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 6 effective January 16, 2025 (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.

The organization takes the necessary measures to protect the personal or confidential information for which it is responsible.

Employees are responsible for complying with privacy guidelines to minimize the risk of breach of confidentiality and invasion of privacy.

Anyone who may potentially have access to confidential and personal information at Valoris is informed is informed of his or her responsibilities in terms of maintaining confidentiality and protecting privacy when hired. Everyone must certify that they understand and agree to respect the parameters surrounding personal and confidential information before being exposed to it. This moral and legal commitment continues at the end of the association with the agency: it is perpetual.

In the event of a privacy breach, follow-up and corrective action will be taken to reduce the negative impact of the breach, as well as to minimize the risk of reoccurrence, as required by the Information and Privacy Commissioner of Ontario (IPC).

Procedure

1. **Respect to 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 their association with Valoris as an employee, volunteer, intern or external consultant at the beginning of that association.

2. **Notice to clients**
   Unless otherwise provided by law, the consent of any individual about whom personal information is to be collected is obtained prior to collection. The person concerned is informed of the purpose of the collection and the intended use of the information. The employee must also inform the individual that he or she may request access to his or her personal information, and that he or she may request that certain corrections be made.

The employee must advise the customer that more information about the collection, use and disclosure of his or her personal information can be found on the Valoris website or on the website 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.

Personal, confidential or identifying information must not be mentioned in public places or in any other circumstances where the information could be overheard or intercepted by unauthorized persons. Measures must be taken to prevent theft or loss of confidential information during transport or storage. For example, physical documents must be transported and stored under lock and key, while electronic documents must be protected by encryption, passwords, biometric keys or other approved technologies.

The people concerned must refrain from mentioning personal or confidential information of which Valoris is the custodian in the presence of unauthorized persons, even if they believe that the situation is known to unauthorized persons or the general public.

Personal information stored on physical media must be stored securely under lock and key. Only authorized persons have access to these premises. Appropriate measures must be taken to prevent access by unauthorized 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). Personnel may not transport physical documents containing personal information (including agendas, notebooks, forms, or other documents containing names or personal, confidential or identifying information) outside the service centers unless they do so in a locked container (e.g., in the lockable transport pouches provided by L Valoris).

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 is protected under Part X of the *Child, Youth and Family Services Act, 2017 (CYFSA)*.

Because Valoris 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.

The transmission of personal or confidential information by electronic means is permitted only using technologies approved by Valoris for their encryption and security standards.

Personal information may be communicated by e-mail between internal e-mail addresses only, due to the encryption automatically present on all documents that remain within the agency's IT infrastructure.

In circumstances where a client can only be reached through such non-confidential means of communication (email, SMS, snap chat, 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 judgment in the use of such communication technologies to minimize the risk of breaching the client's privacy.

Everyone takes the necessary precautions to ensure the confidentiality of the information displayed on the screens of their devices (computers, telephones, etc.): locking the device during absences (meetings, bathroom, printer, etc.), using privacy filters on certain screens, etc. Documents sent by fax are marked "confidential".

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 appoints a member of the leadership team as Information and Privacy Officer. This person acts as a resource person for all matters relating to the proper use of personal information held by Valoris under the various laws in force. Duties include:

a) Facilitate compliance with privacy legislation by Valoris (the Custodian).
b) Ensure that all authorized employees are adequately informed of their obligations under privacy legislation.
c) Respond to public inquiries about Valoris' (the Custodian) information practices.
d) Receive complaints from the public by e-mail at PVPO@valorispr.ca about any contravention of privacy legislation by Valoris (the Custodian) and notify the Office of the Information and Privacy Commissioner as required.

Employees may contact the Information and Privacy Officer at vieprivee_privacy@valorispr.ca.

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., use without consent data on the sexual orientation of customers or employees to target them directly with advertising from a community group offering services to LGBTQ communitie); or
4) *Unauthorized disclosure of personal information* (e.g., sending an email to the wrong address).

As soon as a person is made aware of a potential invasion of privacy, the following procedure is set in motion:

1. The person at the origin of the potential breach, or the first person to discover it, immediately notifies his or her immediate superior of the situation;
2. The person causing the potential breach, or the first person to discover it, and his or her immediate supervisor notify the Information and Privacy Officer by sending an e-mail to (vieprivee_privacy@valorispr.ca).
3. The person at the origin of the potential breach, or a person appointed by the immediate supervisor, takes the necessary steps to assess and control the potential privacy breach:

    a. The personal information involved is identified
    b. Corrective action is taken, for example:
        i. Ensure that the recipient who was not authorized to receive personal information has not retained it, and request confirmation that it has been destroyed. In the case of physical documents (letters, paper files, etc.), ensure that they are recovered.
        ii. We ensure that the information that was mistakenly shared does not give access to other information (for example, if it was a user name and password). If so, steps are taken to close these access paths to other unauthorized data (e.g., by changing passwords, blocking access, etc.).
        iii. In the event that unauthorized personal information has been accessed voluntarily by an employee, consider whether it is necessary to suspend his or her access rights.

4. The person who initiated the invasion of privacy, or a person appointed by his or her immediate supervisor, notifies those affected by the invasion of privacy as soon as possible. Notification must be direct, i.e., by telephone, letter or e-mail, or in person. Indirect notification is acceptable in situations where direct notification cannot reasonably be used, where the contact details of the persons concerned are unknown or where the invasion of privacy affects a large number of people. The notice to data subjects must:
    a. indicate the scope of the privacy breach and describe the personal information involved;
    b. indicate the measures that have been or will be taken to rectify the situation, both immediately and in the long term;

c. provide contact information for someone at Valoris who can provide additional information and assistance, and answer questions;
d. specify that the person has the right to file a complaint with the CIPVP and how to go about doing so.

5. In the event that the situation is deemed serious according to the guidelines published by the Information and Privacy Commissioner (IPC), the General Manager is informed of the situation as provided for in policy A-203 Situations to be communicated to the General Manager.
6. As the case may be, the Information and Privacy Officer will notify the CIPVP, Valoris' insurer or the police.
    a. The main circumstances to be reported to the CIPVP are as follows:
        i. Valoris determines that the breach is material after assessing the sensitivity, volume, number of people affected and number of service providers involved.
        ii. Personal information has been used or disclosed to a person who knew or ought to have known that it was being used or disclosed without authorization.
        iii. Valoris has reasonable grounds to believe that Personal Information has been stolen.
        iv. Valoris has reasonable grounds to believe that the Personal Information that has been breached has been or is likely to continue to be used or disclosed without authorization, or there is a pattern of similar breaches.
        v. An employee has resigned or has been dismissed, suspended or disciplined as a result of the breach.7. Depending on the type of breach of confidentiality, a serious incident will be completed and sent to the department, as described in the guidelines.
7. Depending on the type of breach of confidentiality, a serious incident will be completed and sent to the Ministry, as described in the guidelines.

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 denying 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, color, religion, age, gender, sexual orientation or marital or family status.
- The individual's medical, psychiatric, psychological, criminal or employment history.
- Any number, symbol or other identifying detail assigned to the individual
- (e.g., health card or driver's licence).
- The individual's address, telephone number, fingerprints or blood type.
- Letters received by us from the individual that are implicitly or explicitly of a private or confidential nature and replies to such correspondence that would disclose the contents of the original correspondence.
- The individual's personal views or opinions, unless they relate to another person.
- The views or opinions of another person about the individual.
- The individual's name when it appears among other personal information about the individual or when disclosure of the name would reveal other personal information about the individual.

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*