S-103 CONFIDENTIALITY AND PRIVACY

In this document, the masculine gender may be used for the sake of conciseness, but it applies to everyone.

Version 5 effective February 19, 2020 (previously DG-05)

Policy

Valoris undertakes to comply with legislation governing the privacy and confidentiality of information about clients, and to take reasonable steps to protect personal information with which we have been entrusted or that is under our control against theft, loss and any unauthorized use, disclosure, duplication, modification or destruction.

Valoris manages part of the risk related to the protection of personal information, most of which is on Web databases, through a secure technology infrastructure. Those databases are monitored on a regular basis to guarantee their security.

Employees who use technology tools and provide services in either public places or Valoris offices are responsible for complying with specifications regarding the protection of personal information to minimize the risk of breach of confidentiality and privacy.

Anyone who may eventually have access to confidential information and personal information at Valoris is informed upon being hired of his responsibilities in regard to maintaining confidentiality and protecting privacy. He must certify that he understands and agrees to respect the parameters related to personal and confidential information before he is exposed to any such information. His moral and legal commitment goes beyond the end of his association with the agency: it is permanent.

In the event of a breach of privacy, steps and corrective measures will be taken to reduce the risk of recurrence, as required by the Information and Privacy Commissioner (IPC).

Procedure

1. **Oath to protect confidentiality and privacy**
   The document entitled ***Confidentiality and Protection of Privacy Declaration*** shall be signed by any person who may have access to personal information by virtue of his association with Valoris as an employee, volunteer, intern or outside consultant at the very start of that association.

2. **Notice to clients**
   An employee shall notify a client that he will collect, use or at times disclose his personal information with or without his consent if so authorized under the law, and if not, his personal information will remain confidential. An employee shall also inform a client that

the latter may request access to his personal information, and may request that certain corrections be made thereto.

An employee shall notify a client that additional information about the collection, use and disclosure of personal information can be found on the Valoris Web site and on that of the Information and Privacy Commissioner at www.ipc.on.ca .

3. Professional behaviour and attitude

An employee, student or trainee with access to the client databases is required to respect the confidentiality of all, as provided in the code of ethics. When such a person consults a client record for reasons other than as part of his functions, he is committing a breach of confidentiality and is subject to disciplinary action up to and including dismissal, or termination of his association with the agency.

An employee, student or trainee shall abstain from identifying an individual or discussing facts that could identify that individual in a public place (at or outside the agency) or a place that is accessible to the public such as a restaurant, waiting room, cafeteria or speaker phone. Such a person shall use every means to prevent the theft or loss of confidential information while in transit or at home: case notes, laptops, agendas and files. Cell phone conversations must never include information that could lead to the identification of a person.

An employee, student or trainee shall abstain from making comments in public, even if he believes that a client's situation has been covered by the media and is public knowledge.

In every service centre, clients' physical files must be stored in a water and fire-proof room that is kept locked outside of business hours. Access to those rooms is restricted to authorized persons.

Authorized persons may only consult files (physical or electronic) when necessary in the course of their duties. They must return the files to the designated areas as soon as possible. Any person accessing a physical or electronic file is responsible for safeguarding its confidentiality (for example, by locking his computer when not using it or by never leaving an unlocked physical file unattended). Staff may not remove physical documents containing personal information from a service centre unless they are under lock and key.

4. Multidisciplinary approach (integrated services)

Because of our integrated multi-service model, any given client file may contain different types of personal information that is subject to different laws.

For example, integrated services provided to a client may require that we work with him as a health care provider as well as a provider of services related to child protection. In such cases, some of the information on file is subject to the *Personal Health Information Protection Act, 2004* (better known by its acronym PHIPA) while other information will be protected under Part X of the *Child, Youth and Family Services Act, 2017 (CYFSA)*.

Because our agency combines several types of services, the integrated approach sometimes requires the agency's professional staff to share information about clients. Only pertinent and necessary information is shared. As provided under legislation, the client's consent is encouraged, but is not mandatory under certain circumstances.

Given the risk of breach of confidentiality, email, SMS and other forms of instant communication may not be used to communicate with or about Valoris clients to provide services or to communicate or receive clients' personal or personal health information. However, such means of instant communication may be used to make, confirm or cancel an appointment or to send general information about services offered by Valoris or externally.

Personal information may only be communicated by email between internal addresses.

In circumstances where a client can only be reached through such non-confidential means of communication (email, SMS, etc.), the client is to be informed of the risk presented by the use of such technologies in communicating with Valoris. If the client consents to the use of such technologies despite the risks, the client's consent will be recorded in the file. Valoris staff are to use their judgement in the use of such communication technologies to minimize the risk of breaching the client's privacy.

Staff are to use the necessary precautions to ensure the confidentiality of information visible on a computer screen: sign out of the network when away from their desk (to go to a meeting, the washroom, the printer, etc.), or use a screen saver with a password. Documents sent by fax are to be identified as "confidential".

The files of individuals who are now adults but who received mental health or other services as children may not be consulted in child protection matters without their consent.

Confidential documents may only be destroyed in accordance with applicable laws and the Valoris conservation calendar (policy *A-102 Gestion des documents et archives*).

5. Official in charge of the protection of information and privacy

Valoris' Director of Quality and Information Systems is the contact for all issues related to the proper use of personal information entrusted to Valoris under applicable laws. The functions in this regard include:

a) promoting compliance with privacy laws at Valoris (the agent);
b) ensuring that all employee agents are properly informed about their obligations under privacy laws;
c) responding to requests for information from the public about the information practices followed by Valoris (the agent);
d) forwarding to the legal team any requests from individuals requesting access or corrections to personal health information on file that concerns them and that is in the possession or under the control of the agent; and
e) receiving complaints from the public by email at PVPO@valorispr.ca about a violation of privacy laws allegedly committed by Valoris (the agent) and notify the Office of the Information and Privacy Commissioner, as required.

6. Privacy breach

Examples of confidentiality and privacy breaches include:

1) *theft of personal information* (e.g. hacking of a computer to gain access to its files);
2) *loss of personal information* (e.g. loss of a form identifying a client);

3) *unauthorized use of personal information* (e.g. talking about a case in an open and public area); or
4) *unauthorized disclosure of personal information* (e.g. sending an email to the wrong address.

As soon as an employee becomes aware of a possible breach of privacy, he must notify his immediate supervisor and send an email to PVPO@valorispr.ca with information about the situation. The employee's supervisor or the employee shall record the breach of privacy. All of these actions must take place as soon as possible, but no more than 24 hours after first becoming aware of the breach of privacy.

The supervisor shall notify the departmental director, who shall then inform the Executive Director of the situation, as set out in Policy *A-203 Situations à communiquer au directeur général.* As required, the official in charge of information and privacy shall notify the Information and Privacy Commissioner, Valoris' insurance company and the police. Depending on the nature of the breach of confidentiality, a serious occurrence report shall be filled out and sent to the Department, as set out in the policy.

It should be noted that if the privacy breach is accidental and occasional, for example information being sent to the wrong recipient, the employee, in consultation with his supervisor, shall inform the official in charge of the protection of information and privacy by email to PIPV@valorispr.ca and as soon as possible notify the individuals affected by the breach and explain the steps being taken to correct the situation. The employee will record all of this in the client's file. It is not necessary to report this to the IPC unless there is reason to believe that the breach is being used or copied without permission.

The following are the main circumstances that must be reported to the IPC:

1) Valoris determines that the breach is significant after weighing the sensitivity, volume, number of people affected and number of service providers involved;
2) the personal information was used or disclosed to a person who knew or should have known that it was released without authorization;
3) Valoris has reason to believe that the personal information was stolen;
4) Valoris has reason to believe that the personal information released was or will likely be used or disclosed without authorization or there is a pattern of similar breaches; or
5) an employee resigned or was dismissed, suspended or disciplined as a result of the breach.

On the fifth business day following the initial notification, the supervisor or the employee shall send the following information to PVPO@valorispr.ca :

1) the nature of the privacy breach (information stolen, lost or used, or disclosed without authorization);
2) the circumstances (how the personal information was stolen, lost, used without authorization or disclosed without authorization, and the date when it happened);
3) how many individuals were involved and how the privacy breach was discovered; and

4) the steps taken to bring the situation under control (e.g. the steps taken to recover the personal information) and the plans for correcting it.

Within seven business days after the initial notification, the official in charge of the protection of information and privacy shall send a letter to notify the individuals affected by the situation and their right to file a complaint with the Information and Privacy Commissioner.

If deemed necessary or useful, the official in charge of the protection of information and privacy shall conduct an internal investigation to determine how the privacy breach could be avoided in the future. He will then submit recommendations on procedural changes.

7. Public media

The agency is committed to protecting the confidentiality of client information in all contacts with the media. When a client makes a statement to the media revealing his relationship with the agency, Valoris will continue to respect its commitment to confidentiality even in situations where the information provided by the client is incorrect.

Definition

***Personal and confidential information*:**

Means information in our possession about an individual to whom we offer a service, or that could lead to the identification of the individual based on that information. The simple fact of confirming or infirming that we are offering services to that individual is also personal and confidential information. That information may be in paper, electronic, digital audio, photo, video or other form. The following are examples of personal information:

- the individual's race, national or ethnic origin, colour, religion, age, gender, sexual orientation, marital status or family status;
- the individual's medical, psychiatric, psychological, criminal or work history;
- any number, symbol or other identifying detail assigned to the individual (e.g. health card or driver's licence);
- the individual's address, phone number, finger prints or blood type;
- letters sent to Valoris by the individual that are implicitly or explicitly of a private or confidential nature, and replies to such letters that would disclose the contents of the initial letter;
- the individual's personal opinions or points of view, except if they pertain to another person;
- the points of view or opinions of another person about the individual; and
- the name of the individual when it appears with other personal information concerning him, or when disclosing the individual's name would reveal other personal information about him.

Annex

- Confidentiality and Protection of Privacy Declaration.

References

- *Personal Health Information Protection Act, 2004*
- *Child, Youth and Family Services Act, 2017* (CYFS), Part X
- *Youth Criminal Justice Act*, 2002
- *Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act, 2008*
- S-102 Accès aux renseignements personnels des particuliers et rectification
- S-104 Collection, Use and Disclosure of Personal information and Consent
- S-105 Complaints from Clients
- A-101 Communications
- A-102 Gestion des documents et archives
- RH-116 Sanctions disciplinaires
- A-301 Authorization and Use of Valoris Information Technology Systems and Data Resources

CONFIDENTIALITY AND PROTECTION OF PRIVACY DECLARATION

Name :_____

I solemnly declare and promise not to reveal any confidential information received by me for the duration of my contract/employment/term of service with Valoris for Children and Adults of Prescott-Russell, unless I am obliged to do so by the law. I also pledge to respect the principles related to the protection of privacy.

This commitment is perpetual and will remain until after I leave the organization.

_____ _____

Signature **Witness**

Dated at _____(Ontario), this _____

Day of _____201_____.