Oncidium
clarity when you need it

Privacy of personal information is an important principle to Oncidium. We are committed to collecting, using and disclosing personal information responsibly, and only to the extent necessary for the goods and services we provide. We also try to be open and transparent as to how we handle personal information. This document describes our privacy policies.

What is Personal Information?

Personal information is information about an identifiable individual. Personal information includes information that relates to their personal characteristics (e.g. gender, age, income, home address or phone number, ethnic background, family status), their health (e.g. health history, health conditions, health services, received by them) or their activities and views (e.g. opinions expressed by an individual, an opinion or evaluation of an individual). Personal information is to be contrasted with business information (e.g. an individual's business address and telephone number), which is not protected by privacy legislation.

Who We Are

We use a number of consultants and agencies that may, in the course of their duties, have limited access to personal information we hold. These include computer consultants, office security and maintenance, bookkeepers and accountants, temporary workers to cover holidays, credit card companies, website managers, cleaners and lawyers We restrict their access to any personal information we hold as much as is reasonably possible. We also have their assurance that they follow appropriate privacy principles.

About Clients

Primary Purposes

Like all health care companies, we collect, use and disclose personal information in order to serve our clients. For our clients, the primary purposes for collecting personal information are as follows:

1) Ensure the assessing and treating practitioners and professionals can provide excellence in service provision by accessing all appropriate information when needed along a continuum of care
2) Ensure that ONCIDIUM can help you to schedule/reschedule your appointments when needed.

Examples of the type of personal information we collect for those purposes include the following: gender, age, income, home address or phone number, family status and their health (e.g., health history, health conditions, and health services received by them) or their families.

We collect, use and disclose personal information in order to serve our clients. For example, we collect information about a client's health history, including their family history, physical condition and function and social situation in order to help us assess what their health needs are, to advise them of their options and then to provide the health care they choose to have. A second primary purpose is to obtain a baseline of health and social information so that in providing ongoing health services we can identify changes that are occurring over time.

It would be rare for ONCIDIUM to collect such information without the client's express consent, but this might occur in an emergency (e.g. the client is unconscious) or where we believe the client would consent if asked and it is impractical to obtain consent (e.g. a family member passes a message on from our client and we have no reason to believe that the message is not genuine).

About Members of the General Public

On our ONCIDIUM website we only collect, with the exception of cookies, the personal information you provide and only use that information for the purpose you gave it to us (e.g. to respond to your email message, to register for a course, to subscribe to our newsletter). Cookies are only used to help you navigate our website and are not used to monitor you.

About Contract Staff, Volunteers and Students

For contract staff (e.g., temporary workers, students or consultants to ONCIDIUM), our primary purposes for collecting personal information are as follows:

1) To confirm professional status and standing with respective College
2) To contact you in a timely manner when required
3) To complete business transactions.

Examples of the type of personal information we collect for those purposes include the following:

1) Name and Professional registration number.
2) Contact information
3) Banking/invoicing information
4) Work History (Curriculum Vitae).

We Collect Personal Information: Related to Secondary Purposes

Like most organizations, we also collect, use and disclose information for purposes related to or secondary to our primary purposes. The most common examples of our related and secondary purposes are as follows:

- Collect sufficient information to ensure that the service(s) provided will be paid for by the appropriate body(ies)
- To invoice clients for goods or services that were not paid for at the time, to process credit card payments or to collect unpaid accounts
- Ensure that alternate funding for services is identified and offer you any additional benefits that the facility may be able to provide to you
- To advise clients that their product or service should be reviewed (e.g. to ensure a product is still functioning properly and appropriate for their then current needs and to consider modifications or replacement)
- To advise clients and others of special events (e.g. a seminar, development of a new service, arrival of a new product) or opportunities to participate in drug trial research that we have available
- Our client's review and other files for the purpose of ensuring that we provide high quality services, including assessing the performance of our staff. In addition, external consultants (e.g. auditors, lawyers, practice consultants, voluntary accreditation programs) may on our behalf do audits and continuing quality improvement reviews of our clinic, including reviewing client files and interviewing our staff
- Our medical professionals are regulated by various medical colleges in Ontario who may inspect our records and interview our staff as a part of their regulatory activities in the public interest. In addition, as professionals, we will report serious misconduct, incompetence or incapacity of other practitioners, whether they belong to other organizations or our own
- Also our organization believes that it should report information suggesting serious illegal behaviour to the authorities. External regulators have their own strict privacy obligations. Sometimes these reports include personal information about our clients, or other individuals,

to support the concern (e.g. improper services)

- Also, like all organizations, various government agencies (e.g. Canada Customs and Revenue Agency, Information and Privacy Commissioner, Human Rights Commission, etc.) have the authority to review our files and interview our staff as a part of their mandates. In these circumstances, we may consult with professionals (e.g. lawyers, accountants) who will investigate the matter and report back to us
- The cost of some goods/services provided by the organization to clients is paid for by third parties (e.g. OHIP, WSIB, private insurance, Assistive Devices Program). These third-party payers often have your consent or legislative authority to direct us to collect and disclose to them certain information in order to demonstrate client entitlement to this funding
- Clients or other individuals we deal with may have questions about our goods or services after they have been received. We also provide ongoing services for many of our clients over a period of months or years for which our previous records are helpful. We retain our client information for a minimum of ten (10) years after the last contact to enable us to respond to those questions and provide these services (our regulatory College also requires us to retain our client records)
- From time to time, ONCIDIUM is required to provide staff/consultant CVs through FRIs/RFPS to secure future business

You can choose not to be part of some of these related or secondary purposes (e.g. by declining to receive notice of special events or opportunities, by paying for your services in advance). We do not, however, have much choice about some of these related or secondary purposes (e.g. external regulation).

Protecting Personal Information

We understand the importance of protecting personal information. For that reason, we have taken the following steps:

- Paper information is either under supervision or secured in a locked or restricted area. Electronic hardware is either under supervision or secured in a locked or restricted area at all times. In addition, passwords are used on computers. All of our cell phones are digital, as such signals are more difficult to intercept.
- Paper information is transmitted through sealed, addressed envelopes or boxes by reputable companies and staff/consultants.
- Electronic information is pass-worded prior to transmission.
- Staff is trained to collect, use and disclose personal information only as necessary to fulfil their duties and in accordance with our privacy policy.
- External consultants and agencies with access to personal information must enter into privacy agreements with us.

Retention and Destruction of Personal Information

We need to retain personal information for some time to ensure that we can answer any questions you might have about the services provided and for our own accountability to external regulatory bodies. However, we do not want to keep personal information too long in order to protect your privacy. We keep our clients files for about ten years. Our client and contact directories are much more difficult to systematically destroy, so we remove such information when we can if it does not appear that we will be contact you again. However, if you ask, we will remove such contact information right away. We keep any personal information relating to our general correspondence (e.g. with people who are not clients) newsletters, seminars and marketing activities for about six months after the newsletter ceases publication or a seminar or marketing activity is over.

We destroy paper files containing personal information by shredding. We destroy electronic information by deleting it and, when the hardware is discarded, we ensure that the hard drive is physically destroyed. Alternatively, we may send some or the entire client file to our client.

You Can Look at Your Information

With only a few exceptions, you have the right to see what personal information we hold about you. Often all you have to do is ask. We can help you identify what records we might have about you. We will also try to help you understand any information you do not understand (e.g.. short forms, technical language, etc.). We will need to confirm your identity, if we do not know you, before providing you with this access. We reserve the right to charge a nominal fee for such requests. If there is a problem we may ask you to put your request in writing. If we cannot give you access, we will tell you within 30 days if at all possible and tell you the reason, as best we can, as to why we cannot give you access. If you believe there is a mistake in the information, you have the right to ask for it to be corrected. This applies to factual information and not to any professional opinions we may have formed. We may ask you to provide documentation that our files are wrong. Where we agree that we made a mistake, we will make the correction and notify anyone to whom we sent this information. If we do not agree that we have made a mistake, we will still agree to include in our file a brief statement from you on the point and we will forward that statement to anyone else who received the earlier information.

DO YOU HAVE A QUESTION?
The Facility Information Officer (FIO) would be pleased to respond to any question or concern you may have. The FIO can be reached at:

100-19 Allstate Parkway, Markham, ON L3R 5A4
Bus: 905-475-3353, Fax: 905-475-6134

The officer will attempt to answer any questions or concerns you might have. If you wish to make a formal complaint about our privacy practices, you may make it in writing to our Information Officer. She/he will acknowledge receipt of your complaint; ensure that it is investigated promptly and that you are provided with a formal decision and reasons in writing. If you have a concern about the professionalism or competence of our services or the mental or physical capacity of any of our professional staff we would ask you to discuss those concerns with us. However, if we cannot satisfy your concerns, you should contact our CEO and President Dr. Lu Barbuto. You are also entitled to contact the regulatory college of the practitioner that was treating you.

This policy is made under the *Personal Information Protection and Electronic Documents Act.* That is a complex Act and provides some additional exceptions to the privacy principles that are too detailed to set out here. There are some rare exceptions to the commitments set out above.

For more general inquiries, the Privacy Commissioner of Canada oversees the administration of the privacy legislation in the private sector. The Commissioner also acts as a kind of ombudsman for privacy disputes. The Privacy Commissioner can be reached at:

112 Kent Street, Ottawa, ON, K1A 1H3
Bus: 613-995-8210 Toll-Free: 1-800-282-1376 Fax: 613-947-6850 TTY: 613-992-9190
WWW.PRIVCOM.GC.CA