Privacy Policy

Nanostics Inc.

Nanostics is committed to safeguarding the personal information that our clients have entrusted to us. This policy outlines the principles and practices we follow in protecting clients/patients personal information. We have appointed a Privacy Officer who is responsible for ensuring that this privacy policy is complied with.

This policy applies to Nanostics and also applies to any person providing services on our behalf. A copy of this policy is provided to any individual on request.

What is personal information?

Personal information means information about an identifiable individual. This includes, but is not limited to, an individual's name, home address, email address, phone number, age, date of birth, sex, marital or family status, an identifying number including provincial health number, social insurance number, bank account number, ethnicity, height and weight, and educational history.

Personal information also includes health related information from clinical study participants and patients including, but not limited to, laboratory test results, biopsy results, treatments provided, use of medications, disease outcomes, familial history of disease, and previous medical history.

What personal information do we collect?

We collect only the personal information that we need for the purposes of providing services, including personal information needed to:

- to provide high quality services
- to allow us to communicate with you for the distribution of health-care information
- to enable us to have the ability to follow up for testing and billing
- for learning and teaching purposes on an anonymous basis
- for research, health surveillance and statistical analysis purposes
- for administrative activities related to planning, resource allocation, or reporting
- to comply with legal and regulatory requirements mandated by the government
- for additional purposes that have been identified to you when information is collected

Personal data collected as part of clinical studies will be used to:

- identify patient eligibility for clinical studies,
- access health data needed for clinical studies,
- create models for predicting disease states.

We directly collect an individual's personal information. We may collect clients/patients information from other persons with clients/patients consent or as authorized by law.

We inform individuals, before or at the time of collecting personal information, of the purposes for which we are collecting the information. However, we don't provide this notification when an individual volunteers information for an obvious purpose.

Storage of individual personal information in Canada

Personal information from individuals from the U.S.A. collected as part of clinical studies may be delivered and stored on electronic systems within Canada. Some of Nanostics' clinical studies involve patients from both Canada and the U.S.A. and data will be centralized in Canada for batch analysis

of all clinical data. Electronic storage systems in Canada containing personal information will contain sufficient safeguards required to ensure adequate protection of personal information.

Consent

We ask for consent to collect, use or disclose personal information, except in specific circumstances where collection, use or disclosure without consent is authorized or required by law. We may assume clients/patients consent in cases where the information is voluntarily provided for an obvious purpose. Someone is 'deemed to consent' if he or she, without actually giving consent, voluntarily provides the information to the organization and it is reasonable for that purpose. This is also called 'implied consent'.

We ask for clients/patients express consent for some purposes and may not be able to provide certain services if clients/patients are unwilling to provide consent to the collection, use or disclosure of certain personal information. Where express consent is needed, we will ask individuals to provide their consent orally (in person, by telephone), in writing (clinical study participants will sign a consent form), or electronically (by clicking a button).

An individual may withdraw consent to the use and disclosure of personal information at any time unless the personal information is necessary for us to fulfill our legal obligations. We will respect clients/patients decision, but we may not be able to provide clients/patients with certain products and services if we do not have the necessary personal information.

We may collect, use, or disclose personal information without consent only as authorized by law. For example, we may not request consent when the collection, use, or disclosure is reasonable for an investigation or legal proceeding, to collect a debt owed to our organization, or in an emergency that threatens life, health, or safety.

Nanostics may collect, use, and disclose personal employee information of a potential, current, or former employee without his or her consent if it is reasonable and if:

- it is solely for the purposes of establishing, managing, or terminating an employment or volunteer-work relationship between the organization and that person, or
- it is for managing a post-employment or post-volunteer-work relationship between the organization and that person.

How do we use and disclose personal information?

We use and disclose personal information only for the purposes for which the information was collected, except as authorized by law. For example, we may use contact information to deliver information. We will use contact information for the purpose of collecting a debt owed to our organization, should that be necessary.

If we wish to use or disclose clients/patients personal information for any new business purpose, we will ask for clients/patients consent.

How do we safeguard personal information?

We make every reasonable effort to ensure that personal information is accurate and complete. Our employees received necessary training on information privacy based on relevant regulations as well as best security practices. We rely on individuals to notify us if there is a change to their personal information that may affect their relationship with our organization. If clients/patients are aware of an error about them in our information systems, please let us know and we will correct it on request wherever possible. We may ask for a written request for corrections as described below.

We protect personal information in a manner appropriate for the sensitivity of the information. We make every reasonable effort to prevent any loss, misuse, disclosure, or modification of personal information, as well as any unauthorized access to personal information. Nanostics employs administrative, physical, and technical safeguards for minimizing security events which may breach personnel information.

Administrative safeguards

Nanostics collects and stores records of consent for customer personnel and health information whenever required for our products and processes. We have created and follow a variety of security and privacy policies, procedures, and processes to minimize the occurrence of data breaches and security events. A security team periodically reviews user access to information systems containing personal data and ensures personal data is only accessible to those that require it. The security team are also periodically review all internal security and privacy documentation, including this document, for compliance with relevant regulations at least once per year.

Physical safeguards

Personal information in physical and electronic forms are securely stored to minimize the risk of physical loss of the information.

Electronic personal information is stored on third-party data servers. These third party data storage providers which have been evaluated and approved for use based on their compliance with security and privacy regulations including ISO 27001 and SOC 2 audit reports.

Hard copies of health records are stored within 3 secured areas. File cabinets that store the source documents are located:

a) at participating sites within facilities with secured main door entry access,
b) housed in the secure Research Unit department(s) which has restricted access,
c) within rooms that have key access,
d) filed within the delegated filing cabinets which are locked when not in use.

Technical safeguards

Electronic personal information resides on information systems that are password protected with the minimum required personnel having access to these systems. Files containing sensitive personal information, such as financial information or clinical results, are individually encrypted with only authorized individuals having the capability to decrypt and read the information. When mobile devices containing personal information are lost, the personal information on the lost devices will be remotely deleted.

Patient-reported data and clinical parameters are captured using a secure web application designed to meet the security and privacy needs of clinical research. Access restrictions are assigned individually, user activities are logged for auditing, and a de-identifying feature is available for data extraction. Electronic information is kept in secured, encrypted, firewall protected servers.

We retain personal information only as long as is reasonable to fulfil the purposes for which the information was collected or for regulatory, legal, or business purposes.

We render personal information non-identifying, or destroy records containing personal information once the information is no longer needed.

We use appropriate security measures when destroying personal information, including shredding paper records and securely sanitizing electronic data.

How do we respond to data breaches?

When personal information on Albertans is breached, we will notify the Office of the Information and Privacy Commissioner of Alberta, without delay, if it creates a real risk of significant harm to individuals.

When personal information on individuals from the U.S.A. is breached, we will notify the Secretary of Health and Human Services, without delay, if it creates a real risk of significant harm to individuals.

Access to records containing personal information

Individuals have a right of access to their own personal information in a record that is in our custody or under our control, subject to some exceptions. For example, organizations are required under the Personal Information Protection Act to refuse to provide access to information that would reveal personal information about another individual. Organizations are authorized under the Act to refuse access to personal information if disclosure would reveal confidential business information. Access may also be refused if the information is privileged or contained in mediation records.

If we refuse a request in whole or in part, we will provide the reasons for the refusal. In some cases where exceptions to access apply, we may withhold that information and provide clients/patients with the remainder of the record.

Clients/patients may make a request for access to their personal information via email at privacy@nanosticsdx.com. Clients/patients must provide sufficient information in their request to allow us to identify the information they are seeking.

Clients/patients may also request information about our use of their personal information and any disclosure of that information to persons outside our organization.

Nanostics strives to have up-to-date and accurate health records. Clients/patients may request a correction of an error or omission in their personal information by email at privacy@nanosticsdx.com. Clients/patients will be provided with a Modify Record Form, which can be used to process record modification requests.

All requests for accessing or correcting personal information coming from email addresses not belonging to Nanostics will require one piece of photo identification (e.g., driver's licence, passport) **or** two pieces of identification without a photo (e.g., health care card, birth certificate, marriage certificate). Copies of identification should be sent in a separate email to privacy@nanosticsdx.com from the initial request so that the email containing the identification can and will be destroyed in a confidential and secure manner when the request is processed.

If clients/patients are requesting to access or correct another individual's personal information, justification must be provided for why they have the authority to do so with any supporting documentation provided in the request. If the supporting documentation contains sensitive information, send this information in a separate email so that it can and will be destroyed in a confidential and secure manner when the request is processed.

We will respond to clients/patients requests within 30 calendar days. If requests takes longer than 30 days, clients/patients will be notified about the reason for the delay. We may charge a reasonable fee to provide information, but not to make a correction. We will advise clients/patients of any fees that may apply before beginning to process requests.

Questions and complaints

If clients/patients have a question or concern about any collection, use or disclosure of personal information by Nanostics, or about a request for access or modification to clients/patients own personal information, please contact Nanostics using the contact information below:

Nanostics, Inc.
privacy@nanosticsdx.com

If clients/patients are from Alberta and are not satisfied with the response they received, they may contact the Information and Privacy Commissioner of Alberta:

Office of the Information and Privacy Commissioner of Alberta
Suite 2460, 801 - 6 Avenue, SW
Calgary, Alberta T2P 3W2
Phone: 403-297-2728
Toll Free: 1-888-878-4044
E-mail: generalinfo@oipc.ab.ca
Website: www.oipc.ab.ca

If clients/patients are from the U.S.A and are not satisfied with the response they received regarding a complaint about Nanostics, clients/patients may contact the Office for Civil Rights by visiting: https://www.hhs.gov/hipaa/filing-a-complaint/index.html.
A written complaint can be sent to:

Centralized Case Management Operations
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F HHH Bldg.
Washington, D.C. 20201
Email: OCRComplaint@hhs.gov