide for the recording of security breaches; and
> (*g*) corrective procedures to address security breaches.
>
> **20**(2) A custodian shall keep a record of all security breaches by recording the security breaches and corrective procedures taken to diminish the likelihood of future breaches.

As in the case of the reasonable security safeguards referred to in section 50 above, the *Regulation*'s additional obligations make custodians aware of the additional requirements for personal health information in electronic format. Passwords and encryption for data stored electronically is mandatory and these measures have become the norm in our highly technical and integrated professional world of portable computers, wireless networked systems, and other mobile electronic devices such as flash drives.

In the present matter, given the sensitivity and amount of personal health information contained on the flash drive used by Dr. Sanderson's office, we are of the view that it was reasonable to demand a very high standard of security safeguards. By contrast, the security of the information was not ensured as evidenced by these facts:

- The use of a portable flash drive to store highly sensitive patient information;
- The flash drive was not password protected or encrypted;
- The flash drive was stored in an unlocked drawer in an unlocked room sometimes unattended and often accessible by the public; and,
- The handling and storage of highly sensitive patient files in an unlocked room sometimes unattended and often accessible by the public.

For these reasons, we find that the information practices adopted and used by Dr. Sanderson's office and Horizon Health Network at the time of the breach did not meet the standards required of custodians for the protection of personal health information and were not in compliance with the *Act*. In this regard, Dr. Sanderson and Horizon Health Network failed in their duty to have the required security safeguards to protect the personal health information of their patients as required by the *Act*.

Corrective measures to prevent similar future privacy breaches

Storing data on mobile electronic devices

This breach incident has brought about a thorough review of Horizon Health Network's policies and practices regarding the storage of health records data. These new policies and practices are meant to prevent the loss of personal health information such as described in the present case.

We have been advised that Horizon Health Network is developing a USB Storage Device Policy. The Chief Privacy Officer for Horizon Health Network undertook in October 2011 an assessment to identify the various ways sensitive health information is being stored throughout the entire Horizon Health Network. This assessment and accompanying questionnaire are designed to look into current storage methods of sensitive data in order to develop better practices and standards to ensure the proper protection of the information.

In cases where the use of such devices is necessary, encryption will be made mandatory. New measures will be created to replace existing practices of storing medical files on mobile electronic devices such as a flash drive or USB key. These new measures include:

- restrictions on use of mobile devices to store confidential, personal information, and personal health information;
- use of passwords;
- approval before use of these devices;
- encryption of these devices;
- storage of these devices in locked quarters when not in use; and,
- a ban on use of such devices as a means to back-up data.

We have also been informed that Dr. Sanderson's patient health information used on the Excel database will no longer be stored on a USB key and that this data will continue to be backed up only on the Horizon Health Network's secure network. Other staff members working in the same clinic at the Hospital were informed of this decision.

The Chief Technology Officer for Horizon Health Network is currently assisting with the development of guidelines for the creation of databases and necessary safeguards to protect such information as well as addressing the issue of the use of portable media.

Moreover, information handling practices have been reviewed with Dr. Sanderson and her staff.

The Commissioner will be kept informed of these developments to ensure that they incorporate the requirements of the *Act*'s security safeguards.

New offices

In February 2011, and thus prior to the notification of this privacy breach matter, Dr. Sanderson's Administrative Assistant moved to a new office. This new work location is next to Dr. Sanderson's office, away from the previous busy environment that was accessible to patients and staff. The Administrative Assistant now has her own work space with storage for patient files. Arrangements were to be made to provide her with a locked drawer or locked cabinet in which to store patient charts handled on a daily basis.

The new office should provide an environment where personal health information is secure. The office is accessible through one door, which is locked whenever the Administrative Assistant leaves her work area.

Loss of personal information and identity theft

In this matter, one of the main concerns brought to our attention was the risk of identity theft. The loss of personal health information belonging to Dr. Sanderson's patients could lead to identity theft. The information lost in this case included patients' names, date of birth, Medicare number, address, and so on. While it is impossible to determine with any degree of certainty the risk to an individual when his or her personal information has been compromised, it cannot be assumed that there is no risk and the loss of information should be taken seriously. With each additional piece of identifying information that is compromised, the risk of fraud and identity theft increases.

Identity thieves have many ways to get their hands on personal information, some of which include the exploitation of information lost or stolen from databases operated by both private and public organizations. There is no agreement on the meaning of "identity theft," but the term is used for everything from cheque forgery and the use of stolen credit cards to sophisticated scams in which an impostor adopts somebody else's identity to gain access to their assets.

Incorporating simple measures in a one's monthly schedule such as the following tips found below will significantly lessen the chances that personal information winding up in the wrong hands:

- Keeping track of when credit card statement is supposed to arrive, and calling the credit card company if the statement is late;
- Reviewing all credit card and bank statements to make sure there are no unauthorized purchases;
- Checking your credit report annually. Major credit reporting bureaus provide one free report each year;
- Creating a new password and changing if often for each online account on your computer. A strong password is one which is hard for anyone to guess;
- Remaining vigilant and suspicious of emails that appear to come from banks, government agencies, credit card companies which ask to provide personal information online. Real banks and other agencies do not do that, yet scammers often hijack real logos to make their fraudulent messages look authentic;
- Consulting the website of the Office of the Privacy Commissioner of Canada (www.priv.gc.ca) which offers other useful information and tips on how to report and correct the damage resulting from identity theft or related frauds.

Those affected by this breach in this case were given the contact information for credit monitoring services. It was pointed out by those monitoring agencies that the children whose personal information was lost in this breach were very young, and these children would not yet have established financial or credit history requiring such monitoring.

New Medicare cards and new Medicare numbers

In the present case of privacy breach of personal information including Medicare numbers of patients, there is no need to obtain a new Medicare number. The facts gathered in this case show that despite the USB key in question having been missing since November of 2010 (or before that time), Horizon Health Network has not received reports of inappropriate use of the personal health information contained on that flash drive.

Officials at Medicare have interpreted this fact as a minimal threat for identity theft at this time. In that regard, Medicare proceeded to follow its general rule not to automatically renew

the Medicare numbers of the affected individuals in this case. Nevertheless, upon notification of the breach, individuals were given the contact information of Medicare services and were allowed to make a request to be issued new Medicare cards.

Commissioner's concluding comments

We have been working with Dr. Sanderson, her staff, and her employer, Horizon Health Network, in relation to this privacy breach. We are confident that we have uncovered all the facts surrounding this incident, and we understand the impact of this matter upon everyone involved, including Dr. Sanderson and her staff.

Immediate attention should have been paid by Dr. Sanderson when she was first advised that the flash drive was missing. Dr. Sanderson has admittedly fully realized the ramifications for her actions, and we trust the consequences have significantly influenced her practice now and in the future. The delay in notifying affected individuals and our Office of such breaches has been addressed, and rules regarding privacy breach notification have been reviewed with Dr. Sanderson.

As indicated earlier in this Report of Findings, new measures have already been put in place to discontinue the previous unsafe methods of storing sensitive personal information such as patient medical files on mobile electronic devices unless absolutely necessary. In those exceptional cases, the flash drive must be encrypted and securely stored in locked quarters.

Additionally, a thorough review of Horizon Health Network's policies and practices regarding the storage of health records data in electronic format has been on-going since the time of this breach.

We are confident that the corrective measures proposed, once fully vetted and approved, will be implemented. Our Office will be following-up on the proposed corrective measures.

It is important to state that this case was not one which questioned the integrity of those health care professionals entrusted with the care and protection of patients' private information. We recognize that those who work in the health care field take their duty to protect personal health information very seriously; however, this incident has demonstrated that breaches can occur easily when those who should be protecting personal information rely on the convenience of routine tasks to perform our work.

Ordinary habits become such a big part of our work lives that we fail to notice that those same habits prevent us from fulfilling our duty to protect the information. This is where the problem remains. It is important to keep in mind our duty to protect personal health information at all times. Adopting convenient but less secure methods to handle the sensitive information belonging to others does not respect that duty. A lower level of vigilance, prudence and awareness invariably leads to relaxed security safeguards resulting in less protection, albeit non intentional but nevertheless tangible. This is when privacy breaches can and unfortunately do occur.

Much chagrin has been felt by all those affected by this particular privacy breach incident. Perhaps the reason for this was the obvious root cause of the incident itself: a portable small item, a flash drive, containing so much precious information, plainly left unsafe. The difficult experiences felt by all involved in and affected by the privacy breach will leave a lasting impression. Lessons derived from this incident include an increased awareness of the ease with which data can be lost and lives affected, and a renewed respect for the need to remain vigilant at all times in safeguarding the personal health information. These lessons will help rebuild the trusting relationships with those whose lives have been affected. Implementation of corrective measures will ensure that these types of incidents are not repeated.

In that regard, we have no doubt that Dr. Sanderson and her staff have learned a valuable lesson as a result of this privacy breach, an experience we know was not intended but was nevertheless occurred on their watch. We hope that this Report of Findings and accompanying recommendations will go a long way to provide answers to those affected by this privacy breach, as well to members of the general public who will continue to entrust health care professionals on a daily basis with their private information.

RECOMMENDATIONS

Based on the above findings, the Commissioner recommends as follows:

1. That Dr. Sanderson review the obligations of custodians under the *Act* and ensure that her current information practices meet these obligations;

2. That Dr. Sanderson review Horizon Health Network's policies regarding the safe use and storage of personal health information;

3. That Dr. Sanderson review with her staff the information practices used in her practice along with Horizon Health Network's policy regarding safe use and storage of personal health information;

4. That Dr. Sanderson review the requirements of breach notification found in the *Act* and that she review Horizon Health Network's policy for steps to be taken when reporting a privacy breach;

5. That Horizon Health Network continue its efforts to finalize its policy regarding safe practices for the use and storage of USB keys (flash drives) containing personal health information, and to proceed with its implementation, and that Horizon Health Network provide an update to the Commissioner when this process has been accomplished;

6. That Horizon Health Network issue an advisory to all its salaried physicians and their staff reminding them of their obligations to protect the personal health information at all times and in conformity with the *Act*;

7. That Horizon Health Network issue an advisory to all its salaried physicians and their staff reminding them of their obligation to follow Horizon Health Network's policy to report a privacy breach in accordance with the *Act*.

Dated at Fredericton, New Brunswick, this _____ day of February 2012.

_____
Anne E. Bertrand, Q.C.
Commissioner