This document (this "**Schedule**") is the Schedule for Services related to the ONE Network Service **("ONE Network Services")** made pursuant to the eHealth Ontario Services Agreement (the "**Agreement**") between eHealth Ontario and Client ("**Client**") dated **<effective date of SA: MMMM, dd, yyyy>** and is made effective as of **<this schedule signing date: MMMM, dd, yyyy>** (the "**Effective Date**"). ONE Network Services will be provided by eHealth Ontario upon Client's acceptance of the terms and conditions in this Schedule and eHealth Ontario's written confirmation that it has received and accepted that signed Schedule.

Full Name of Client

<Insert full client name from CIF>

1. Definitions

Unless otherwise specified in this Schedule, capitalised terms in this Schedule have the same meanings as those assigned to them in the Agreement:

"Client Systems" means the computer systems, peripherals, terminals, communications equipment and all related hardware owned or leased by Client that will be used by Client in connection with Client's use of the ONE Network Services;

"**Computer Application**" means any software program which is licensed to or owned by Client to further any of its legitimate business interests and used in connection with Client's use of the ONE Network Services;

"**ONE Network Client Form**" means the form completed jointly by Client and eHealth Ontario that contains contact and technical information used in connection with Client's use of the ONE Network Services;

"ONE Network Services" means the services provided by eHealth Ontario to Client to connect to eHealth Ontario's technology infrastructure and any related services through the managed private network operated by eHealth Ontario ("**ONE Network**"), as further described in section 2 below, and

"**Service Equipment**" means any equipment or software which may be selected by and provided by eHealth Ontario (or any Representative of eHealth Ontario) to Client in conjunction with the ONE Network Services including firewalls, routers, switches, media converters, modems, cables, fibre optic cable, panels, desktops/laptop/servers, cabinets, uninterruptible power supplies, terminal servers, or hardware tokens but not including any equipment that has been purchased by Client.

2. ONE Network Services

2.1 **Provision of Services.** When requesting ONE Network Services, Client should complete the ONE Network Client Form and complete, sign and submit this Schedule. The provision of ONE Network Services to Client is subject to the terms and conditions of the Agreement including this Schedule and its Exhibits, and eHealth Ontario's written confirmation that it can provide the ONE Network Services. No ownership in or to the ONE Network Services is transferred to Client by virtue of this Schedule and Client has only the limited right to access the Services as set out in this Schedule.

2.2 **ONE Network Services.** Each party will provide the other party with such information as the other party may reasonably require in connection with the ONE Network Services. Client acknowledges that the ONE Network Services are provided to Client solely for Client's own use and not for use by any other organization or person. Client will not permit any other organization or person to use the ONE Network Services.

2.3 **Client Obligations.** The Client agrees to provide an appropriate and secure environment for eHealth Ontario to install and locate the Service Equipment, and reasonable access to the site to deliver, install, maintain, inspect, disconnect or remove the Service Equipment. The Client will bear the local infrastructure cost of interfacing to and using the Service Equipment and ensure that any Service Equipment on its premises is protected from risk of loss or damage, in an environment which conforms to the relevant manufacturer's specifications. Client will be responsible for the loss of and risk or damage to the Service Equipment, except where caused by the negligence or wilful misconduct of eHealth Ontario,

and upon termination of the ONE Network Services (for any reason), the Client agrees to return all Service Equipment to eHealth Ontario.

2.4 **Client Equipment and Premises.** The Client will bear the cost and responsibility of engaging, acquiring and installing any necessary infrastructure it may need to access and use the ONE Network Services including any equipment, software, cabling, conduit, power, heating/cooling systems, entrance ducts, racks and shelving. In order to allow eHealth Ontario to perform its obligation under this Schedule, Client will obtain (at its cost) such rights or authorisations as may be necessary to allow eHealth Ontario to access or connect to any equipment or software used by Client in connection with the ONE Network Services. Client will permit eHealth Ontario reasonable access to Client's premises as may be necessary to enable eHealth Ontario to perform its responsibilities or to exercise its rights under this Schedule. When attending the Client's premises, eHealth Ontario will comply, and will cause its Representatives to comply, with such reasonable policies regarding access and security as are communicated in writing by Client.

2.5 **Service Equipment.** eHealth Ontario may replace or modify any item of Service Equipment, so long as doing so does not have a material adverse impact on the ONE Network Services. Service Equipment remains the property of eHealth Ontario or its Representatives, and the Client will not acquire any interest in, nor file or permit any liens or other encumbrances upon the Service Equipment.

2.6 **Change to the Services.** eHealth Ontario may, in its sole discretion, modify or upgrade the infrastructure that eHealth Ontario uses to provide the ONE Network Services, from time to time. Client is solely responsible for any modification or upgrade of its Client Systems or Computer Applications caused by the modification or upgrade of the infrastructure that eHealth Ontario uses to provide the ONE Network Services.

2.7 **Service Level Commitment.** eHealth Ontario will use commercially reasonable efforts to provide the ONE Network Services and makes no service level commitments in this Schedule or in connection with the ONE Network Services.

2.8 **Support.** eHealth Ontario will provide Client with technical support and assistance relating to the ONE Network Services through a help desk available by telephone. eHealth Ontario may change the applicable telephone number from time to time. eHealth Ontario does not guarantee that it will be able to verify or resolve all problems presented by Client to the help desk. Client acknowledges that Client, and not eHealth Ontario, is solely responsible for resolving any problems with Client's own technology infrastructure and for maintaining the accuracy of information contained in the ONE Network Client Form.

2.9 **Plain Language Descriptions.** Client acknowledges receiving from eHealth Ontario the plain language descriptions of the ONE Network Services, including a description of the safeguards pertaining to the ONE Network Services. The current copy of the plain language descriptions is attached to this Schedule as Exhibit "A" and is also available on line at www.ehealthontario.on.ca/en/services/one-network. eHealth Ontario may amend the plain language descriptions from time-to-time in accordance with the Agreement.

2.10 **Policies.** Client acknowledges receiving from eHealth Ontario the Acceptable Use Policy and security policy related to the use of the ONE Network Services. The current copy of the Acceptable Use Policy and security policy is attached to this Schedule as Exhibit "B" and Exhibit "C" respectively and is also available on line at www.ehealthontario.on.ca/en/services/one-network. eHealth Ontario may amend these policies from time-to-time in accordance with the Agreement.

3. Audit

Client authorises eHealth Ontario and its Representatives, upon five (5) days written notice and during business hours, to inspect any records and documents in the possession or under the control of Client relating to responsibilities of Client as provided under this Schedule. eHealth Ontario may exercise its rights under this section 3 to verify compliance with the terms and conditions of this Schedule and any applicable terms of the Agreement.

4. Term and Termination

4.1 **Term**. This Schedule will be effective as of the Effective Date and will continue unless terminated in accordance with sections 4.2 or 4.3.

4.2 **Termination for Convenience**. Either party may in its sole discretion, without liability, cost or penalty, and without prejudice to any other rights or remedies under this Schedule or at law or in equity, terminate this Schedule at any time upon giving at least ninety (90) days written notice to the other party.

4.3 **Suspension.** eHealth Ontario will be permitted to immediately suspend the provision of the ONE Network Services if it reasonably believes that there is an emergency or a circumstance that would warrant such action.

4.4 **Termination of Agreement**. This Schedule terminates automatically without liability, cost or penalty, and without prejudice to any other rights or remedies of eHealth Ontario under this Schedule or the Agreement or at law or in equity, should the Agreement expire or be terminated for any reason whatsoever.

4.5 **Effect of Termination**. Client acknowledges that upon termination of this Schedule all access to the ONE Network Services will be revoked.

4.6 **Survival**. In the event of any expiration or termination of this Schedule for any reason whatsoever, sections 4.4, 4.5 and 5 will survive.

5. Limitation of Liability

5.1 **Limitation.** Except as otherwise expressly set forth in this Schedule, in no event will either party be liable for indirect, special, consequential, incidental, punitive or exemplary losses, damage or expenses or for loss of data, lost revenue or lost profit, even if it has been advised of their possible existence, or even if same were reasonably foreseeable. The limit of a party's liability to the other party concerning performance or non-performance or in any manner related to this Schedule or the Agreement, for any and all claims will not in the aggregate exceed the greater of:

(i) $250,000.00 or

(ii) $5,000.00 multiplied by the number equal to all of the enrolments of any Registrant in any Sponsored Service initiated or completed by a Representative of Client

This limitation will apply irrespective of the nature of the cause of action, demand or claim, including breach of contract, negligence, tort or any other legal theory.

5.2 **Disclaimer.** eHealth Ontario expressly disclaims any representations, warranties, or conditions with respect to or arising from the ONE Network Services described in this Schedule whether express or implied, past or present, statutory or otherwise, including without limitation, any implied warranties and conditions of merchantable quality or fitness for a particular purpose.

6. General Provisions

Entire Agreement. With the exception of the Agreement and any other document attached thereto or referencing this Schedule, this Schedule constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes any prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties. The parties acknowledge and agree that the execution of this Schedule has not been induced by, nor have either of the parties relied upon or regard as material, any representations or writings whatsoever not incorporated and made a part of this Schedule. This Schedule includes the following Exhibits and Attachments, if any:

(a) Exhibit "A": Plain Language Description;
(b) Exhibit "B": Acceptable Use Policy; and
(c) Exhibit "C": Security Policy

eHealth Ontario and Client identified below have entered into an eHealth Ontario Services Agreement. The terms and conditions which apply to the ONE Network Services and related services are set out in the Agreement and this Schedule.

By signing below, Client is requesting the ONE Network Services and acknowledging that eHealth Ontario's provision of such services and Clients' use of such services will be in accordance with the terms and conditions of this Schedule and the Agreement.

Signature block has been removed for this sample

Exhibit A – Plain Language Description

1. Network Services. ONE Network allows health care providers to confidently share information over a high-speed network built for health care. When eHealth Ontario provides ONE Network Services to Client, eHealth Ontario is providing one or more telecommunications circuits to Client which will result in one or more networks under the control of Client being interconnected with eHealth Ontario's technology infrastructure. A circuit may be based on any one of a number of technologies such as a digital subscriber line, cable, satellite or fibre optic cable.

2. Security and Privacy Safeguards.

2.1 All eHealth Ontario Products and Services:

eHealth Ontario's security program is based on two standards from the International Organization for Standardization (ISO), as recommended by the Government of Canada:

- ISO/IEC 27002:2005, – Code of Practice for Information Security Management, and
- ISO/IEC 27001:2005, – Information Security Management Systems – Requirements.

and is in compliance with the *Personal Health Information Protection Act* and the *Freedom of Information and Protection of Privacy Act*. Security of information and protection of privacy within, and by use of, eHealth Ontario's products and services is achieved by collaboration of all parties who are partners in providing or using these services. For its part, eHealth Ontario has implemented the following safeguards:

(i) Administrative Safeguards

- eHealth Ontario regularly reviews and enhances its security policies. Staff and contractors read the relevant policies and sign that they have read and understood them.
- eHealth Ontario has mandatory security staff awareness and training programs.
- eHealth Ontario Staff and contractors generally have no ability or permission to access personal health information. If access to personal health information is required in the course of providing eHealth Ontario services, individuals are prohibited from using or disclosing such information.
- All staff and contractors must sign confidentiality agreements and undergo criminal background checks prior to joining eHealth Ontario. eHealth Ontario has a security screening policy that requires staff to have an appropriate level of clearance for the sensitivity of the information they may access.
- Client obligations, for their part in maintaining security, are detailed in individual contracts and Service Level Agreements (SLAs).
- eHealth Ontario ensures, through formal contracts/SLAs, that any third party it retains to assist in providing services to health information custodians will comply with the restrictions and conditions necessary for eHealth Ontario to fulfil its legal responsibilities.
- eHealth Ontario staff, consultants, suppliers and clients must promptly report any security breaches to eHealth Ontario for investigation.
- Security risk assessments are conducted as part of both product/service development and client deployments. Mitigation activities are well established and tracked as part of each assessment.
- eHealth Ontario provides a written copy of the results of a security risk assessment to the affected health information custodians.
- eHealth Ontario has established a formal risk management program, including an enterprise risk management policy and guidelines.
- eHealth Ontario conducts regular independent vulnerability assessments of technical configurations and operational security practices.

(ii) Technology Safeguards

- For access to sensitive systems, strong passwords, secure tokens, and other authenticators are required.
- Administrative access to all IT equipment is controlled via strong, two-factor authentication, and is recorded.
- eHealth Ontario monitors and manages network traffic using security mechanisms such as routers, switches, network firewalls, intrusion detection systems, and anti-virus programs.
- eHealth Ontario encrypts all data stored on staff computers.

(iii) Physical Safeguards

- The eHealth Ontario datacentres are purpose-built facilities, physically secured against unauthorized access, and are staffed and monitored continuously by security personnel.
- Datacentre physical security controls have been validated by an independent third party in accordance with federal government standards.

- eHealth Ontario requires escorted access at all times for third party vendors and maintenance personnel who require access to the datacentre.

2.2 ONE Network Safeguards. In addition to the generic safeguards which apply to all eHealth Ontario products and services, the following security safeguards are in place for ONE Network:

- ONE Network eHealth traffic is segregated from the Internet, and is protected by a defence-in-depth approach against threats originating from external networks.
- Clients are expected to take appropriate measures to segregate their own internal network(s) from untrusted networks.
- ONE Network equipment is deployed for exclusive use by eHealth Ontario to provide the ONE Network service, and is operated in accordance with eHealth Ontario practices and policies.
- ONE Network is implemented province-wide and makes use of dedicated optical fibre links and 3rd party carrier networks.
- Encryption using IPSec tunnels over 3rd party carrier networks ensures the security of eHealth communications traversing these networks.
- All Clients sign agreements that they will ensure ONE Network equipment on their premises will be located in physically secure environments that will be controlled and monitored.
- eHealth Ontario has implemented a full enterprise security and privacy incident management program.
- All changes to the network are controlled by eHealth Ontario and subject to formal eHealth Ontario change management practices.
- Administrative personnel have no access to the e-Health data flowing through the ONE Network.
- eHealth Ontario optionally segregates communications between selected client sites (e.g. for geographically separated offices)
- Every network point of access has controls for protecting the network from security threats, whether malicious or unintentional.

Exhibit B – Acceptable Use Policy

1. Summary

This policy establishes the acceptable use requirements for eHealth Ontario products and services, as well as the technology infrastructure used by eHealth Ontario to provide such products and services. eHealth Ontario may revise this policy from time-to-time in its sole discretion, and any revisions will be posted at http://www.ehealthontario.on.ca/en/services/one-network. Notice of any revision will be given to you in accordance with the agreement pursuant to which eHealth Ontario provides products or services to you.

2. Scope and Application

This policy applies to all users. Any person who accesses or uses the technology infrastructure or uses a product or service provided by eHealth Ontario is a "user". A "person" includes any individual, person, estate, trust, firm, partnership or corporation, government or any agency or ministry of any government, and includes any successor to any of the foregoing.

3. Accountability

Each client organization is responsible for any access or use of eHealth Ontario's products, services or technology infrastructure made by any user who is an individual and who obtained his or her passwords, secure tokens, digital certificates and any other identifiers **("credentials")** to access the technology infrastructure and any product or service provided by eHealth Ontario from that client organisation or at the direction of that client organisation.

4. Acceptable Use

Users are permitted to use eHealth Ontario's products, services and technology infrastructure solely for health care-related business activities.

5. Inappropriate and Unacceptable Uses

Users must not use eHealth Ontario's products, services or technology infrastructure in any manner that constitutes an inappropriate or unacceptable use, which include, but is not limited to:

a) the creation, collection, transmission, storage or exchange of any material in violation of applicable laws;
b) Defaming other persons (e.g., spreading false allegations or rumours about others);
c) Accessing, using, collecting, destroying, encrypting, altering or disposing of information in violation of any applicable laws;
d) Making, possessing or distributing computer programs that are designed to assist in obtaining access to computer systems in violation of applicable laws;
e) Promoting hatred against any identifiable group or individual by communicating such statements in violation of applicable laws;
f) Harassing other persons electronically (e.g., making threats to a person's safety or property);
g) Possessing, viewing, downloading, transmitting, or storing any pornography or any involvement whatsoever with the traffic of such material;
h) Using another user's password, secure token, digital certificates, or any other identifier to engage in any activity in violation of applicable laws;
i) Breaching copyright, trade secret, or other intellectual property rights (e.g., breaching software licences, pirating recorded music or movies or stealing trade secrets);
j) Wilfully bypassing or subverting eHealth Ontario's physical, logical or procedural safeguards such as firewalls, web-filtering software or other access controls;
k) Vandalism, which is defined as any malicious attempt to harm or destroy the information of another user, the Internet or other networks;
l) Harassment, including but not limited to persistent non-work related contact with another user when such contact is unwelcome or creating a poisoned work environment by accessing, displaying, storing, downloading or transmitting any content which is offensive;
m) The sending of unwanted email or unsolicited commercial or advertising material to any other person;
n) Deliberate unauthorised access to information, facilities or services accessible through the eHealth Ontario infrastructure;

o) Unauthorised use, collection, disposal, destruction, encryption, alteration or disclosure of any personal information, business trade secrets, or sensitive information provided by or obtained from eHealth Ontario;

p) Sending anonymous messages or impersonating any other person;

q) Selling, sharing or otherwise redistributing eHealth Ontario products or services without written authorization from eHealth Ontario;

r) Electronic gambling over the Internet; and

s) Any other activity that may expose eHealth Ontario to civil liability.

6. Security

6.1 Users must ensure that any credentials used by the user to directly or indirectly gain access to the products, services or technology infrastructure are safeguarded.

6.2 Users must immediately notify their client organization help desk or system administrator if they suspect or know that any credentials have been or may be breached or compromised.

6.3 Client organisations that suspect or know any credentials have been or may be breached or compromised must notify eHealth Ontario.

7. Breaches of This Policy

7.1 Users and client organisations must report all breaches of this policy of which they are aware to eHealth Ontario. Users must do so through the help desk from which they receive technical support, and client organisations must contact eHealth Ontario directly.

7.2 eHealth Ontario reserves the right to investigate suspected breaches of this policy, and users and client organisations will cooperate when asked to assist in any such investigation.

7.3 eHealth Ontario may, in its sole discretion, suspend or revoke a user's access to eHealth Ontario's products, services, or technology infrastructure should such user breach this policy.

7.4 Client organisations will cooperate with eHealth Ontario on the management of breaches of this policy. This responsibility includes, but is not limited to, assisting with the development and distribution of communications regarding breaches or incidents.

7.5 Breaches of this policy may result in criminal prosecution or civil liability.

7.6 Although eHealth Ontario is not obligated to monitor content and assumes no responsibility for any information or material that is transmitted by users of the products, services, technology infrastructure or Internet, eHealth Ontario reserves the right, subject to all applicable laws relating to the protection of personal information, to investigate content posted to or transmitted over eHealth Ontario's technology infrastructure and may block access to, refuse to post, or remove any information or material that it deems to be in breach of this policy.

7.7 eHealth Ontario may report breaches of this policy committed by a user to the client organisation responsible for that user's actions.

7.8 eHealth Ontario assumes no liability for enforcing or not enforcing this policy, and any failure by eHealth Ontario to enforce any part of this policy will not constitute waiver by eHealth Ontario of any right to do so at any time.

7.9 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.

Exhibit C – Security Policy

1. **Additional Definitions.** In addition to those definitions set out elsewhere in this Agreement, the following definitions apply to this Schedule:
   (a) "Client Equipment" means any equipment or software in the possession or control of Client that Client uses in conjunction with the Services that is not Service Equipment.
   (b) "Client Network" means any network(s) operated or controlled by Client up to the demarcation point where such network(s) interconnect with eHealth Ontario's technology infrastructure.
   (c) "ONE Network Remote" means the remote virtual private network.
   (d) "ONE Network" means the managed private network operated by eHealth Ontario.

2. **eHealth Ontario Safeguards.** eHealth Ontario has designed and implemented the ONE Network as a secure private network to be used by health care professionals when communicating with each other. For further information on the types of safeguards that eHealth Ontario uses, please contact eHealth Ontario.

3. **Client Data.** Client is responsible for any materials that Client transmits over the ONE Network and determining whether such materials can appropriately be transmitted over the ONE Network without encryption or other safeguards (given the nature and sensitivity of the materials being transmitted). If Client determines that any safeguard is required when transmitting such materials, Client will implement such safeguard. As well, Client is responsible for verifying the accuracy of any data that it receives over the ONE Network.

4. **Equipment.** Client is responsible for the security of the Service Equipment and Client's own tangible assets, including but not limited to Client Equipment, premises and utilities. This obligation includes maintenance of an inventory of Client's assets forming part of the Client Network, identification of possible risks and implementation of administrative, physical and technical means to secure such assets.

5. **Safeguards.** Client is responsible for managing the security of Client Equipment to reasonably limit the risk that Client Equipment will be accessed and used to attack the eHealth Ontario ONE Network or systems connected to it. This obligation includes but is not limited to establishing security policies and implementing appropriate physical, procedural and technical controls to prevent, detect and respond to security violations.

6. **No Changes.** Client will not connect to, modify, reconfigure, or alter the Service Equipment in any manner without the prior written approval of eHealth Ontario.

7. **Infrastructure and Environment.** Client will provide the infrastructure and environment necessary for the safe operation of the Service Equipment such as locating the Service Equipment in a dry, clean, well ventilated, and temperature controlled location and providing an appropriate uninterrupted power supply. All Service Equipment must be placed on a rack or appropriate shelf and positioned to provide ample working space in and around it.

8. **Compatibility.** From time to time, eHealth Ontario may provide to Client certain guidelines with respect to Client Equipment. Client acknowledges that it may not be able to receive and use the Services (because of compatibility issues) should its Client Equipment not conform to such guidelines.

9. **Client Network Security**. Client is responsible for the security and operation of Client Network, and Client will use organizational, administrative, physical and technical means to limit physical and virtual access to any computer terminal or other device interconnected with the ONE Network. Client will:
   (a) implement and regularly up-date reasonable anti-virus and anti-spam software on the Client Network;
   (b) regularly monitor the Client Network for security breaches;
   (c) implement such controls as are reasonably necessary to prevent security breaches relating to the Client Network and, in any event, use commercially reasonable efforts to minimize the impact of any security breaches on the Client Network; and
   (d) regularly monitor the Client Network and applications used on the Client Network in a manner consistent with good network administration practices.

10. **Access Control.** Client will use organizational, administrative, physical and technical means to protect any user identifications, passwords, secure tokens or other authentication credentials assigned to Client or Client's End Users that enable them to connect to the ONE Network or obtain services over the ONE Network.

11. **Passwords.** Should Client determine that a password or any other user authentication credential has been or may have been compromised, Client's Primary Contact (as set out in the client form at the start of this Agreement) will report that incident or concern to the help desk from which Client receives technical support.

12. **Program.** Client will establish its own security program that includes an incident response approach and risk management process. At a minimum, Client will, and will cause its End Users to, immediately report all actual or potential security incidents affecting the ONE Network or any network connected to the ONE Network of which they are aware to Client's Primary Contact who will immediately report them to the help desk from which Client receives technical support. When reporting any such incident, Client will provide all information that it is reasonably able to provide with respect to that security incident and reasonable assistance to enable eHealth Ontario to verify and resolve that security incident. eHealth Ontario will use commercially reasonable efforts to resolve each such security incident.

13. **Third-Party Networks.** Client is responsible for: (i) putting in place safeguards (such as security gateways and firewalls) to prevent any network traffic originating in a third party network from being routed through the Client Network directly to the ONE Network; and (ii) maintaining appropriate configuration and security controls over the Client Network to reasonably ensure that no person who has accessed the Client Network from a third party network may use any computing device forming part of the Client Network to gain unauthorized access to the ONE Network. If eHealth Ontario acting reasonably (after having given Client an opportunity to improve its security safeguards) determines that Client is unable to secure the Client Network as described in this section 13, Client agrees to relinquish such connections between the Client Network and any network other than the ONE Network as are needed to secure the Client Network in such a manner.

14. **Firewall.** eHealth Ontario recommends that Client deploy a firewall between the network equipment provided by eHealth Ontario and Client Network. Client will be responsible for creating and administering its own remote virtual private network solution, managing and administering their firewall, and ensuring that its firewall service performs network address translation (NAT) and stateful packet inspection.

15. **Local Area Network**. Client is responsible for managing its own local area network address space including the potential use of DHCP and DNS services, and for routing Client local area network address space.

16. Tools. Client will not run network contouring, vulnerability assessment, hacking tools, or configuration tools against any Service Equipment or any network circuits provided pursuant to this Agreement.

17. **Client Contact.** Client's Primary Contact is responsible for coordinating all matters relating to End User access (including password changes and the addition, modification or removal of End Users with eHealth Ontario) and will be the sole representative of Client who is authorized to communicate any related requests to eHealth Ontario.

18. **Compliance.** Upon the request of eHealth Ontario acting reasonably, Client will provide to eHealth Ontario evidence of its compliance with all or part of this Security Policy.