SAFEGUARD

A quarterly newsletter published by the Office of the Information and Privacy Commissioner

Volume 7, Issue 2 May 2023

Contact Information

Office of the Information and Privacy Commissioner

3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8

Telephone:

709-729-6309

Fax:

709-729-6500

Toll Free in Newfoundland and Labrador:

1-877-729-6309

Email:

commissioner@oipc.nl.ca

www.oipc.nl.ca

This Issue:

OIPC Issues Report into 2021 Cyber Attack

On May 23, 2023, the Office of the Information and Privacy Commissioner issued its Report into the 2021 Cyber Attack. Our next Safeguard issue will feature some highlights from that Report, which contained 34 findings and six recommendations. Please review this Report which is available on our web site.

NEW Guidance – *PHIA* Toolkit for Small Custodians (Summary Part 1)

This Office released new guidance for small custodians – *PHIA* Toolkit for Small Custodians on March 31, 2023. As this guidance piece is detailed, we have broken it down into two parts and included some highlights in this newsletter - Summary Part 1 – with our next newsletter continuing with Summary Part 2. A review of the full guidance piece is still recommended.

PHIA applies to custodians who have custody or control of personal health information as a result of or in connection with the performance of their powers, duties or work. *PHIA* outlines obligations for all custodians, regardless of the size of their organization.

This toolkit is intended as a guide to help small custodians, such as individual health care professionals/practitioners and private long term care facilities, understand and comply with their obligations under *PHIA*.

At the outset, it is important to identify certain individuals within an organization and to understand how their roles are defined under *PHIA*.

1. **Custodian** - With smaller organizations, the custodian is usually the individual who is responsible for making decisions and overseeing operations. Some examples are:
   - if you are a physician in private practice, regardless of the ownership of the practice, you are typically the custodian, unless you are employed by another custodian;
   - if you are the pharmacist in charge of a pharmacy, regardless of whether you own it or not, you are the custodian;
   - if you are a chiropractor, physiotherapist, psychologist, dentist, etc. in private practice, you are typically the custodian, unless you are employed by another custodian; and
   - if you own a private long term care home, you are a custodian.

   To review the detailed definition of "custodian" please see section 4(1) of *PHIA*.

2. **Agent** - An agent under *PHIA* means a person that 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 purposes. An agent must have the authorization of the custodian to act on their behalf. Some examples are:
   - medical office assistant(s);
   - office manager(s);
   - reception/front desk staff;
   - volunteers;
   - locum physicians; and
   - trainees and students.

   To review the definition of "agent" please see section 2(1)(a) of *PHIA*.

3. **Information Manager** - An information manager is a person or body, other than an employee of a custodian, acting in the course of their employment, that processes, retrieves, stores or disposes of personal health information for a custodian or provides information management or information technology services to a custodian.

   Custodians are required to enter into a written agreement with all information managers they retain. These agreements are commonly referred to as Information Management Agreements (IMAs). This Office has just recently issued a guidance piece dealing with information managers and IMAs, Best Practices for Information Management Agreements, which is discussed later in this newsletter.

   To review the definition of "information manager" please see section 2(1)(l) of *PHIA*.

   To review the obligations and requirements of information managers with respect to IMAs please see section 22 of *PHIA*.

Custodian Obligations under *PHIA*

Custodians have many different obligations under *PHIA* and must comply with *PHIA* as there is no mechanism to "opt out" of the *Act* and its Regulations. Please review *PHIA* in its entirety to understand ALL custodian obligations. Some brief examples of sections for review are as follows:

- Information practices, policies and procedures (Section 13)

  A custodian that has custody or control of personal health information must establish and implement information policies and procedures ensuring compliance with *PHIA* and its regulations.

- Obligations of Employees, etc. (Section 14)

  A custodian is responsible for ensuring *PHIA* compliance among staff, agent(s), the information manager, contractors, volunteers, etc.

- Accuracy of Information (Section 16)

  Before using or disclosing personal health information that is in its custody or under its control, a custodian shall take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purpose for which the information is used or disclosed. A custodian must also ensure that the person to whom a disclosure is made is the person intended and authorized to receive the information.

- Contact Person (Section 18)

  A custodian must identify a contact person. If a contact person is not identified, the custodian themselves is automatically the contact person. The contact person will facilitate the custodian's compliance with *PHIA* and Regulations. The contact person must also ensure that employees, contractors, agents and volunteers of the custodian and those health care professionals who have the right to treat persons at a health care facility operated by a custodian are informed of their duties under *PHIA* and the Regulations.

- Written Public Statement (Section 19)

  A custodian must make available to those who are, or who are likely to be, affected by the custodian's activities, a written statement that provides for a contact person and a general description of the custodian's information policies and procedures. A custodian must also describes how an individual may obtain access to or request correction of a record of personal health information about the individual that is in the custody or control of the custodian.

- Duty of Custodian to Inform or Notify (Section 20)

  Where a custodian collects personal health information directly from the individual or a representative, the custodian shall take reasonable steps to inform the individual or representative of the purpose for the collection, use and disclosure of the information.

PHIA Toolkit for Small Custodian - Summary Part 2 – will be in our next Safeguard issue and will cover Security, Collection, Use and Disclosure of personal health information as well as Access and Correction of personal health information.

NEW Guidance – Best Practices for Information Management Agreements

This Office recently released new guidance – Best Practices for Information Management Agreements. We have included a brief overview below, however please review the entire guidance piece for more details.

Section 22 of *PHIA* requires custodians enter into a written agreement with all information managers they retain. In turn, an information manager must comply with *PHIA* and the terms of the agreement with respect to the personal health information disclosed to them, including only using and disclosing information as authorized by the agreement. These agreements are known as Information Management Agreements (IMAs).

An IMA will outline the terms and conditions under which personal health information is shared between the parties and the protection of the personal health information involved by ensuring compliance with *PHIA*.

This guidance is intended to help custodians be aware of their obligations under *PHIA* when entering into IMAs as well as the considerations around the protection of personal health information.

Custodians Retain Obligations under *PHIA*

Even if a custodian enters into IMAs, it is important to remember that an IMA does not relieve the custodian of their legal responsibilities and obligations under *PHIA*.

While a custodian may include terms within an IMA that relate to its own obligations, for example terms requiring an information manager to adhere to certain security measures, this does not relieve the custodian from its compliance with *PHIA*. In our example, this means the custodian remains legally responsible for ensuring there are reasonable security measures in place to protect information and, therefore, a custodian will want to ensure its due diligence when selecting a service provider. It must also be remembered that personal health information handled by the information manager on behalf of the custodian is ultimately the responsibility of the custodian.

Definition of Information Manager

An information manager is any third party that deals with a custodian's personal health information on behalf of that custodian. *PHIA* defines "information manager" in section 2(1)(l) as:

> *a person or body, other than an employee of a custodian acting in the course of his or her employment, that:*
>
> *(i) processes, retrieves, stores or disposes of personal health information for a custodian, or*
>
> *(ii) provides information management or information technology services to a custodian.*

Examples of information managers include: an entity providing information technology services (i.e. software vendors or developers); an entity providing information management services; data storage service providers; and data destruction service providers.

Disclosure to Information Managers

Prior to drafting an IMA, a custodian must consider the risks of disclosing personal health information to an information manager. The following are some examples a custodian should examine when thinking about using an IMA:

- the purpose of the information management agreement;
- what specific tasks are intended to be performed in relation to the personal health information;
- the sensitivity of the personal health information to be shared with the information manager;
- how much personal health information will be shared with the information manager and is it the minimum amount necessary;
- the security measures needed to safeguard the personal health information against unauthorized access, use, disclosure, disposition, loss or modification;
- the permitted uses and disclosures by the information manager with respect to the personal health information that are necessary for the performance of the service that is the subject of the agreement; and
- the extent of the disclosure - who within the information manager's organization needs access to the personal health information being disclosed.

A custodian may wish to consult a legal or privacy expert prior to entering into an IMA to fully canvass any privacy risks or concerns.

Creating an IMA

If a custodian is satisfied that they can address any risks associated with disclosure of the information to an information manager and wish to proceed with an IMA, our guidance contains a longer list of considerations for inclusion in an IMA.

There is no template in *PHIA* for an IMA, as each agreement will be specific to the custodian and information manager involved for the services provided. To the extent possible, an IMA should be specific, precise, and written in plain language to ensure that all terms are fully understood. It should also be flexible enough to allow for amendments and, where possible, the IMA should be published for greater transparency.

The Department of Health and Community Services' *PHIA* Policy Development Manual also contains guidance on the development of IMAs and should be consulted by custodians seeking to create an IMA.

Noteworthy Commissioner Report

The Commissioner released report PH-2023-001 on March 8, 2023.

This report involved a number of psychologists and social workers (the "Clinicians") who ended their contracts with Key Assets (KA), a social services organization. The Clinicians requested possession of their active and closed clinical files from KA, however, KA refused to transfer the files on the

grounds that the files were the property of KA and that KA was the custodian of the files under the *Personal Health Information Act* (*PHIA*).

The Clinicians filed a group complaint with our Office under section 66(3) of *PHIA*. The only issue in this Report was whether KA or each individual clinician is the custodian of the clinical files under *PHIA*.

Summary of Factual Findings

These factual findings are based on interviews with the Clinicians as well as documentation and submissions received from the Clinicians and KA.

KA provides support staff including a business support person/receptionist and an intake coordinator for the Clinicians. The Clinicians' files are kept in a cabinet in the support staff space and only the business support person/receptionist, intake coordinator, and the individual clinicians have access to the files. The Clinicians use offices in the same building where KA has offices, however, KA management occupies a separate part of the building with their own administrative staff and separate filing system.

KA is under no duty to offer work to the Clinicians and the Clinicians are under no contractual obligation to accept work from KA and are free to work elsewhere. KA knows nothing about the client except for the small amount of business and contact information held by the receptionist. KA management plays no role in the treatment plan for the client and the Clinicians do not make reports to KA management on their work with clients.

The professional fee for service was established collectively by the Clinicians and was provided to KA. The fees were not determined by KA. Under the contract with clients, all payments are made to KA via the business support person/receptionist, who does the bookkeeping for the Clinicians. Each clinician gets a monthly direct deposit from KA, consisting of the total fees with a percentage deducted by KA to cover administrative costs.

The amount paid to the clinicians is set at two-thirds of the amount billed, and KA keeps one-third of the amount as its share. KA does not withhold tax from the amount paid to the Clinicians, nor does KA provide benefits of any kind. Each Clinician is expected to provide his or her own liability insurance.

Summary of Contractual Issues

The KA Clinical Services Service Contract (the "Contract") is signed by individual clients when they first enter into the relationship with a clinician. It is a standard form that sets out the fee, the nature of the services to be provided, and some terms and conditions, such as the cancellation policy. While it states on its face that it is a contract between the client and KA, it is actually signed by the client and by the clinician, not by KA management or staff person.

The Contract explicitly states that each clinician is "at all times an independent contractor" and is not an employee of KA, but is in business on his or her own account. Therefore, the Contract with the client cannot be signed by a clinician as the agent of KA. Rather, the Contract must be deemed to be an agreement between the individual clinician and the client, for the provision of clinical services to the client.

The conclusion is clear that the Clinicians are not employees of KA, but provide professional clinical services on their own account.

Interpretation under *PHIA*

The clinical therapies that are provided to the clients meet the definition of "health care" in section 2(1)(h) of *PHIA*.

PHIA defines different kinds of "custodians" in section 4(1) and out of all the possible enumerated categories, paragraphs 4(1)(e) and 4(1)(f) could apply:

> *(e) a health care professional, when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;*
>
> *(f) a health care provider;*
>
> *[…]*

Since a custodian may be either a health care professional or a health care provider, the question is whether KA meets the definition of 'health care provider" as it is clear that that the Clinicians meet the definition of "health care professional".

> *"health care professional" means a person, including a corporation, that is licensed or registered to provide health care by a body authorized to regulate a health care professional under one of the following enumerated Acts but does not include an employee of a health care professional when acting in the course of his or her employment:*
>
> *[…]*
>
> *"health care provider" means a person, other than a health care professional, who is paid by MCP, another insurer or person, whether directly or indirectly or in whole or in part, to provide health care services to an individual;*
>
> *[…]*

It must be noted that these two definitions are mutually exclusive. A person (which under *PHIA* is defined broadly enough to include a corporation) may be a health care professional or a health care provider, but not both.

KA invoices the clients or their referring agency for the services provided to the clients, and receives the payments for those services. However, KA does not "provide health care services to an individual". The reality of the clinical relationship between the Clinicians and the clients is that it is each clinician as a "self-employed associate", not KA, who is the provider of the health care services to the client.

KA's role in the overall arrangement is that for a fee (one-third of the clinicians' billings) it provides a number of services, not to the client, but to the Clinicians, including office and meeting room space, reception and appointment-booking services, and bookkeeping, invoicing and marketing services. While KA may have the outward appearance of a health care provider, the essence of the relationship between KA and the Clinicians is that KA is simply an administrative facilitator of the work of the clinicians.

It is therefore the individual clinician who is the custodian and who has custody or control of personal health information.

Conclusion

The Commissioner concluded that the Clinicians, not KA, are the custodians of the clinical files.

The Clinicians are independent contractors and the therapeutic relationship is between the clinician and the client. That relationship is legally, and in practice, regulated and overseen by the Clinicians' own regulatory bodies under the *Psychologists Act, 2005* and the *Social Workers Act*, as well as by *PHIA*.

PHIA sets out in detail the rules that govern the collection, use and disclosure of personal health information. In Part II, it prescribes practices to protect personal health information. It is clear from the provisions of section 13 that the legal responsibility for the control of, access to, and protection and security of confidential client files, and therefore the authority to make decisions about the storage and retention of those files, rests with the custodian. The Clinicians have the right and the responsibility under *PHIA* to secure and protect the records and to control access to, use and disclosure of the information.

The Commissioner recommended that the Clinicians take steps to ensure an orderly transfer of the records to their own custody and to make all necessary arrangements to accommodate the storage and protection of their clinical files in compliance with *PHIA*.

Reminder New Provincial Health Authority

As of April 1, 2023, the four former regional health authorities and the Newfoundland and Labrador Centre for Health Information are one entity known as Newfoundland and Labrador Health Services. Please see the news release from the Department of Health and Community Services.

The Department advised that the amalgamation was a recommendation of Health Accord NL and while there is now only one health authority, a focus on specific regional issues will be maintained through the five regional health councils. The regional health councils will be responsible for advising the provincial health authority on the particular needs of the regions, informing health care delivery at the regional level.

The Department advised that patients, clients and residents can continue to access care in the same way they always have and that there are no immediate changes to health care services, facilities or contact information.

Breach Notifications

Between February 1, 2023 and April 30, 2023, OIPC received seven breach notifications from five different custodians. Some of these breaches of personal health information included: a fax that went to the wrong organization; a patient 's information scanned to the wrong chart and disclosed to the wrong patient; an email going to a group of individuals without using the bcc function; and a missing hard drive containing minimal personal health information.