Subject:	Privacy Policy	Date Approved:
Approved by:	Board of Directors	Date Revised:
Specific to:	All Staff: Board of Directors, Preceptors, Students, Researchers	Next Review Date:

PRINCIPLE:

The Discovery Pharmacy (DRx) is committed to patient privacy and to protecting the confidentiality of the personal health information (PHI) that we hold while facilitating the effective provision of health care. The term "patient" includes all individuals whose personal health information the DRx holds (E.g., former patients). The privacy policy applies to all of those individuals.

POLICY:

Our pharmacist(s) are fully accredited members in good standing of the Ontario College of Pharmacists. They all also belong to the DRx and are agents of the DRx, which is a health information custodian (HIC) under the *Personal Health Information Protection Act, 2004* (PHIPA). The DRx is accountable and liable for compliance with PHIPA and the protection of health records. For the purposes of privacy obligations, the DRx Leadership Team and our staff are agents of the DRx. This relationship has been established through a "PHIPA Agency Agreement" signed by each Pharmacist and the DRx Team.

In this Privacy Policy, we use the language of "**Team Members**" to capture the commitment that all pharmacists, and all DRx Leadership Team and DRx staff, volunteers, students and vendors are bound by under this Privacy Policy, which embody our shared commitment to protecting personal health information, always consistent with, and in the effective provision of health care.

This Privacy Policy acts as the articulation of the privacy practices and standards to guide all Team Members and any other agents. Additional privacy requirements or policies, set out in **Appendix A** of this Policy also apply to and must be followed by all Team Members.

Principle 1 – Accountability for Personal Health Information

Our pharmacists are responsible for any personal health information held. The following position has been designated as the Privacy Officer: Executive Director. The Privacy Officer is accountable for compliance with this Privacy Policy and compliance with PHIPA.

Our commitment to privacy is demonstrated by adherence to privacy policies and procedures to protect the personal health information we hold and by educating our staff and any others who collect, use or disclose personal health information on our behalf about their privacy responsibilities, by requiring them to enter into agent agreements consistent with PHIPA requirements, and by monitoring and ensuring their compliance with their agent responsibilities, PHIPA, and all other applicable requirements. Additionally, any agent who act in a manner inconsistent with any of these obligations will be notified, instructed to make necessary corrections/improvements as appropriate, and/or disciplined or terminated as appropriate. Where necessary or consistent with College or other professional, practice, legal, or policy requirements or expectations, information about their actions will be shared with investigators, the OCP, or other officials and bodies as appropriate.

Principle 2 – Identifying Purposes for Collecting Personal Health Information

We collect personal health information for purposes related to the provision of health care, including direct patient care, administration and management of our programs and services, patient billing, administration and management of the health care system, research, teaching, statistical reporting, meeting legal obligations, fundraising, marketing and as otherwise permitted or required by law.

When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. As necessary by law, consent may be required before the information can be used for that purpose.

Principle 3 – Consent for the Collection, Use and Disclosure of Personal Health Information

We require consent in order to collect, use, or disclose personal health information. However, there are some cases where we may collect, use or disclose person health information without consent as permitted or required by law.

Express consent

Should a patient wish his/her other health care providers (outside of their health care providers at the Discovery Pharmacy) to have access to the patient health record, the patient can provide a verbal or written consent to this effect, which will be communicated to the patient's health care provider.

Should a patient wish his/her lawyer, insurance company, family, employer, landlord or other third party individuals or agencies (non-health care providers) to have access to his/her health record, the patient must provide verbal or written consent to this effect.

Implied consent (Disclosures to other health care providers for health care purposes) – Circle of Care

Patient information may also be released to a patient's other health care providers for health care purposes (within the "circle of care") without the express written or verbal consent of the patient as long as it is reasonable in the circumstances to believe that the patient wants the information shared with the other health care providers. No patient information will be released to other health care providers if a patient has stated that he/she/they does not want the information shared.

A patient's request for treatment constitutes implied consent to use and disclose his/her personal health information for health care purposes, unless the patient expressly instructs otherwise.

Who can be in the "circle of care" includes (among others providing direct patient care if authorized by PHIPA):

Within the Discovery Pharmacy Team:

- All pharmacists in this practice
- Interprofessional health providers
- Medical students, residents and locums
- Nursing or other health care students

Outside of the Discovery Pharmacy Team:

- University Health Network
- University of Toronto
- Hospitals
- Community Care Access Centres
- Community Health Centres
- Long-term care homes
- Ambulance
- Pharmacists
- Laboratories
- Regulated health professionals in sole practice or group
- Social workers and social service workers in sole practice or group
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care
- Any other HIC that needs the PHI for provision of health care to the patient, and which the patient has not identified as one with which he/she/they does not what their PHI shared.

No Consent

There are certain activities for which consent is not required to use or disclose personal health information. These activities are permitted or required by law. For example, we do not need consent from patients to (this is not an exhaustive list):

- Plan, administer and manage our internal operations, programs and services
- Reimbursements and payments
- Engage in quality improvement, error management, and risk management activities
- Participate in the analysis, administration and management of the health care system
- Engage in research (subject to research ethics board requirements)
- Teach, train and educate our Team Members and others
- Compile statistics for internal or mandatory external reporting

- Respond to legal proceedings
- Comply with mandatory reporting obligations

Team Members should direct any questions they have about using and disclosing personal health information without consent or otherwise to the Privacy Officer.

Withholding or Withdrawal of Consent

If consent is sought, a patient may choose not to give consent ("withholding consent"). If consent is given, a patient may withdraw consent at any time, but the withdrawal cannot be retrospective. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

PHIPA gives patients the opportunity to restrict access to any personal health information or their entire health record by their health care providers within the Discovery Pharmacy or by external health care providers. The patient has the ability to withdraw or withhold consent for the use or disclosure of their personal health information for health care purposes.

Principle 4 – Limiting Collection of Personal Health Information

We limit the amount and type of personal health information we collect to that which is necessary to fulfill the purposes identified. Information is collected directly from the patient, unless the law permits or requires collection from third parties. For example, from time to time we may need to collect information from patients' family members or other health care providers.

Personal health information may only be collected within the limits of each Team Member's role and the conditions of their agent agreement.

Team Members are strictly prohibited from initiating their own projects to collect new personal health information from any source without being explicitly authorized in writing by DRx or the Privacy Officer**.**

Principle 5 – Limiting Use, Disclosure and Retention of Personal Health Information Use

Personal health information is not used for purposes other than those for which it was collected, except with the consent of the patient or as permitted or required by law.

Personal health information may only be used within the limits of each Team Member's role and the conditions of their agent agreement. Team Members may not read, look at, receive or otherwise use personal health information unless they have a legitimate "need to know" that is consistent with PHIPA requirements and the conditions of their agent agreement, as part of their position. If a Team Member is in doubt whether an activity to use personal health information is part of his/her position – he/she should ask the Privacy Officer**.** For example, self-directed learning is not allowed (randomly or intentionally looking at health records for self-initiated educational purposes) without specific prior written authorization.

Disclosure

Personal health information is not disclosed for purposes other than those for which it was collected, except with the consent of the patient or as permitted or as permitted or required by law.

Personal health information may only be disclosed within the limits of each Team Member's role. Team Members may not share, talk about, send to or otherwise disclose personal health information to anyone else unless that activity is an authorized part of their position, consistent with PHIPA requirements, and with the terms of their agent agreement. If a Team Member is in doubt whether an activity to disclose personal health information is part of his/her position – he/she should ask the Privacy Officer.

Retention

Health records are retained as required by law and professional regulations and to fulfill our own purposes for collecting personal health information.

The Ontario College of Pharmacists advise their members to retain health records for at least 10 years from the date of last entry or, in the case of minors, 10 years from the time the patient would have reached the age of majority (age 18). There may be reasons to keep records for longer than this minimum period.

Personal health information that is no longer required to fulfill the identified purposes is destroyed, erased, or made anonymous safely and securely, so that it cannot be reidentified.

Principle 6 – Accuracy of Personal Health Information

We will take reasonable steps to ensure that information we hold is as accurate, complete, and up to date. This is done to comply with legal and professional standards, and as necessary to minimize the possibility that inappropriate information may be used to make a decision about a patient.

Principle 7 – Safeguards for Personal Health Information

We have put in place safeguards for the personal health information we hold, which include:

- Physical safeguards (such as locked cabinets within locked rooms);
- Organizational safeguards (such as permitting access to personal health information by staff on a "need-to-know" basis, and consistent with proper agent agreements only); and
- Technological safeguards (such as the use of passwords, encryption, and audits).

We take steps to ensure that the personal health information we hold is protected against theft, loss and unauthorized use or disclosure.

We require anyone who collects, uses or discloses personal health information on our behalf to be aware of the importance of maintaining the confidentiality of personal health information. This is done through the signing of agent agreements, which include confidentiality requirements, privacy training, and contractual means.

Care is used in the disposal or destruction of personal health information, to effectively prevent unauthorized parties from gaining access to the information.

Principle 8 – Openness about Personal Health Information

Information about our policies and practices relating to the management of personal health information are available to the public, including:

- Contact information for our Privacy Officer, to whom complaints or inquiries can be made;
- The process for obtaining access to personal health information we hold, and making requests for its correction;
- A description of the type of personal health information we hold, including a general account of our uses and disclosures and information practices; and
- A description of how a patient may make a complaint to the Discovery Pharmacy or to the Information and Privacy Commissioner of Ontario.

Principle 9 – Patient Access to Personal Health Information

Patients may make written requests to have access to their records of personal health information, in accordance with the Discovery Pharmacy's "*Access and Correction Policy – Release of Patient Information*".

We will respond to a patient's request for access within reasonable timelines and costs to the patient, as required by law. We will take reasonable steps to ensure that the requested information is made available in a format that is understandable.

Patients who successfully demonstrate the inaccuracy or incompleteness of their personal health information may request that we correct amend the record of their personal health information. In some cases instead of making a correction, patients may ask to append a statement of disagreement to their file.

Please Note: In certain situations, we may not be able to provide access to all the personal health information we hold about a patient. Exceptions to the right of access requirement will be in accordance with law and patient safety. Examples may include information that could reasonably be expected to result in a risk of serious harm or the information is subject to legal privilege.

Principle 10 – Challenging Compliance with the DRx's Privacy Policies and Practices

Any person may ask questions or challenge our compliance with this policy or with PHIPA by contacting our Privacy Officer:

Executive Director
Discovery Pharmacy
144 College St
Toronto, ON
M3S 3M2

We will receive and respond to complaints or inquiries about our policies and practices relating to the handling of personal health information. We will inform patients who make inquiries or lodge complaints of other available complaint procedures.

We will investigate all complaints. If a complaint is found to be justified, we will take appropriate measures to respond.

The Information and Privacy Commissioner of Ontario oversees our compliance with privacy and PHIPA. Any individual can make an inquiry or complaint directly to the Information and Privacy Commissioner of Ontario by writing to or calling:

2 Bloor Street East, Suite
1400 Toronto, Ontario
M4W 1A8 Canada
Phone: 1 (800) 387-0073 (or 416-326-3333 in Toronto)
Fax: 416-325-9195
www.ipc.on.ca

Appendix A –Supporting Privacy Policies

The following policies and documents are incorporated into the Privacy Policy and must be followed by all pharmacists, the DRx Team and all staff, students, volunteers, and vendors:

Policies	**Last Updated**
University of Toronto Governing Council – Statement Regarding Access to Information and Protection of Privacy at the University of Toronto https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwitnu3tpff0AhXzdM0KHdyHA30QFnoECCUQAQ&url=https%3A%2F%2Fgoverningcouncil.utoronto.ca%2Fmedia%2F4299%2Fview&usg=AOvVaw3Sqbwx_RAah4ncTXPRr8ZK	November 2, 2006
University of Toronto Governing Council – University Health Service Policy https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiY9LOBpvf0AhXGXc0KHWduDJEQFnoECAIQAQ&url=https%3A%2F%2Fgoverningcouncil.utoronto.ca%2Fsecretariat%2Fpolicies%2Fhealth-service-policy-november-9-1993&usg=AOvVaw3mpoEMQ9f_Ev8Mi8_nsr7y	November 9, 1993
University of Toronto Governing Council – Standards of Professional Practice Behaviour for all Health Professional Students https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiYkN-Mpvf0AhXFWc0KHZ5hDy8QFnoECAIQAQ&url=https%3A%2F%2Fgoverningcouncil.utoronto.ca%2Fsecretariat%2Fpolicies%2Fprofessional-practice-behaviour-all-health-professional-students-standards-0&usg=AOvVaw0LzXZRGuxj-O6AO1plPJXs	September 2008
SCHEDULE B ACCEPTABLE USE POLICY - COVAX$_{ON}$	March 29, 2021
SCHEDULE D - COVAX$_{ON}$ PRIVACY AND INFORMATION MANAGEMEN ANNEX	March 29, 2021

SCHEDULE B

ACCEPTABLE USE POLICY - COVAX$_{ON}$

1. Definitions

"**Confidential Information**" means any business or technical information which is proprietary to the Ministry, whether it is received, accessed or viewed by the recipient in writing, visually, electronically or orally. Confidential Information shall include, without limitation, technical information, business plans, databases, specifications, prototypes, sketches, specifications, software (source and object codes).

"**End User**" or "**you**" or "**your**" means you, the individual who has signed into the Solution, and who has been authorized by your User Organization to access and use the Solution.

"**Ministry**" means the Ontario Ministry of Health.

"**Personal Information**" means any recorded information about an identifiable individual or that may identify an individual and includes "personal health information" as such term is defined in the *Personal Health Information Protection Act, 2004* (Ontario).

"Purpose" means reporting COVID-19 vaccine administration, demographic and adverse event information to the Chief Medical Officer of Health, a Medical Officer of Health or a Board of Health as authorized or permitted under PHIPA or the HPPA, and other purposes permitted or required by law.

"**Solution**" means the platform called "COVAX$_{ON}$" or and such extensions and upgrade to the platform, as may be owned by, licensed or subscribed to by the Ministry and made available to your User Organization.

"**Policy**" means this Acceptable Use Policy.

"**User Organization**" means the legal entity who authorized you to access and use the Solution.

2. Scope and Application

This Policy governs your access to and use of the Solution. The Ministry may revise this Policy from time-to-time at its sole discretion, by providing notice to your User Organization. By continuing to access and use the Solution after a revised version of the Policy has been provided to your User Organization, you agree to comply with the latest version of the Policy.

When you click the "Accept" button when entering the Solution, you are agreeing to be bound by this Policy. Please review the following terms carefully. If you do not agree with these terms you cannot use or gain access to the Solution.

3. Accountability

- Your User Organization is responsible for your access to and use of the Solution.

- You must obtain your credentials, or other system access tools required to access the Solution as well as related hardware (mobile devices) and technology components only as authorized by your User Organization.
- You are responsible for complying with this Policy.

4. Acceptable Use

You may access and use the Solution solely for the Purpose. You agree to access and use the Solution in compliance with all applicable laws, regulations or policies including the *Personal Health Information Protection Act, 2004* and all guidelines, policies, and manuals prescribed by your User Organization.

5. Inappropriate and Unacceptable Use

You shall not use the Solution in any manner that constitutes inappropriate or unacceptable use, which includes, but is not limited to:

(a) Collecting, using, or disclosing Personal Information in contravention of the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act, 2004*, or any other applicable law.
(b) Accessing the Solution and the Personal Information contained within the Solution for any purpose other than the Purpose.
(c) Collecting, using or disclosing Personal Information in the Solution which is not required for your use of the Solution.
(d) Accessing, viewing, editing, updating or modifying any information or data in the Solution unless such access, viewing, editing, updating or modification is for the Purpose.
(e) Destroying or encrypting data and visual aids except as expressly permitted in documentation supplied by the Ministry or as required by applicable law.
(f) Making, possessing or distributing computer programs that are designed to assist in obtaining access to the Solution in violation of any agreement, this Policy or applicable laws.
(g) Wilfully bypassing or subverting physical, logical or procedural safeguards such as firewalls, web-filtering software or other access controls or attempting to gain access to the Solution other than through your access contemplated by this Policy.
(h) Sharing passwords, or other system access tools with un-authorized individuals or entities for any purpose.
(i) Facilitating the violation of this Policy.
(j) Violating or facilitating the violation of a third party's acceptable use policy during your use of the Solution.
(k) Infringing intellectual property rights including copyrights, trade secrets, or trademarks.
(l) Disclosing Confidential Information about the Solution, except as required by law.
(m) Posting or submitting any material or information into the Solution that:
    (i) is abusive, defamatory, discriminatory, offensive, irrelevant or unlawful;

(ii) you do not have the legal right to post in the Solution, or otherwise to publish or distribute;
(iii) is for advertising or commercial purposes; or
(iv) you know to be false, inaccurate or misleading.

6. Security

You are responsible for safeguarding your login credentials. Any password or ability to access the Solution given to you is not transferable.

You must immediately notify your User Organization if you suspect or know that passwords or other system access tools have been or may be breached or compromised and change your password as soon as possible in such circumstances.

You agree to provide all assistance in regard to any privacy complaints of individuals and reviews conducted by the Information and Privacy Commissioner of Ontario.

You will take all reasonable steps to safeguard confidential information from unauthorized use or disclosure.

You will only enter information into the Solution that you know to be accurate.

You will report any errors in the Solution to the Ministry.

You will promptly report any breach or suspected breach of privacy to your User Organization.

You are responsible for the security of the device that you are using to access Solution.

7. Collection, Use and Disclosure of Confidential Information

By using the Solution you confirm that you are authorized by your User Organization to access the Solution and you and your User Organization have the legal authority to access the Solution pursuant to PHIPA.

You acknowledge that in using the Solution, you may have access to Confidential Information.

You will not access, collect, use, disclose, retain or dispose of any information in Solution unless authorized by law to do so and as required in the proper discharge of your duties. In particular, you understand that you are only authorized to access, collect, use, disclose, retain or dispose of Personal Information as it relates to the Purpose, and as directed by your User Organization.

8. Non-Compliance with this Policy

You must report all instances of suspected or actual breaches of this Policy to your User Organization.

The Ministry reserves the right to investigate suspected or actual breaches of this Policy. You shall fully cooperate with any such investigation. For greater certainty, you shall:

(a) Provide access to all documentation requested orally or in writing by the Ministry; and
(b) Provide any other assistance that may reasonably be requested by the Ministry in connection with an actual or suspected breach.

The Ministry or your User Organization may, at their sole discretion, suspend or revoke your access to the Solution as a result of your actual or suspected breach of this Policy.

Breaches of this Policy may result in criminal prosecution or civil liability and/or other sanctions deemed appropriate by the Ministry or your User Organization.

9. Third Party Rules

Your access to the Solution includes access to third party services that publish rules, guidelines or agreements to govern their use. You must adhere to any such rules, guidelines or agreements. Such third party services include, but are not limited to:

(a) Salesforce and MuleSoft: Acceptable Use Policy
- https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/Agreements/policies/ExternalFacing_Services_Policy.pdf

(b) Amazon Web Services: Acceptable Use Policy
- https://aws.amazon.com/service-terms/

10. Liability, Intellectual Property and General

The Ministry shall not be liable for any losses, expenses, costs, claims, damages or liabilities howsoever arising in connection with or as a result of a User's End User's access to or use of the Solution.

Nothing in this Policy or your access to the Solution will transfer any right, title or interest in or to Solution to you, including any intellectual property rights.

Any failure by the Ministry to enforce any part of this Policy shall not constitute waiver by the Ministry of any right to do so at any time. If any provision of this Policy is found to be invalid or unenforceable, then that provision will be enforced to the extent permissible, and all other provisions will remain in full force and effect.

Acceptance

By selecting the 'I Accept' button you are acknowledging that you have read, understood, accept and will comply with the terms of use set out above.

SCHEDULE D - COVAX$_{ON}$
PRIVACY AND INFORMATION MANAGEMENT ANNEX

(a) Acknowledgements

By accessing the Solution, the User acknowledges that:

1. Medical Officers of Health of boards of health and their agents, and the Chief Medical Officer of Health and its agents and permitted users ("Other Users") may collect Relevant PHI that the User inputs into the Solution, for the Purpose, in accordance with terms that are substantially the same as the terms that the User is agreeing to in the Agreement.
2. By inputting Relevant PHI into the Solution, the User agrees to disclose that Relevant PHI to Other Users for the Purpose, if those Other Users collect that Relevant PHI in accordance with Applicable Law (including PHIPA), and in accordance with terms that are substantially the same as the terms that the User is agreeing to in the Agreement.
3. The User may only input into the Solution, Relevant PHI that the User is legally permitted to disclose to Other Users under Applicable Law (including PHIPA). For greater certainty, the User may not input Relevant PHI into the Solution if making that Relevant PHI available to Other Users would violate any consent, promise or agreement between the User and another person, including the person to whom the Relevant PHI relates to, unless the law permits the User to make that information available to Other Users despite the consent, promise or other agreement. Other Users are relying on the User's acknowledgements and agreements in the Agreement and this Schedule for the purposes of ensuring their compliance with Applicable Law.
4. The User is responsible for the manner in which its End Users access the Solution, including any Relevant PHI in the Solution.
5. The User has conducted or will conduct a privacy impact assessment and threat and risk assessment, regarding the Solution, as may be required by User policies and guidelines.

(b) Accessing the Solution and Personal Information

In accessing the Solution, the User shall:

1. Only access or otherwise collect Relevant PHI, from one or more Other Users who are authorized to disclose the Relevant PHI into the Solution for the Purpose.
2. Only use or disclose Relevant PHI that the User has collected from the Solution as permitted or required by law.
3. Only access Relevant PHI that the User has inputted into the Solution for the Purpose.
4. Not access or collect more Relevant PHI than the User needs for the particular purpose for which the User is accessing or collecting Relevant PHI from the Solution.
5. Comply with any acceptable use polices, terms of use or other supplementary rules or documentation related to Solution access that are provided to the User by the Ministry from time to time.

6. Review any audit logs or other reports relating to access to the Solution that are provided by the Ministry, to ensure that the User's end users are in compliance with the Agreement, including this Schedule.
7. Only provide access to Relevant PHI in the Solution to the User's End Users that require such access in order to perform their work on the User's behalf.
8. Ensure that the User's End Users understand the User's obligations under the Agreement, including this Schedule.
9. Do such other things as may be necessary in order to ensure that the User's end users comply with the requirements of this Schedule on the User's behalf.
10. Immediately notify the Ministry of any breaches of the Agreement, including this Schedule, any breaches of Applicable Law (including PHIPA) in connection with Relevant PHI accessed from or available through the Solution, or any other matter that could reasonably be regarded as a privacy or security breach in connection with the Solution.
11. Put in place policies and procedures to respond to and manage any relevant privacy or security issue or concern, including matters referred to in items 9 and 10 above.
12. Provide any assistance reasonably requested by the Ministry or any Other User in connection with any relevant privacy or security issue or concern, including matters referred to in item 10, above.
13. Put in place policies and procedures governing the collection, use and disclosure of Relevant PHI accessed in the Solution.
14. Review and approve the policies and procedures put in place in accordance with items 11 and 13 at a regular interval.
15. Not provide access to the Solution to any individuals that are not employees or under direct contract to the User.
16. Subject to any policies provided to the User by the Ministry under item 5 above, if the User receives an access or correction request from any individual pursuant to Section 52 or 55 of PHIPA for Relevant PHI, it shall:
    (a) Where the request relates to Relevant PHI about the individual in the custody or control of the User, respond to the access or correction request; or
    (b) Where the request relates to Relevant PHI about the individual in the custody or control of an Other User, immediately notify the Other User that has custody or control of the Relevant PHI that relates to the individual and permit that Other User to respond exclusively to the request.
17. Regularly review and evaluate each of the User's end user's access permissions in the Solution, and adjust these permissions as is necessary to ensure that each of the User's end users only has access to the minimum amount of Relevant PHI in the Solution that they need in order to perform their work for the User.
18. Immediately deactivate a User's End User's account if that End User ceases to work for the User or no longer requires access to Relevant PHI in the Solution in order to do their work for the User.
19. Designate a contact person at all times for privacy matters relating to the Solution and advise the Ministry of the identity