Privacy Policy

Nanostics Inc.

Nanostics is committed to safeguarding the personal information in our care. This policy outlines the principles and practices we follow in protecting personal information. We have appointed a Privacy Officer that 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 not limited to, an individual's name, home address, email address, and 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 communication 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 someone's information from another person 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 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 express consent for some purposes and may not be able to provide certain services if consent is not provided 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 writing, or electronically.

Individuals may withdraw consent to the use and disclosure of their personal information at any time, unless the personal information is necessary for us to fulfil our legal obligations. We will respect their decision, but we may not be able to provide them with certain products and services if we do not have the necessary 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 their 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 personal information for any new business purpose, we will ask for 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 you are aware of an error 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 likelihood 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.

Physical and electronic data are stored at facilities with appropriate physical safeguards. Electronic personal information is stored on third-party data servers. These third party data storage providers have been evaluated and approved for use based on their compliance with security and privacy regulations including ISO 27001 certification and SOC 2 audit reports.

Technical safeguards

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

Patient-reported data and clinical parameters are captured using secure web applications. 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?

We have a data breach procedure that contacts relevant privacy commissioners and individuals affected in an appropriate time frame as required by law.

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, as appropriate by law. If we refuse a request in whole or in part, we will provide the legal reasons for the refusal.

Requests for access to personal information can be made via email at privacy@nanosticsdx.com. Sufficient information must be provided in the request to allow us to verify that the requestor is allowed the personal information and to identify the information that they seek.

Requests for how personal information was used or disclosed may be made via email at privacy@nanosticsdx.com.

Nanostics strives to have up-to-date and accurate health records. Individuals may request a correction of an error or omission in their personal information by email at privacy@nanosticsdx.com. Indivuduals 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 be destroyed in a confidential and secure manner when the request is processed.

If individuals 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 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 individuals 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 their personal information, please contact Nanostics using the contact information below:

Nanostics, Inc.
privacy@nanosticsdx.com

Individuals that are unsatisfied with how we have processed their requests may submit a formal complaint to their relevant privacy commissioner, who may be able to review our decision.

NADOC-0041, Nanostics Privacy Policy (DOC-883) Ver. 1

Approved By:

(CO-533) Rev to Ver 1.0 - NADOC-0041, Nanostics Privacy Policy

Description

1. Privacy policy now includes additional jurisdictions.

Justification

1. Nanostics now operates outside Alberta, additional requirements have been added to the privacy policy to include additional jurisdiction requirements.

Assigned To:	Initiated By:	Priority:	Impact:
Colin Coros	Colin Coros	High	Minor

Version History:

Author	Effective Date	CO#	Ver.	Status
Sean Rah	September 16, 2024 8:57 AM MDT	CO-533	1	Published
Colin Coros	August 21, 2023 8:26 PM MDT	CO-438	0	Superseded