PRIMARY DATA SHARING AND SERVICES AGREEMENT

This Primary Data Sharing and Services Agreement is effective as of [Insert date. Delete this instruction.],

Between

HIS MAJESTY THE KING IN RIGHT OF ONTARIO
as represented by the MINISTER OF HEALTH
(the "**Ministry**")

And

[NTD: Insert legal name of the Land Ambulance Service Provider, Central Ambulance Communication Centre, or Air Ambulance Service Provider]
(the "**Contracting Participant**")

RECITALS

A. The purpose of this Primary Data Sharing and Service Agreement is to establish terms and conditions applicable to the provision and receipt of ambulance dispatch equipment and services between the Ministry, Land Ambulance Service Providers (LASPs), Central Ambulance Communication Centres (CACCs) and Air Ambulance Service Providers, and to document the privacy framework when these organizations share identifying information with each other as part of providing or receiving ambulance dispatch services.

B. The intention is to create a multi-party contractual framework with common terms at the provincial level and eliminate the need for bi-lateral agreements between the various organizations to create consistency and expediate access to new technologies and services. The structure of the framework is a participant agreement model: all participating LASPs and CACCs will enter into the same agreement directly with the Ministry and in doing so will take on obligations to one another as well as to the Ministry.

C. The framework will be scalable to allow the Ministry to add service-specific conditions and new services.

D. Ambulance dispatch services are the initial access point for Ontarians who are injured or ill and require emergency health services. A critical component of dispatch services is the 24/7/365 communication between ambulance communication officers within CCACs and paramedics employed by LASPs.

E. The Ministry provides emergency ambulance dispatch services to CACCs and LASPs, comprised of certain Ministry owned or licensed software, Equipment, and other components which comprise the Services.

F. The Contracting Participant is either a LASP, a CACC, or an Air Ambulance Service Provider uses the Services, and in doing so may share PI with the Ministry and/or other Participants for the Designated Purposes.

G. Each organization that enters into a Primary Data Sharing and Service Agreement with the Ministry is called a Participant. The Ministry is also a Participant in its role as an operator of

CACCs. Each Participant is an operator of communication or ambulance services within the meaning of the *Ambulance Act*, and wishes to access the Services and to share PI where reasonably necessary for one or more of the Designated Purposes or as permitted or required by law.

H. The Ministry is subject to FIPPA, the *Ambulance Act* and PHIPA and is a PHIPA Agent, HINP or Electronic Service Provider in providing the Services. The Ministry is also a health information custodian per s. 3(1)7 of PHIPA when it has custody or control of PHI as a result of or in connection with performing its own powers or duties, including its duty and power to operate communication services under s. 4(1)(c) of the *Ambulance Act*. Requirements associated with these four roles are set out in PHIPA and the PHIPA Regulation. This PDSSA is intended to satisfy the requirements under PHIPA for all four roles.

I. The Participants, other than the Ministry, are subject to the *Municipal Act*, *Ambulance Act*, PHIPA, FIPPA, MFIPPA and PIPEDA, as applicable.

J. All Participants are health information custodians with respect to the PHI in their custody or control. The Ministry is a health information custodian per s. 3(1)7 of PHIPA. LASPs are health information custodians per s. 3(1)4(v) of PHIPA. CACCs are health information custodians per s. 3(6) of the PHIPA Regulation or s. 3(1)4(i) of PHIPA. The Ontario Air Ambulance Services Corporation is a health information custodian per s. 3(5) of the PHIPA Regulation.

FOR GOOD AND VALUABLE CONSIDERATION, the receipt and sufficiency of which is acknowledged by each Party, the Parties covenant and agree as follows:

1. Definitions

In this Primary Data Sharing and ServicesAgreement, including the Recitals, the following terms have the following meanings.

1) **"Agreement"** means this Primary Data Sharing and Services including all attachments, as amended, supplemented or restated from time to time.

2) **"Applicable Law"** means all federal or provincial laws, regulations, common law, any orders, rules or by-laws that are applicable to the Participants, the Services, the Agreement or the Participant's obligations under the Agreement, which mayinclude the *Ambulance Act* and its regulations, PHIPA, FIPPA, MFIPPA, and any other legislation, as may be amended from time to time.

3) **"Authorization"** means a written direction respecting the processing of PI or PHI.

4) **"Authorized User**" means the Personnel of a Participant that the Participant authorizes to access the Services.

5) **"Authorized User Terms"** means the terms and conditions upon which an Authorized User is granted access to the Services substantially as set out in Attachment 5, as may be amended from time to time.

6) **"Business Day"** means any day except Saturday, Sunday or any statutory holiday in the Province of Ontario.

7) "**CACC**" means the legal operator of a "Central Ambulance Communication Centre", which provides communication services within the meaning of the *Ambulance Act*.

8) **"Confidential Information"** means information, including records, data and other information, in any form or medium, including PI, financial information, books and records, policies and procedures, computer technology, business information and other data, disclosed or made available by one Participant (the "**Disclosing Party**") to another Participant (the "**Receiving Party**") as a result of the relationship of the Participants under the Agreement or the provision of the Services by the Ministry, that is either marked or otherwise identified as confidential by the Disclosing Party at the time of disclosure, or is information that would at the time of disclosure be understood by theParticipants exercising reasonable judgment to be confidential, but, except with respect to PHI or PI, "Confidential Information" does not include information that:

   (i) is or becomes generally available to the public without fault or breach on the part of the Receiving Party of any duty of confidentiality owed to the Disclosing Party or to any third-party;

   (ii) the Receiving Party can demonstrate to have been rightfully obtained by the Receiving Party, without any obligation of confidence, from a third-party who had the right to transfer or disclose it to the Receiving Party free of any obligation of confidence; or

   (iii) has been developed independently by the Receiving Party without any reliance on the Disclosing Party's Confidential Information.

9) **"Contact"** means the person identified at the link referenced the Service Schedule as the contact for a Party.

10) **"Designated Purposes"** means the purposes set out in section 4 below.

11) **"Disclosing Party"** means Disclosing Party as defined in the definition of "Confidential Information" above.

12) **"Dispute"** means a Dispute as defined in section 12.

13) **"Electronic Service Provider"** means a person who supplies services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of PHI or PI and who is not a PHIPA Agent of the health information custodian.

14) **"Equipment"** means hardware including communication consoles, or portable communication devices.

15) **"FIPPA"** means the *Freedom of Information and Protection of Privacy Act* (Ontario) and its regulations as amended from time to time.

16) **"health care"** has the meaning ascribed thereto in PHIPA.

17) **"health information custodian"** has the meaning ascribed thereto in PHIPA.

18) **"HINP"** means a health information network provider as defined in the PHIPA

Regulation.

19) **"Intellectual Property"** means intellectual property, industrial and intangible of whatever nature and kind in any jurisdiction, including software, trademarks, official marks, brand names, business names, trade names, domain names, trading styles, logos, trade secrets, inventions, innovations, discoveries, developments, formulae, product formulations, compositions of matter, databases, works of authorship, works subject to copyright, guides, manuals and designs, and including modifications to any of the foregoing, in all cases whether patented or patentable, whether registered or unregistered, and in any medium whatsoever.

20) **"LASP"** means a "Land Ambulance Service Provider" who is a person who operates an ambulance service within the meaning of the *Ambulance Act*.

21) **"Moral rights"** has the same meaning as in the *Copyright Act* (Canada), as amended or replaced from time to time, and includes comparable rights in applicable jurisdictions.

22) **"MFIPPA"** means the *Municipal Freedom of Information and Protection of Privacy Act* (Ontario) and its regulations as amended from time to time.

23) **"Minister"** means such minister of the Crown as may be designated as the responsible minister in relation to the Agreement or in relation to any subject matter under the Agreement, as the case may be, in accordance with the *Executive Council Act*, as amended.

24) "**Ministry**" means, as the context requires, the Ministry of Health or such other ministry as may be designated in accordance with Applicable Law as the ministry responsible in relation to the relevant matter.

25) **"non-PHI"** means information that does not contain PHI.

26) **"Notice"** means a Notice as described in section 21.

27) **"Participant"** means a CACC, LASP or air ambulance service provider that has entered into a PDSSA with the Ministry and is listed at the link referenced in the Service Schedule, and for clarity, includes the Contracting Participant, as well as the Ministry in its role as operator of CACCs.

28) **"Participant's PI"** means in respect of a Participant, the PI (including PHI) in the possession of the Ministry that originated from that Participant.

29) **"Party"** means the Ministry or the Contracting Participant, and **"Parties"** means both of them.

30) **"Patient"** or **"Client"** means a patient or client receiving health care or communication or ambulance services under the *Ambulance Act* or its regulations, as applicable, from a Participant and, in respect of PI, the individual to whom it relates.

31) **"Primary Data Sharing and Services Agreement"** and **"PDSSA"** mean this Primary Data Sharingand Services Agreement, including all attachments to it.

32) **"Personnel"** means the employees, officers, subcontractors, agents (both PHIPA Agents otherwise), and other persons authorized by a Participant to access PI for any Designated Purposes, and for certainty includes Authorized Users.

33) **"PHI"** means personal health information as defined in PHIPA.

34) **"PHIPA"** means the *Personal Health Information Protection Act*, *2004* (Ontario) and its regulations as amended from time to time.

35) **"PHIPA Agent"** means an agent as defined in section 2 of PHIPA.

36) **"PHIPA Regulation"** means Ontario Regulation 329/04, as amended from time to time.

37) **"PI"** means information about an identifiable individual and includes PHI.

38) **"Privacy Breach"** means any actual or suspected theft, loss, or unauthorized access, use, disclosure, copying, modification, disposal or destruction of PHI or PI processed by (i) the Ministry when providing the Services, or (iii) a Participant when receiving the Services under the Agreement, whether inadvertent or intentional.

39) **"Privacy Officer"** means the person identified as the Privacy Officer of a Participant at the link referenced in the Service Schedule.

40) **"process", "processing" and "processes"** and grammatical variations thereof**,** means any use of or operation or set of operations which is performed upon or in connection with data or information, by any means and in any form or medium, including collection, recording, analysis, consultation, organization, maintenance, storage, adaptation, modeling, retrieval, disclosure or otherwise making available, combination, matching, erasure or destruction.

41) **"Receiving Party"** means Receiving Party as defined in the definition of "Confidential Information" above.

42) "**Record**" means a record of information however recorded.

43) "**Services**" has the meaning set out in the Service Schedule.

44) **"Service Schedule"** means the Service Schedule attached to and forming part of this Primary Data Sharing Services Agreement as Attachment 6.

45) **"Service-Specific Additional Terms"** means terms and conditions that apply to a Participant's access to a specific Service in addition to the terms of the Agreement and as further described in sections 6(4) and 7(7) of this Agreement.

46) **"Steering Committee"** means the committee if any, established pursuant to section 11.

2. Scope of Agreement

1) The Contracting Participant wishes to receive from the Ministry certain Services as described in the Service Schedule. The Contracting Participant may disclose PI to

and receive PI from the Ministry and or other Participants through its use of the Services.

2) The Contracting Participant may choose to access some or all of the Services and may change the Services it accesses by providing Notice to the Ministry. By accessing a Service, the Contracting Participant will take on the obligations of the Agreement as they apply to that Service.

3) The Contracting Participant agrees to be fully bound by, and subject to, all of the covenants, terms and conditions in the Agreement including as they apply to the Participants other than the Ministry and agrees that privity of contract is deemed to exist between Participants who are not the Ministry so that all applicable covenants, terms and conditions will be enforceable as between Participants who are not the Ministry.

4) For certainty, the Ministry will ensure that every Participant has entered into the same Agreement.

3. Relationship of the Participants

It is understood and agreed that:

1) in giving effect to the Agreement, no Participants will be, or be deemed to be, a partner, agent (other than a PHIPA Agent, if applicable) or employee of another Participant for any purpose, and that the relationship of each Participant to the Participants will be that of independent contractor; and

2) nothing in the Agreement will constitute a partnership or a joint venture between the Participants.

4. Designated Purposes

Each Participant will only collect, use and disclose PI, and will ensure that its Personnel only collect, use and disclose PI:

1) for the purposes of providing health care or assisting in providing health care in accordance with and as permitted by Applicable Law, including without limitation PHIPA;

2) for purposes of or relating to the discharge or exercise by a Participant of its rights, duties or powers under the *Ambulance Act* or its regulations, including for purposes relating to the provision, administration, management, operation, use, inspection, investigation or regulation of ambulance services, communication services or base hospital programs or the enforcement of the *Ambulance Act*; or

3) where the collection, use or disclosure is otherwise required or permitted by Applicable Law.

5. Compliance with Patient or Client Instructions

To the extent that a Participant has been made aware by a Patient or Client that they have restricted the collection, use or disclosure of PI, the Participant will not, and will ensure that its

Personnel do not, collect, use or disclose such PI except in accordance with the Patient's or Client's instructions unless otherwise required or permitted by Applicable Law.

6. Obligations of Participants

1) Each Participant will take all reasonable steps to ensure that PI is as accurate, complete and up-to-date as required for the purpose for which it is disclosed and used, as the case may be, or if unable to do so a Participant will promptly provide Notice to the other Participants, as applicable to such PI, as to any limitations on the accuracy, completeness and currency of such PI.

2) Without limiting the generality of the preceding, where a Participant has received instructions from a Patient or Client not to disclose PHI that the Participant considers reasonably necessary to disclose for the Designated Purpose the Participant will give the Participant or Participants to whom it otherwise would disclose the PHI Notice of its receiving such instructions.

3) Each Participant will comply with Applicable Law when collecting, using or disclosing PI and prior to disclosing or collecting PI under the Agreement, and prior to accessing and using the Services as permitted by the Agreement, will require each of its Personnel who is an Authorized User to be bound by the Authorized User Terms and to comply with Applicable Law and the Agreement.

4) When accessing a Service, the Contracting Participant will comply with any Service-Specific Additional Terms that apply to that Service and will ensure that, prior to accessing a Service, each of its Authorized Users has agreed to be bound by any Service Specific Additional Terms that apply to that Service.

5) The Contracting Participant will report to the Ministry any changes in its own information practices or electronic information systems, that could have a material adverse effect on its data sharing under the Agreement or on the Services. The Ministry in its sole discretion, may refer any such matter to the Steering Committee, if any.

6) The Contracting Participant will ensure the integrity, availability and good working order of its own electronic information systems (and all related components and interfaces, hardware and software), and of those of its Authorized Users, that:

    i. are owned or operated by the Participant or such Authorized Users; or

    ii. are operated on behalf of the Participant or such Authorized Users,

    to ensure such systems do not adversely impact or delay the data sharing under the Agreement or the Services provided to any other Participant.

7) The Contracting Participant will maintain active and up-to-date anti-virus protection on all computer hardware or devices that its Authorized Users use to access the Services.

8) Each Participant will have in place systems, internal controls, policies and procedures, including administrative, technological and physical safeguards that

meet or exceed industry and regulatory requirements and standards, to ensure only authorized access to PI and to prevent the disruption, theft, loss and unauthorized access, copying, modification, use, disclosure or disposal of PI.

9) Each Participant will maintain internal controls, policies, procedures and systems that guide the retention and destruction of PI held by it in connection with the Designated Purposes in accordance with Applicable Law.

10) **Intentionally left blank.**

11) Each Participant will notify forthwith the Ministry and each other affected Participant of any Privacy Breach or suspected Privacy Breach involving the Services of which it becomes aware. A Participant is affected by a Privacy Breach if its information is involved. All affected Participants will collaborate and cooperate, to the extent reasonably required, to investigate, resolve and remediate privacy and security-related incidents that affect or that are likely to affect PI.

12) The Contracting Participant will provide Notice to the Ministry forthwith upon becoming aware of a software error in connection with the Services including (i) any software coding error; or (ii) failure of software to substantially perform in accordance with the applicable specifications.

13) The Contracting Participant will conduct a privacy and security self-assessment, if required by the Ministry, at its own cost and submit the results of the self-assessment in accordance with the manner and frequency prescribed by the Ministry, provided that the Ministry will not request a privacy and security self-assessment more than once every contract year. The Ministry will ensure that the privacy and security self-assessment verifies that each Participant is maintaining a privacy program that will allow it to comply with its obligations under the Agreement provided that each Participant will not be required to provide information in such detail that disclosure could reasonably threaten the security of the Participant's electronic information systems. The Ministry will provide Participants with at least 30 Business Days' Notice of any change to the frequency or manner of submission.

14) Each Participant will designate a Contact and may, at any time from time to time, change their Contact by Notice to all Participants.

15) With respect to Equipment provided by the Ministry,

a. The Contacting Participant will make best efforts to ensure that its Authorized Users:
    i. use any Equipment provided by the Ministry carefully so as to avoid damage to the Equipment, to refrain from altering the Equipment, and only use the Equipment for the purposes and in the manner specified by the Ministry or the Participant; and

    ii. keep any Equipment provided by the Ministry in a secure location and take other reasonable steps to protect against loss or theft of the Equipment and to ensure no unauthorized person hasaccess to Equipment, including any specific steps required by the Participant, and immediately notify the Ministry if Equipment is lost, stolen or accessed by an unauthorized person.

b. In the event Equipment provided by the Ministry is lost or damaged, the Ministry may require reimbursement from the Contracting Participant in accordance with fee schedules incorporated into this Agreement as Service Specific Additional Terms.

7. Rights and Obligations of the Ministry in providing the Services

The following rights and obligations apply to the Ministry when providing the Services:

1) The Ministry will only use as much PI as reasonably necessary to perform its obligations under the Agreement and will make PI available only to those Personnel that require access in order to satisfy those obligations.

2) The Ministry will only use and disclose any PI it receives from the Contracting Participant or any other Participant as the case may be, as is permitted or required under the Agreement or Applicable Law.

3) The Ministry will ensure that any of its Personnel who have access to PI have agreed in writing to the same restrictions and conditions that applyto the Ministry with respect to PI.

4) The Services will be performed by the Ministry in accordance with Good Industry Practice. “Good Industry Practice” means using standards, practices, methods and procedures to a good commercial standard, conforming to Applicable Laws, and exercising that degree of skill and care, diligence, prudence and foresight that would reasonably and ordinarily be expected from a qualified, skilled, experienced, and, to the extent required by Applicable Law, licensed and certified person engaged in a similar type of undertaking in the Province of Ontario under the same or similar circumstances.

5) Despite sections 21 and 26 of the Agreement, the Ministry may amend or change all or part of the Services or the Authorized User Terms by providingsixty (60) days advance Notice to the Participants through the Ministry’s website at the link in the Service Schedule. The Contracting Participant acknowledges this method of Notice and agrees within sixty (60) days of receiving such Notice to either comply with the changes to the Services, or to the Authorized User Terms, or to stop accessing the Service to which they relate.

6) Despite section 21 and 26 of the Agreement, the Ministry may apply Service-Specific Additional Terms to any Service it provides under the Agreement, and may amend or change all or part of existing Service-Specific Additional Terms, by providing sixty (60) days advance Notice to the Participants through the Ministry’s website at the link in the Service Schedule. The Contracting Participant acknowledges this method of Notice and agrees within sixty (60) days of receiving such Notice to either comply with any new or modified Service-Specific Additional Terms or to stop accessing the Service to which they relate.

7) In addition to its other express obligations under the Agreement, the Ministry may, for the purposes of ensuring compliance with the Agreement, make recommendations that specific privacy or security audits, reviews or assessments be conducted of the privacy or information security practices of one or more of the Participants at their own cost.

8. Confidential Information

Except with respect to PI collected by a Participant pursuant to the Agreement (which will be governed by the other provisions of the Agreement including section 6) each Receiving Party will:

1) keep all Confidential Information of a Disclosing Party confidential and secure, using at least the same degree of care to protect that Confidential Information as it uses to protect its own Confidential Information of a similar nature, and in any event, no less than a reasonable degree of care;

2) not disclose or use, or allow to be disclosed or used, in any manner whatsoever, other than as expressly contemplated by the Agreement, as may be required to carry out the terms of the Agreement, or as may be required for the Ministry to perform the Services, and then only on a need-to-know basis, any Confidential Information of a Disclosing Party, either during the term of the Agreement or at any time thereafter, except with the prior written consent of such Disclosing Party;

3) ensure that all Personnel of the Receiving Party who have access to Confidential Information of the Disclosing Party are informed of the confidential nature of that Confidential Information so as to know to keep such information confidential as required by the Agreement, and not use it for any purpose except as permitted under the Agreement; and

4) provide Notice to the Disclosing Party promptly in the event of a breach of obligations under this section 8, or loss of, or inability to account for, any of the Disclosing Party's Confidential Information.

The Participants acknowledge and agree that any Confidential Information of a Participant provided to another Participant under the Agreement will be a copy of the Confidential Information. Following the termination or expiry of the Agreement, the Receiving Party will, upon the demand of the Disclosing Party, securely destroy Confidential Information of the Disclosing Party that it is holding, without keeping any copies in any form or format, and provide the Disclosing Party with an attestation to the destruction by a senior officer or manager. Notwithstanding the preceding, a Receiving Party may retain Confidential Information of a Disclosing Party to the extent and for the period of time required by Applicable Law or as permitted by Applicable Law and required by a Participant's established internal policies, and the Receiving Party will continue to comply with this section 8 in relation to such retained Confidential Information.

For greater clarity, the obligation to destroy Confidential Information in the preceding paragraph does not apply to PI collected by a Participant from another Participant under the Agreement.

Notwithstanding the foregoing, the Participants acknowledge that certain Participants are bound by FIPPA or MFIPPA and that the Agreement and any information provided to a Participant in connection with its performance or otherwise in connection with the Agreement may be subject to disclosure in accordance with FIPPA or MFIPPA.

9. HINP/Electronic Service Provider/PHIPA Agent Obligations for the Services

A. General

1) Subject to the terms and conditions of the Agreement, the Ministry will provide Services to the Participants for the Designated Purposes, and Participants including the Contracting Participant will onlyuse the Services for the Designated Purposes.

2) The Ministry will make commercially reasonable efforts to provide the Services.

B. The following provisions apply where the Ministry is acting as a HINP, Electronic Service Provider or PHIPA Agent with respect to the Services.

1) **Status of the Ministry in respect of Records connected with the Services**

The Parties acknowledge and agree that (i) the Ministry is an institution under FIPPA and the Contracting Participant may be an institution under MFIPPA, and (ii) for the purposes of the Agreement the Ministry does not have custody or control of any Participant's Records related to the Services including on the basis that:

i. The Ministry is not creating the Records but only processing the Records on behalf of and for the sole benefit of the Participants;

ii. The Ministry has received the Records from the Participants as the creators thereof, and in some cases the health information custodians with respect to PHI, only to provide the Services for the Designated Purposes and not for any other purposes;

iii. The Ministry would not otherwise have any right, entitlement or interest in or to the Records but for this Agreement

iv. The Records do not relate to and are not used for the Ministry's core business or mandate other than for the purposes of providing the Services;

v. The Ministry has no right or authority to regulate theuse of the Records, such rights and authority being determined and prescribedby the Participants at their sole discretion within the confines of Applicable Law;

vi. The Ministry is restricted from viewing, accessing, using or manipulating the Records of a Participant, except (i) with prior Authorization from such Participant, or (ii) for the purposes of fulfilling its obligations to the Participant under this Agreement and not for any other purpose except where permitted or required by Applicable Law;

vii. The Participants have supplied the Records in confidence, have required that they be kept strictly confidential and restricted the ability of the Ministry to disclose the Records to any other person or entity except as prescribed in the Agreement for the sole benefit of the Participants or where permitted or

required by Applicable Law; and

viii. The Ministry cannot retain or dispose of the Records except as permitted by the Agreement or as otherwise directed by the Participants or permitted or required by Applicable Law.

2) **Security Standards and Procedures**

The Ministry will protect and ensure the confidentiality of all Confidential Information including PI processed by it pursuant to the Agreement with the physical, organizational and technological safeguards and security standards and procedures set out in Attachment 3.

3) **HINP Obligations**

In the event that it provides the Services to the Participants asa HINP, the Ministry covenants and agrees that it will:

a. provide to each Participant a plain language description of the Services that it provides, that is appropriate for sharing with the individual to whom the PHI relates, including a general description of the safeguards in place to:

    i. protect against unauthorized use and disclosure; and

    ii. to protect the integrity of the information;

    such plain language description to be substantially in the form set out in Attachment 1;

b. make available to each Participant for the purposes of providing it to the public if required,

    i. the description referred to in subparagraph (a);

    ii. any directives, guidelines and policies that apply to the Services, to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information; and

    iii. a general description of the safeguards implemented by the Ministry in respect of the Services in relation to the security and confidentiality of the PHI substantially in the form set out in Attachment 3;

c. on request of any Participant provide, to the extent reasonably practical and in amanner that is reasonably practical, an electronic record of:

    i. all accesses to all or part of the Participant PHI being held in Equipment controlled by the Ministry, which record will identify the person who accessed the information and the date and time of the access; and

ii. all transfers of all or part of the Participant PHI by means of Equipment controlled by the Ministry, which record will identify the person who transferred the PHI and the person or address to whom it was sent, and the date and time it was sent; such electronic record to be substantially in the form set out in Attachment 2;

d. perform and provide each Participant with a written copy of the results of an assessment of the Services with respect to:

i. threats, vulnerabilities and risks to the security and integrity of the PHI processed by it; and

ii. how the Services may affect the privacy of the individuals who are the subject of the PHI;

e. ensure that any third party it retains to assist in providing the Services agrees to comply with the restrictions and conditions that are necessary toenable the Ministry to comply with this section 9;

f. comply with the PHIPA Regulation and without restriction have in place information practices that comply with the requirements of PHIPA and the PHIPA Regulation;

g. comply with its own information practices; and

h. take steps that are reasonable in the circumstances to ensure that:

i. PHI processed by it pursuant to the Agreement is protected against theft, loss and unauthorized use or disclosure; and

ii. the records containing the PHI are protected against unauthorized copying, modification or disposal.

4) **PHIPA Agent Obligations**

In connection with providing certain of the Services the Ministry processes Participant PHI. The Ministry and the Participants acknowledge and agree that in connection with its processing of Participant PHI on behalf of the Participants, including without restriction inproviding the Services the Ministry may be acting as the PHIPA Agent of the applicable Participants. In the event the Ministry is acting as a PHIPA Agent of a Participant, the Ministry acknowledges and agrees that it will process Participant PHI only in accordance with the Designated Purposes and in accordance with the Agreement, or as it may be additionally authorized or directed by any Participants and will not acquire any custody or control of any such Participant PHI.

The Participants hereby authorize the Ministry to process, on their behalf, all PHI of which they have custody or control and have provided to the Ministry or authorized the Ministry to collect, only for the Designated Purposes and as otherwise authorized by the Agreement. It is acknowledged and agreed that in acting as a PHIPA Agent, the Ministry is doing so only in the capacity in which the term PHIPA

Agent is defined in the Agreement and, unless specifically authorized in writing, is not acting as an agent of the Participants in any other capacity.

5) **Electronic Service Provider Obligations**

The Participants and the Ministry acknowledge and agree that, in providing certain of the Services the Ministry may be acting as an Electronic Service Provider and not a PHIPA Agent. In the event that it is acting as an Electronic Service Provider, the Ministry will not:

i. use any Participant PHI to which it has access in the course of providing the Services except as necessary in the course of providing the Services;

ii. disclose any Participant PHI to which it has access in the course of providing the Services to the Participants; or

iii. permit its Personnel to have access to the Participant PHI unless they agree to comply with the restrictions that apply to the Ministry under the Agreement.

6) **Notification of Unauthorized Access or Loss**

The Ministry will notify each affected Participant, at the first reasonable opportunity, but in any event no more than 2 Business Days after the Ministry becomes aware of (i) any use, disclosure (including being legally compelled), theft, or unauthorized access of PI by anyone including the Ministry or any ofthe Ministry's Personnel to whom the Ministry provided the Participant PI, and (ii) any Privacy Breach or suspected Privacy Breach, of which it is aware, by Notice in accordance with Attachment4 hereto, and will include in such notification the information set out in Attachment 4 heretoand will provide, as reasonably requested by each affected other Participant, all necessary cooperation and assistance in responding to the Privacy Breach or suspected Privacy Breach, it being understood that no notification of affected persons or regulatory or law enforcement authorities will be made without the express direction of the affected other Participant.

7) **Right of Inspection**

At the reasonable request of the Steering Committee if established, or otherwise of any Participant, any Participant or its authorized representatives will be granted the right to enter upon any premises of the Ministry at which the Ministry processes that Participant's PI pursuant to the Agreement, at any time during normal business hours, upon at least twenty-four (24) hours prior Notice, for the purposes of inspecting and auditing the Ministry's adherence to the provisions of the Agreement, including its security standards, systems and procedures and the level of adherence to and actual implementation of those standards, systems and procedures as required by the Agreement. For greater certainty, this right of inspection applies only to premises and locations that the Ministry has possession of or control over, and not to any premises or locations of third parties and every audit and every inspection will be subject to any reasonable limits imposed by the Ministry to protect PI and other sensitive information of any Participant, in accordance with the Ministry's obligations under the Agreement or any Applicable Law.

In the event that a Participant undertakes an inspection or audit pursuant to this section 9(7), that Participant will be responsible for its own costs and, upon request of the Ministry will compensate the Ministry for all reasonable costs incurred by the Ministry in relation to that inspection or audit, provided that if the audit or inspection reveals that the Ministry has not complied with the terms of the Agreement,the Ministry will be responsible for reasonable and necessary costs of remediation.

8) **Audit**

As reasonably requested by the Steering Committee if established, or otherwise by any Participant, the Ministry will have performed by its internal audit staff or by an external auditor appropriate audits to confirm the Ministry's compliance with its obligations in the Agreement, including the security measures used to protect PI and the systems and processes established and used by the Ministry with respect to the collection, use, disclosure, storage and handling of PI. The Ministry will provide summary reports of these audits to the Steering Committee or the Participant requesting, as applicable. The Ministry will promptly and properly respond to all reasonable inquiries from the Steering Committee or such Participant, as applicable, with respect to the Ministry's handling of PI and the Ministry's compliance with the Agreement.

The Ministry may require an audit where it has reasonable grounds to believe that a Participant is not complying with the terms of the Agreement or relevant Applicable Law.

In the event that the Ministry undertakes an audit pursuant to this section 9(8), the Participant that requested that audit will, upon request of the Ministry, compensate the Ministry or the Contracting Participant for all reasonable costs incurred by the Ministry in relation to that audit, provided that if the audit reveals that the Ministry has not complied with the terms of the Agreement, the Ministry will be responsible for all reasonable and necessary costs of remediation.

9) **Third Party Requests for Access**

The Ministry will refer to the applicable Participant all requests by third parties for access to their Participant's PI. The Ministry will not disclose any such Participant's PI to third parties,except with the prior written consent of the applicable Participant or as may be required by Applicable Law. In each circumstance in which the Ministry is authorized pursuant to the Agreement and Applicable Law to disclose PHI, it will disclose only such PHI as strictly is necessary in connection with such authorized disclosure.

10) **Records Retention**

Both during the term of the Agreement and after any termination or expiry thereof, the Participants will retain all PI governed by the Agreement for such period of time as is necessary to satisfy the requirements of the retention policies of the Participants which will comply with all Applicable Law.

10. Disclaimer and Limitation of Liability

The Contracting Participant assumes sole responsibility for its use of the Services and PI for any purpose including without limitation, the Ambulance Act and/or providing and assisting in providing healthcare to Patients.

Despite sections 15 and 16 of this Primary Data Sharing and Services Agreement, in no event will the Ministry: (i) or any other Participant be liable, regardless of the form of action, for loss of profits, revenue or goodwill or for any other indirect, incidental or consequential damages suffered by any other Participant as a result of Services or any other obligation performed or not performed underthe Agreement, whether or not the possibility of such loss or damages was disclosed by one Participant to another or reasonably could have been foreseen by a Participant; and (ii) be liable to any Participant for any theft or loss of PI or any use, disclosure or accessto PI by or to unauthorized persons except to the extent that it is caused by the negligence or malicious conduct of the Ministry or its directors, officers, advisors, agents, appointees or employees.

The foregoing paragraph of this provision will apply in any cause of action, including breach of contract, misrepresentation, negligence or other tort, whether or not there will have been a fundamental breach or a breach of any fundamental provision of the Agreement by a Participant and notwithstanding any election by a Participant to rescind the Agreement if so entitled.

EXCEPT AS SET OUT IN THIS AGREEMENT, THE SERVICES ARE PROVIDED “AS IS” AND “AS AVAILABLE” AND WITHOUT ANY REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES OF ANY NATURE OR KIND WHATSOEVER, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES OF OR RELATING TO ACCURACY, AVAILABILITY, CAPACITY, DELAYS, ERRORS, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES OR OTHER HARMFUL COMPONENT, MERCHANTABILITY, NON-INFRINGEMENT, PERFORMANCE, TITLE,OR WORKMANLIKE EFFORT, ALL OF WHICH ARE HEREBY DISCLAIMED BY THE MINISTRY TO THE FULLEST EXTENT PERMITTED BY LAW.

The Ministry does not represent or warrant that the Services will perform at 100% availability or be error-free. The Contracting Participant will maintain alternate means of disclosing and collecting PI for the purposes for which it uses the Services and down-time procedures for use when the Services are not available. As such, the Ministry will not be liable to the Contracting Participant for any damages solely due to the lack of availability of the Services for any reason. The Services are not guaranteed to be hacker-proof or otherwise not subject to theft or other security or like failures or for performance or functionality failures. The Ministry does not guarantee any specific result and will perform the Services in the manner described in the Service Schedule.

The Participants acknowledge that the Services are being provided to the Participants as a benefit for the Participants and their Patients and Clients. No Participant will seek recourse against the Ministry for damages arising out of or in connection with the Agreement except to the extent that it is caused by the negligence or malicious conduct of the Ministry or its directors, officers, advisors, agents, appointees or employees. The Participants agree to work with their insurers and risk managers to mitigate the risk of third party claims that could potentially flow from their use of the Services.

Without limitation, the Ministry has no responsibility or liability in relation to:

a. the accuracy of any data or information provided to it by any Participant;

b. any claims of infringement of Intellectual Property or other rights (includingmoral rights) from third parties in relation to the Services; or

c. verifying that any Participant is entitled, pursuant to Applicable Law, to collect, use, disclose, transfer any PI that is provided to the Ministry by such Participant.

11. Indemnification of the Ministry

Despite sections 15 and 16 of this Primary Data Sharing and Services Agreement, to the extent permitted by Applicable Law, each of the Participants will indemnify and hold harmless the Ministry and its directors, officers, advisors, agents, appointees and employees from andagainst all losses and proceedings, by whomever made, sustained, incurred, brought or prosecuted, arising out of, or in connection with anything done or omitted to be done by that Participant or that Participant's directors, officers, advisors, agents, appointees or employees in the course of the Agreement, except to the extent that such losses or proceedings are caused by the gross negligence or malicious conduct of the Ministry or its directors, officers, advisors, agents, appointees or employees. The obligations contained in this section will survive the termination or expiry of the Agreement.

12. Licence to Use the Services

(a) The Contracting Participant is granted a limited, non-exclusive, non-transferable right by the Ministry to access and use the Services, along with, any polices and other documentation related to the Services, (collectively, the "**Documentation**") provided by the Ministry to facilitate the use of the Services, only for its own internal use and benefit and only for the Designated Purposes. For greater certainty, the Contracting Participant agrees that such right does not include the right to sublicense or otherwise share, copy or modify all or any portion of the Services, or the Documentation. Each Participant is permitted to authorize and enable any number its of own Authorized Users to access and use the Services on its behalf. Despite sections 15 and 16 of the Agreement, the Contracting Participant will be responsible for the use of the Services by its Authorized Users and will cause each Authorized User to use the Services in accordance with the terms and conditions of the Agreement.

(b) If possible or applicable, the Ministry shall limit the scope of access to the Services for a particular Authorized User based on written instructions provided to the Ministry by the Contracting Participant at the time of onboarding of such Authorized User or at any time thereafter.

(c) The Ministry shall not permit any Authorized User to access the Services unless such Authorized User has confirmed agreement with the Authorized User Terms presented on the Services access splash page, substantially in the form of Attachment 5.

(d) The Contracting Participant will not:

(i) alter, reverse engineer, decompile or disassemble the Services;
(ii) use the Services or the Documentation except as authorized under the Agreement; or
(iii) permit third parties to use the Services or the Documentation in breach of the Agreement.

(e) The Contracting Participant acknowledges that the Services and the Documentation each constitute commercial trade secrets and proprietary information of the Ministry or its licensors. Except for the licence expressly provided in this section 10, nothing in the Agreement

transfers any right, title or interest, including any Intellectual Property right, ownership or title, in or to the Services or the Documentation.

(f) The Ministry represents and warrants to the Contracting Participant that, to the knowledge of the Ministry, the provision of the Services to, and use of the Services by, the Contracting Participant and its Authorized Users in accordance with the Agreement will not infringe the Intellectual Property rights of any third parties in Canada.

(g) In the event that there is a claim for intellectual property infringement brought by a third party against the Contracting Participant in relation to the provision of the Services to, and use of the Services by, the Contracting Participant and its Authorized Users in accordance with the Agreement, and the Ministry is able to seek damages under contracts in place between the Ministry and any third party subcontractors, agents or licensors with respect to any liability or losses incurred by the Contracting Participant with respect to such claim, then the Ministry may pursue such damages from the applicable subcontractors, agents or licensors and any such damages that are recovered by the Ministry will be shared, net of any and all costs incurred by the Ministry in pursuing such damages ("Net of Costs"), on an equitable basis as between all Participants who suffered losses, expenses, costs, damages or liabilities related to such claim. Notwithstanding the foregoing sentence, the total cumulative liability of the Ministry to the Contracting Participant in regard to any such claims shall be limited to the Contracting Participant's equitable share of the amount of damages recovered by the Ministry as described in this paragraph, Net of Costs.

(h) The Contracting Participant will only access the Services and use the Documentation in a manner that is consistent with Applicable Law and the Agreement.

(i) Where a third-party agent or licensor is involved in the provision of Services the Ministry will provide Notice of the third-party involvement to the Participants accessing that Service.

13. Steering Committee

1) The Participants may establish a Steering Committee for the purposes of reviewing the natureand scope of the data sharing under the Agreement and of the Services,overseeing matters relating to Client and Patient privacy and the confidentiality and security of PI, resolving Disputes, and any other responsibilities assigned to it by the Participants, with the approval of the Ministry from time to time. The Steering Committee will consist of a representative of the Ministry, and such representatives of such Participants as may be determined by the Ministry to be appropriately representative of all Participants, including appropriate regional and cross-functional representation.

2) The Steering Committee will meet as required. Such meetings may be held either in person or remotely. The Ministry will act as the secretariat for the Steering Committee and will have custody and control of all records generated by or for the Steering Committee and may be obligated to disclose those records pursuant to FIPPA or MFIPPA. A written status report will be produced by the Ministry reflecting the minutes of each meeting of the Steering Committee.

3) In addition to any express obligations of the Steering Committee set out in the Agreement, the Steering Committee may establish additional objectives for the Steering Committee in its terms of reference, which will be subject to review and approval by the Ministry, and

which, for greater clarity,may include but not be limited to the following:

(a) making recommendations to the Ministry regarding the termination of a Participant;

(b) reviewing and approving recommendations regarding the nature and scope of the Services that could be funded and presenting them to the Ministry for consideration;

(c) requesting an audit of the Ministry in accordance with section 9(8) above;

(d) subject to the Ministry's review and approval, stipulating privacy policies and procedures for Participants with respect to their use of the Services;

(e) making recommendations with respect to disagreements or disputes in accordance with section 14 below; and

(f) discussing any other matter or issue that is pertinent to the Agreement.

14. Dispute Resolution

Any disagreement or dispute between the Participants with respect to the performance of the Agreementor the interpretation of any provision of the Agreement ("**Dispute**") may be:

1) first referred to the chief executive officers of the affected Participants; and

2) failing resolution of the Dispute within thirty (30) Business Days of that referral, or such other period as agreed to by the affected Participants, referred to the Steering Committee which will make a recommendation.

The Participant or Participants seeking relief will provide the Participant or Participants from which the relief is sought with Notice setting out the matters in dispute, a concise statement of the facts on whichit relies and the resolution that it is seeking.

15. Injunctive Relief

Any Participant may seek injunctive or other interim relief from a court of competent jurisdiction from a breach or reasonably likely breach of the Agreement that has or may reasonably threaten the Intellectual Property rights of a Participant and their third party suppliers, or the confidentiality of PI or the privacy of the Patient or Client to whom it relates.

16. Third-Party Software

Any third-party software, including any third-party's plug-in, that may be provided with a Service is included for use at the option of the Participants. If a Participant chooses to use such third-party software, then such use will be governed by the third-party's licence agreement, if any. For certainty, the Ministry is not responsible for any third-party's software and will have no liability for a Participant's use of third-party software.

17. Indemnification

Notwithstanding anything else in the Agreement, any express or implied reference to the Ministry

providing an indemnity or any other form of indebtedness or contingent liability that would directly or indirectly increase the indebtedness or contingent liabilities of the Ministry or His Majesty the King in right of Ontario, whether at the time of execution of the Agreement or at any time during the term of the Agreement, will be void and of no legal effect. Consequently, notwithstanding anything else in the Agreement, the Ministry acting in its capacity as a Participant under the Agreement will not be subject to any indemnity obligation in the Agreement, and for clarity, will be excluded fromthe indemnity rights and obligations in the paragraph that follows below in this section 17.

Each Participant, excluding the Ministry, individually and not jointly and severally (an "Indemnitor"), agreesto indemnify, defend and hold the other Participants, (each an "Indemnified Party") harmless from any and all loss, damages, costs, liabilities, expenses and settlement amounts, which the Indemnified Party may incur or suffer or be required to pay arising out of or in any way relating to any claim by aParticipant or any third party made in respect of the Agreement, to the extent that the claim is due to thenegligence, malicious conduct or breach of the Agreement of the Indemnitor or its directors, officers,advisors, agents, appointees and employees. The indemnification obligations of the Indemnitor willbe subject to the following:

1) the Indemnified Party notifying the Indemnitor in writing within fifteen Business Days after its receipt of Notice of any claim;

2) subject to (4) below, the Indemnitor having sole control of the defence and all settlement negotiations and agreements related thereto so long as no unilateral actions are taken by the Indemnitor (including settlement) which are likely to have anadverse effect upon the Indemnified Party; and

3) the Indemnified Party providing the Indemnitor with reasonable assistance, information and authority necessary to perform its obligations under this section 14.

4) Despite (2) above, where the Indemnified Party is the Ministry, the Ministry may elect to participate in or conduct the defence of any such claim by notifying the Indemnitor in writing of such election without prejudice to any other rights or remedies of the Ministry under the Agreement, at law or in equity. Each Participant participating in the defence will do so by actively participating with the other's counsel. The Indemnitor will not enter into any settlement unless it has obtained the prior written approval of the Ministry. If the Indemnitor is requested by the Ministry to participate in or conductthe defence of any such claim, the Ministry agrees to co-operate with and assist the Indemnitor to the fullest extent possible in the defence of the claim and any related settlement negotiations. If the Ministry conducts the defence of any such claim, the Indemnitor agrees to co-operate with and assist the Ministry to the fullest extent possible in the defence of the claim and any related settlement negotiations. This section will survive any termination or expiry of the Agreement.

18. Insurance

1) Each Participant, other than the Ministry, represents and warrants that it has and will maintain for the term of the Agreement, at its own expense, with insurers having a secure A.M. Best rating of B+ or greater, or equivalent, all necessary and appropriate insurance that a prudent person in the business of that Participant would maintain including the following:

(a) **Commercial General Liability Insurance,** on an occurrence basis for third party bodily injury, personal injury and property damage, to an inclusive limit of not less than five million Canadian dollars (C$5,000,000) per occurrence. The policy will include the following:

(i) His Majesty the King in right of Ontario, her ministers, agents, appointees, employees and subcontractors as an additional insureds with respect to liability arising in the course of performance of the Participant's obligations under, or otherwise in connection with, the Agreement;
(ii) a cross-liability clause;
(iii) contractual liability coverage;
(iv) products and completed operations coverage; and
(v) 30-day written notice of cancellation, termination or material change.

(b) **Errors and Omissions Liability Insurance,** insuring liability for errors and omissions in the use of the Services, in the amount of five million Canadian dollars (C$5,000,000), per claim and in the annual aggregate.

2) Each Participant, other than the Ministry, represents and warrants that it has and will have for the term of the Agreement adequate financial resources to honour the indemnities set out in section 11 and 17 in the event of a failure to protect Confidential Information, which results in an identity theft or other wrongful emulation of the identity of an individual or corporation, failure or violation of the security of a computer system including, without limitation, that which results in or fails to mitigate any unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code.

(a) Upon request by the Ministry each Participant will provide the Ministry with proof of the adequacy of their financial resources to honour the indemnities in section 11 and 17 as described in section 18(2) in the form of:

i. **Security and Privacy Liability Insurance** in the amount of not less than two million Canadian dollars (C$2,000,000) per claim and in the annual aggregate;

ii. Audited financial statements of the Participant that, in the sole discretion of the Ministry prove the Participant has adequate financial resources for the purposes of this Section; or

iii. Audited financial statements of the Participant and proof of insurance that, in the sole discretion of the Ministry together prove the Participant has adequate financial resources for the purposes of this Section.

(b) If, upon reviewing a Participant's audited financial statements provided under this Section, the Ministry determines that a Participant does not have adequate financial resources to honour the indemnities, the Ministry may immediately terminate the Agreement without cause and without penalty, by providing Notice to the Participant.

3) Upon request by the Ministry a Participant will provide the Ministry with proof of the insurance required by the Agreement in the form of a valid certificate of insurance that references the Agreement and confirms the required coverage.

4) Each Participant will provide the Ministry with at least thirty (30) calendar days' advance Notice of any policy cancellation or any change in the amount of coverage or type of insurance stipulated. In no case will a Participant materially alter, cancel or allow a lapse in any insurance during the term of the Agreement.

5) The foregoing insurance provisions will not limit the amount or type of insurance otherwise required by law. It remains the sole responsibility of each Participant to determine the nature and extent of additional insurance coverage, if any, that is necessary or advisable for its own protection and to fulfill its obligations under the Agreement.

6) The obligations contained in this section will survive the termination or expiry of the Agreement.

19. Term, Termination and Suspension

1) The Agreement will remain effective, in respect of a Participant, until:

   (a) this Primary Data Sharing and Services Agreement is terminated by that Participant, or by the Ministry in respect of that Participant, as set out below; or

   (b) this Primary Data Sharing and Services Agreement is terminated by all of the Participants.

2) The Ministry may terminate the Agreement with respect to a Participant on the reasonable recommendation of the Steering Committee, or acting reasonably on its own initiative.

3) The Contracting Participant may terminate the Agreement;

   i. for any reason on 60 Business Days' prior Notice to all other Participants;

   ii. on Notice to all other Participants, if another Participant neglects or fails to perform or observe any material term or obligation in the Agreement and such failure has not been cured to the satisfaction of the Contracting Participant within fifteen (15) Business Days after Notice being provided; and

   iii. immediately on Notice in the event of an actual Privacy Breach caused by another Participant.

4) The Ministry may terminate this Primary Data Sharing and Services Agreement at any time, for any reason on six months' Notice to all of the Participants.

5) The Ministry may, at any time acting reasonably on its own initiative and in its sole discretion, suspend a Participant or Authorized User's access to all or part of the Services or any applicable technology or Equipment owned, licensed or provided by the Ministry.

6) On termination of the Agreement whether in respect of one or more or all Participants, theMinistry will ensure thatevery Participant in respect of whom the Agreement is

terminated promptly ceases to have access to the Services and returns any Confidential Information to the relevant Participant in a form and format deemed suitable by that Participant.

20. Interpretation

In the Agreement, unless otherwise specified, words in the singular include the plural and vice-versa. Words in one gender include all genders. The words “including” and “includes” are not intended to be limiting and mean “including without limitation” or “includes without limitation”, as the case may be. The headings do not form part of the Agreement. They are for convenience of reference only and do not affect the interpretation of the Agreement.

21. Additional Participants

A CACC or LASP who has entered into this Primary Data Sharing and Services Agreement with the Ministry will become a Participant. The Ministry will provide prompt Notice to the existing Participants of any new Participants and when the Agreement is terminated in respect of a Participant and in any event, within 5 Business Days of the joining or departure of a Participant. The Ministry will maintain the authoritative list of all Participants and what Services they are accessing on the website at the link in the Service Schedule.

22. Survival

Except as otherwise provided herein, those sections of the Agreement which, by the nature of the rights or obligations set out therein, might reasonably be expected to survive any termination or expiry of the Agreement will survive any termination or expiry of the Agreement, including, without limitation any privacy or confidentiality obligations, limitation of liabilities, or indemnification obligations.

23. Notice

Any Notice, request, demand or other communication to be given by a Participant under the Agreement will be in writing; delivered personally, by pre-paid courier, by any form of mail where evidence of receipt is provided by the post office, or by facsimile with confirmation of receipt, or by email where no delivery failure notification has been received. For certainty, delivery failure notification includes an automated ‘out of office’ notification. A Notice will be addressed to the Contact of the other Participant and at the address for that Participant as provided at the link referenced in the Service Schedule.

A Notice will be deemed to have been duly given one Business Day after delivery if the Notice is delivered personally, by pre-paid courier or by mail. A Notice that is delivered by facsimile with confirmation of receipt or by email where no delivery failure notification has been received will be deemed to have been duly given one Business Day after the facsimile or email was sent.

24. Assignment

A Participant may not assign this Agreement or any of its rights or obligations under the Agreement, directly or indirectly, without the prior consent of the other Participants, not to be unreasonably withheld. A Participant who is not the Ministry will not engage in any change of control (being an amalgamation, merger, or change in 50% or more of the voting shares) without providing 60 Business Day’s prior Notice to the other Participants. The Ministry may assign the

Agreement or any of its rights and obligations under the Agreement to any agency or ministry of His Majesty the King in right of Ontario and as otherwise directed by His Majesty the King in right of Ontario.

25. Further Assurances

Each Participant agrees to do, or cause to be done, all acts and things necessary to implement and carry into effect the Agreement to its full extent.

26. Entire Agreement

The Agreement constitutes the entire agreement between the Participants pertaining to the subject matter hereof and supersedes all prior understandings, agreements, collateral, oral or otherwise,negotiations and discussions, oral or written, existing between the Participants at the date of executionof the Agreement.

27. Severability

If any term or condition of the Agreement, or the application thereof to the Participants or to any persons or circumstance, is determined to be to any extent invalid or unenforceable, the remainder of the Agreement, and the application of such term or condition to the Participants, persons or circumstances other than those to which it is held invalid or unenforceable, will not be affected thereby.

28. Amendments, Waivers

(a) Except as expressly provided herein, the Agreement may be amended, modified or supplemented only by written agreement signed by each of the Participants. No waiver, alteration, amendment, modification, or cancellation of any of the provisions of the Agreement will be binding upon a Participant unless made in writing and duly signed all of the Participants.

(b) The Ministry and the Contracting Participant may amend the contact information for their representatives in section 8 of Attachment 1 by providing Notice to the other Party.

29. Use of insignia

No Participant will use any insignia or logo of another Participant except where it has receivedthe prior written consent of the other Participant to do so.

30. Governing Law

The Agreement will be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein. The Parties attorn to the exclusive jurisdiction of the courts of the Province of Ontario and all courts competent to hear appeals therefrom.

31. Counterparts

The Agreement may be executed in any number of counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

32. Electronic Signatures

The Parties agree that the Agreement may be validly executed electronically, and that their respective electronic signature is the legal equivalent of a manual signature. The electronic signature of a Party may be evidenced by one of the following means and transmission of the Agreement may be as follows:

(1) a manual signature of an authorized signing representative placed in the respective signature line of the Agreement and the Agreement scanned as a pdf and delivered by email to the other Party; or

(2) a digital signature, including the name of the authorized signing representative typed in the respective signature line of the Agreement, an image of a manual signature or an Adobe signature of an authorized signing representative, or any other digital signature of an authorized signing representative with the other Party's prior written consent, placed in the respective signature line of the Agreement and the Agreement delivered by email to the other Party.

33. Attachments

The Attachments that form part of this Primary Data Sharing and Services Agreement are as follows:

Attachment "1" - Plain Language Description of Services, and Security

Attachment "2" - Data Access and Transfer Log Procedures

Attachment "3" - Security Standards and Procedures

Attachment "4" - Privacy Breach Protocol Outline

Attachment "5" - Authorized User Terms

Attachment "6" - Service Schedule

In the event of any conflict or inconsistency between the main body of this Primary Data Sharing and Services Agreement and any attachment, the main body of the Agreement will govern unless specifically provided otherwise in an attachment.

IN WITNESS WHEREOF, the Parties have agreed to be bound by and have executed the Agreement.

HIS MAJESTY THE KING IN RIGHT ONTARIO as represented by the MINISTER OF HEALTH

Name: _____

Title: _____

Date: _____

Signature: _____

[**Insert full legal name of Contracting Participant. Delete this instruction.**]

Name: _____

Title: _____

Date: _____

Signature: _____

I have authority to bind [**Insert full legal name of Contracting Participant. Delete this instruction.**]

Name: _____

Title: _____

Date: _____

Signature: _____

I have authority to bind [**Insert full legal name of Contracting Participant. Delete this instruction.**]

Attachment 1 - Plain Language Description of Services and Security

1. WHAT SERVICES DOES THE MINISTRY OF HEALTH PROVIDE?

The Ministry of Health provides software and services that improve emergency access to care for Ontarians. It does this through the provision of services, equipment and software that allow operators under the Ambulance Act to track and manage patients who requireservices. Ambulance dispatch services typically replace paper-based processes in favour of an improved electronic process, ensuring that patients are managed safely and efficiently.

Ambulance dispatch services are the initial access point to Ontario's emergency health services system for many victims of illness or injury. A critical component of this service is the 24/7/365 communication between ambulance communication officers within Central Ambulance Communication Centers, and paramedics dispatched by Land Ambulance Service Providers.

2. WHERE DOES THE MINISTRY OF HEALTH GETPERSONAL HEALTH INFORMATION?

The Ministry collects PHI from 9-1-1 callers and patients as well as other sources in the delivery of emergency health services.

The Ministry of Health may also act as a health information network provider (HINP) as defined in s. 6(2) of O. Reg. 329/04 under PHIPA, as an electronic service provider for one health information custodian or as an agent of a health information custodian under a direct authorization from that custodian. In each of these three roles the Ministry of Health receives PHI from a health information custodian.

The Ministry of Health in its role as a HINP only processes personal health information as necessary to enable two or more health information custodians, who need to communicate urgently to provide emergency response services, to use electronic means to disclose personal health information to one another or as required or permitted by law. The Ministry of Health is not a health information custodian in respect of processing this personal health information.

3. HOW DOES THE MINISTRY OF HEALTH USEPERSONAL HEALTH INFORMATION?

When acting in a HINP or ESP role, the Ministry discloses personal health information only as necessary to provide those HINP or ESP services.

The Ministry, in acting as a HINP, is providing the services to facilitate the disclosure of personal health information between the operators of CACCs and ambulance services within the meaning of the Ambulance Act.

Pursuant to s. 10(4) of PHIPA a HINP, must comply with all prescribed requirements in the course of providing goods or services to the health information custodian.

Subsection 6(3) of O. Reg. 329/04 sets out requirements that the Ministry must comply with when providing the HINP Services.

4. TO WHOM DOES THE MINISTRY OF HEALTH DISCLOSE PERSONAL HEALTH INFORMATION?

The Ministry of Health does not disclose personal health information unless required by the health information custodians or permitted or required to by law.

5. WHAT SAFEGUARDS ARE IN PLACE TO PROTECT PERSONAL HEALTH INFORMATION?

The Ministry of Health rigorously protects personal health informationto ensure it is secure at all times and only accessed by those who have a need to access it to carry outtheir work. The Ministry of Health employs or is actively planning to employ the following safeguards to protect personal health information:

- All personal health information is hosted in secure, access-controlled facilities in Canada or in another jurisdiction being held to the same standards of privacy and security as if it were located in Canada.
- All information is encrypted while “at rest” (stored in a database) and “in transit” (being viewed in Ministry of Health software or solutions over the internet)
- Ministry of Health uses software access controls to limit access to its software solutions to authorized users
- Ministry of Health software solutions audit all user access to personal health information

6. WHAT POLICIES DOES THE MINISTRY OF HEALTH HAVE IN PLACE TO ENSURE PERSONAL HEALTH INFORMATION IS PROTECTED?

The Ministry of Health adheres to rigid privacy policies to ensure personal health information is protected. These policies include the following:

- All staff are aware of the purposes for which personal health information is collected and trained on their legal obligations to protect the information.
- Third parties acting on behalf of Ministry of Health are contractually obligated to protect personal health information to the same standard that the Ministry adheres to.
- Staff monitor security on a scheduled basis to detect for any possible breaches in security.
- Requirement to report any security incident to the affected health information custodian and to the Information and Privacy Commissioner where appropriate.
- The Ministry of Health has a privacy officer who is responsible for managing compliance with privacy requirements and implementing best practices as they relate to privacy software features and requirements.
- Personal health information is not used or disclosed for purposes other than those for which it was collected or as required or permitted by law.
- Personal health information is retained only as long as necessary for the fulfillment of the purposes above, and as required by law.
- Ministry of Health works with health information custodians to ensure that the data in their custody is as accurate, complete and up-to-date as possible.

7. CAN PATIENTS WITHDRAW CONSENT TO DISCLOSE PERSONAL HEALTH INFORMATION?

Yes. Patients may withdraw consent at any time provided they do so with their health information custodian as the Ministry of Health cannot process these requests. Patients also have the right to

restrict access to all or part of their personal health information. In either case, this is done by notifying the relevant health information custodian (usually, the patient's physician) who is a user of the Ministry of Health's services.

8. WHO MAY I SPEAK WITH IF I HAVE QUESTIONS ABOUT THE MINISTRY OF HEALTH's PRIVACY POLICIES AND PROCEDURES?

If you have complaint, question or concern regarding the Ministry of Health's privacy policies and procedures, please contact:

The Ministry

Mailing Address:

5700 Yonge St,
Toronto ON
M2M 4K5

Contact: Stuart Mooney**,** Director, Emergency Health Program Management and Delivery Branch
Email Address: Stuart.Mooney@ontario.ca

Contact: Heather Berios, Director, Emergency Health I&IT Solutions & Technology Management Branch
Email Address: Heather.Berios@ontario.ca

Attachment 2 - Data Access and Transfer Log Procedures

For each of the Services the Ministry provides to Participants, the Ministry will create or plan to develop the ability to create access and transfer logs:

1. an *Access Log* recording every access to all or part of the PHI associated with a Participant being held in Equipment controlled by the Ministry, which will include the following information: i) the person who accessed the PHI; and ii) the date and time of the access; and

2. a *Transfer Log* recording every transfer of all or part of the PHI associated with a Participant by means of Equipment controlled by the Ministry, which will include the following information: i) the person who transferred the PHI; ii) the person or address to whom the PHI was sent; and iii) the date and time it was sent.

Log files will also contain the following information that the Ministry currentlycollects:

1. PHI owner (of which Participant is the custodian)
2. Purpose of the disclosure (reporting, troubleshooting, etc...)
3. Format of information (paper/electronic/spoken/visual)
4. Safeguards applied during disclosure (reference a standard safeguard lookup)
5. Subjects the information was disclosed to
6. non-identifying client tracking number

Upon request by a Participant, the Ministry will make such logs available

Attachment 3 - Security Standards and Procedures

The physical, organizational and technological safeguards and security standards and procedures referenced in section 9(3) are as follows.

The Ministry uses administrative, technical and physical security standards and procedures based on GO-ITS 25.X standards and guidelines, good practices such as ISO 27001 and NIST to protect PHI and non-PHI processed by the Ministry pursuant to the network services as described in Attachment 1. These standards and procedures include but are not limited to those described below:

Administrative:

- Security & privacy policies and procedures
- Cyber Security training
- Confidentiality and non- disclosure agreements
- Security TRA & privacy PIA assessments for services provided
- Security roles and responsibilities are defined and documented
- Access rights on termination or change of employment
- Change management procedures
- Continuity plans for business services to continue
- A privacy incident response plan
- Processing of PHI and non- PHI data only according to contractual agreements
- Data transfers only according to established protocols.

Technical

- User Identification and Authentication
- Controls Against Malicious Code
- Offsite backups for production systems, configurations and development code.
- Server Hardening
- Computer Security
- Secure Disposal of Assets prior to disposal, lease return or retirement
- Servers are regularly patched according to the Ministry Vulnerability and Patch Management Policy
- Separation of development, test and operational facilities and roles
- Use of encryption for data transfer
- Use of network logging
- Network security and monitoring

Physical

- Security Perimeter of server rooms with restricted access
- After-hours restricted access

- Protection against environmental threats - heating and fire
- Third-party access to secure areas
- Video Monitoring
- Supporting Utilities are used to protect servers.
- Redundancy & Fault Tolerance to prevent the loss of integrity or availability of PHI and non- PHI

Attachment 4 - Privacy Breach Protocol Outline

The purpose of this Privacy Breach Protocol is to ensure that the Ministry, when processing PHI, responds promptly and effectively in the event of an actual or suspected Privacy Breach. For purposes of this Attachment 4, “Privacy Breach”means the actual or suspected theft, loss, or unauthorized access, use, disclosure, modification or destruction of PHI or PI processed by the Ministry providing Services under the Agreement, whether inadvertent or intentional.

In the event of a Privacy Breach, the Ministry will promptly send Notice of such Privacy Breach in any event no longer than 2 Business Days from first knowledge, to the affected Participant or Participants to the Contact listed at the link referenced the Service Schedule.

The Privacy Breach Protocol consists of the steps outlined below.

1. Reporting of suspected or actual Privacy Breaches

The Ministry Personnel must immediately report any Privacy Breach to their manager and to their director or in the director’s absence, to the Ministry’s Privacy Officer or equivalent position. The director (or delegate) will initiate an internal investigation to determine whether a Privacy Breach has or may have occurred, and will implement containment efforts as may be reasonable in the circumstances. This step will be undertaken concurrently with Step 2, Containment.

2. Containment

The director (or delegate) will initiate all reasonable steps to limit the impact of the Privacy Breach as quickly as possible. Containment efforts by the Ministry will vary depending on the nature of the Privacy Breach, including suspending access rights in cases of unauthorized access, retrieving any copies of PHI or ensuring the secure destruction thereof in cases of unauthorizeddisclosures, and suspending the transmission of PHI. All staff and Authorized Users of the Ministry systems are required to provide assistance in support of containment efforts when requested to do so.

3. Notification

In each instance of a Privacy Breach, the director (or delegate) will at a minimum include in the Notice to the affected Participant or Participants the following information:

- the date and time of the Privacy Breach;
- a description of the PHI involved in the Privacy Breach;
- the circumstances of the Privacy Breach, including the persons to or by whom any PHI has been disclosed or accessed;
- the actions being taken to contain the Privacy Breach and to prevent similar breaches from occurring in the future; and
- any other information that may be pertinent to the affected Participant or Participants.

4. Investigation and Assessment

The director (or delegate) will investigate every Privacy Breach to determine the scope and cause of the Privacy Breach, including the individuals who may have been involved with or are responsible for the Privacy Breach, and the nature and quantity of the PHI that is affected, and will evaluate the adequacy of the Ministry's administrative, technical and physical safeguards relating to the confidentiality and security of the PHI in light of the Privacy Breach. In the process, the director (or delegate) will consult with necessary parties. All Personnel including Authorized Users of the Ministry systems are required to provide assistance to support investigation activities when requested to do so.

Risks associated with the Privacy Breach will be assessed by the Ministry. The following factors are included in this assessment:

- the specific PI and PHI, if any, involved in the Privacy Breach, the sensitivity of that information and its possible misuses;
- the cause and extent of the Privacy Breach, including the risks of ongoing or further exposure of the information;
- the number and types of individuals affected by the breach; and
- foreseeable harms that may arise from the breach.

5. Documentation

In each instance of a Privacy Breach, the director (or delegate) will document all relevant information using a template report called a Breach Event Report template and will submit an incident report ticket to support Privacy Breach record-keeping. On request by one or more affected Participants, the Ministry or will provide the relevant Participant or Participants with preliminary and final reports in a timely manner.

The Ministry staff and third-party service providers will provide all relevant information to the Director, in support of the documentation process.

6. Remediation and Prevention

In each instance of a Privacy Breach, the director will determine what measures must be implemented to remediate or address the Privacy Breach and to prevent similar Privacy Breaches in the future. The director will then develop a plan to implement remediation and prevention measures. The plan and measures will address all requirements and recommendations, if any, stipulated by the Information Privacy Commissioner of Ontario and any requirements and recommendations, determined by the Ministry in its sole discretion to be reasonable and appropriate, of any Participant that was affected by the Privacy Breach, and any requirements of Applicable Law. The Ministry will execute and implement any such plan and measures within a reasonable time in all of the circumstances, including available resources.

This Privacy Breach Protocol is supported by detailed procedures adopted and maintained by the Ministry.

Attachment 5 - Authorized User Terms

Please read carefully, you are agreeing to be bound by these Authorized User Terms and Conditions.

You have been identified as an Authorized User by **[insert name of organization, delete this instruction]** (the "**Contracting Participant**"). The Contracting Participant has entered into a Primary Data Sharing and Services Agreement withthe Ministry of Health (the "**Ministry**") (collectively, the "**Agreements**") to enable its Authorized Users to access and use the Ministry or other participant services (the "**Services**") and possibly to share certain sensitive information of, and with, others.

When you access the Services you will be presented with a set of contract terms and conditions (the "Online Agreement") that you must read and agree to before you access and use the Services. The Online Agreement will be substantially similar to these User Terms and Conditions, but may have some differences. By accepting the Online Agreement electronically (for example, clicking "I Agree") or accessing or using the Services, you: (a) represent that you have been duly authorized by the Contracting Participant to access and use the Services; (b) further represent that the Contracting Participant has informed you of its obligations under the Agreements and you have agreed to comply with them; and (c) agree to bound by these Authorized User Terms as amended from time to time.

1. Additional Definitions

When used in these Authorized User Terms and Conditions, the following terms will have the following meanings:

(a) "**Agent**" has the meaning ascribed to it in PHIPA;

(b) "**Authorized User**" means an Agent of the Contracting Participant who is authorized toaccess PI in connection with one or more Agreements;

(c) "**Health Information Custodian**" has the meaning ascribed to it in PHIPA;

(d) "**Intellectual Property Rights**" means any and all registered and unregistered rights granted,applied for or otherwise now or hereafter in existence under or related to any patent, copyright,trade-mark, trade secret, database protection or other intellectual property rights laws, and all similar or equivalent rights or forms of protection in any part of the world;

(e) "**Personal Health Information**" has the meaning ascribed to it in PHIPA;

(f) "**PHIPA**" means the *Personal Health Information Protection Act, 2004* (Ontario) and the regulations thereunder as may be amended from time to time; and

(g) "**PI**" means information about an identifiable individual and includes Personal Health Information.

2. Access

In accessing and using the Services, I understand that I am acting as an Agent of the Contracting Participant. I have no rights or licence to access or use the Services in any other capacity or for any other purpose.

3. Registration

I agree that all information that I have provided to the Contracting Participant in connection with my access to the Services is accurate and complete. I agree to maintain and update such information as necessary, to keep it accurate, current and complete. I am responsible for keeping every password and all credentials that enable my access to the Services (my "**account**") secure; and I am responsible for all access and other activity that occurs with respect to my account. If I suspect any unauthorized use of my account, I will notify the Contracting Participant immediately.

4. Use of the Services

Restrictions on Use.

I will **NOT** use the Services for any of the following purposes:

(a) to access, collect, use, disclose, print, or copy Personal Information or other confidential or restricted information from or through the Services unless such access, collection, use, disclosure, printing or copying: (i) is authorized by the Contracting Participant; (ii) is necessary for the purpose of carrying out my duties as an Agent of the Contracting Participant; (iii) is not contrary to applicable law; (iv) complies with any conditions or restrictions that the Contracting Participant has imposed on me; and (v) does not, to my knowledge, contravene the Agreements;

(b) to print or otherwise copy Personal Information from the Services except as authorized by the Contracting Participant;

(c) to provide any false or misleading information to the Ministry, the Contracting Participant or any other users of the Services;

(d) to infringe any rights, including but not limited to Intellectual Property rights, or to violate acceptable use policies of any third party;

(e) to upload to or transmit from the Services any data, file or software that contains a virus, Trojan horse, work or other technologies that may harm any of the Services or the interests or property of the Ministry, the Contracting Participant or other Participants;

(f) to distribute spam, advertisements or other bulk messages;

(g) to hack or otherwise interfere with the proper functioning of the Services (including interference with or by-passing security features);

(h) to access the Services from a public network or other unsecure network;

(i) to reproduce, duplicate, copy, sell, resell, distribute or make available to any third party, modify, reverse engineer, decompile, disassemble or create derivative works of or from, or otherwise exploit for any purpose, any part of the Services, without the express written consent of The Ministry;

(j) to use the Services or Confidential Information, as defined in the Agreements, to enable, support, or otherwise aid the Contracting Participant or a third party in developing any product, software or service competitive with the Services or any of the Ministry' products or services;

(k) to use any robot, spider or other automatic program or device, or manual process to modify, monitor, copy, summarize, or otherwise extract information from the Services in whole or in part, except as necessary for the purpose of carrying out my duties as an Agent of the Contracting Participant in accordance with all applicable Agreements and for the "Designated Purposes" under each such Agreement;

(l) to post or submit any material or information into software in connection with the Services that:

1. is abusive, defamatory, discriminatory, offensive, irrelevant or unlawful;
2. I do not have the legal right to post or otherwise to publish or distribute; or
3. is for advertising or commercial purposes;

(m) to make, possess or distribute computer programs that are designed to assist in obtaining access to Ministry Services in violation of any agreement or applicable laws; or

(n) to remove, alter or destroy any trademarks, notice, proprietary codes, means of identification, or digital rights management information on, in or in relation to the Services.

In accessing and using the Services, I agree to:

(o) comply with all conditions or restrictions imposed by the Contracting Participant in respect of my collection, use, disclosure, retention or disposal of Personal Information in connection with the Services;

(p) comply with any policies and procedures prescribed and provided to me by the Ministry and the Contracting Participant in respect of the Services;

(q) participate in any training that the Ministry or the Contracting Participant may require in respect of the Services;

(r) keep all computer access codes (username and password) or access devices in respect of the Services secure and not share them with others;

(s) log out of the Services prior to ever leaving my computer or workstation unattended;

(t) maintain active and up-to-date anti-virus protection on the computer or device that I use to access the Services, unless maintained by the Contracting Participant in accordance with the Primary DataSharing and Services Agreement;

(u) notify the Contracting Participant immediately if I become aware of any potential or actual security or privacy breaches in respect of the Services, including but not limited to the loss, theft or unauthorized use or disclosure of any Personal Information;

(v) not collect Personal Information through the Services, nor use or disclose the Personal Information so collected, if and to the extent that I am aware that an individual has expressly withheld or withdrawn consent to such collection, use or disclosure;

(w) notify the Contracting Participant immediately if I become aware of a software error in connection with the Services including (i) any software coding error; or (ii) failure of software to substantially perform in accordance with the applicable specifications;

(x) keep confidential any information I acquire through my access to the Services that is either marked or appears by its nature to be confidential or proprietary information of the Ministry or any third party, including source code;

(y) use any Equipment provided by the Ministry carefully so as to avoid damage to the Equipment, to refrain from altering the Equipment, and to only use the Equipment for the purposes and in the manner specified by the Ministry or the Contracting Participant;

(z) keep any Equipment provided by the Ministry in a secure location, and to take other reasonable steps to protect against loss or theft of the Equipment and to ensure no unauthorized person has access to Equipment, including any specific steps required by the Contracting Participant, and immediately notify the Contracting Participant if Equipment is lost, stolen or accessed by an unauthorized person; and

(aa) comply with any terms dictated by a third-party as those terms relate to my use of third-party software. I acknowledge that:

1. The Ministry cannot and does not guarantee the reliability or accuracy of any third-party applications, nor does it endorse the content and information provided by third party applications,
2. The Ministry shall not be liable for any form of liability arising from my reliance on, or in connection with my use of third-party applications, and
3. Specifically for third-party mapping software or real-time routing information, I acknowledge that they are provided as optional use and may not align to the mapping information maintained by the Ministry's GIS team, or to the Ministry's systems or databases (such as CAD). Examples include but not limited to data and software used by Ministry tools and applications such as: Apple Maps, Google Maps, Waze, Maps.me.

5. No Transfer of Intellectual Property Rights

I understand that all right, title and interest in and to the Services, including all Intellectual Property rights arising out of or relating to the Services, are and will remain with the Ministry or the Contracting Participant and their third party licensors and service providers.

6. Use of Feedback

In the event that I provide the Ministry with any comments, suggestions, data, information or feedback in respect of the Services, I acknowledge and agree that all such feedback may be freely used by the Ministry or its third party suppliers, at their sole discretion, for the design, development, improvement, marketing, commercialization and operation of the Services and its other products and services, without any restrictions or other obligations to me based on confidentiality or Intellectual Property rights.

7. Term of Access

My right to access and use the Services will commence upon my first access to the Services and will terminate at the earlier of: (i) when the Contracting Participant has determined that I no longer require access to the Services; (ii) upon the expiration or termination of the Agreements; or (iii) where my

access to the Services has been suspended or withdrawn in accordance with these User Terms and Conditions or the Agreements.

8. Termination of Access by the Ministry

I understand that the Ministry will have the right to suspend my access to the Services at any time if: (i) the Ministry suspects, acting reasonably, that my account is being used for unauthorized access to other systems or information; (ii) I am using my account in a manner which has the potential to substantially degrade the performance or integrity of the Services; or (iii) I have failed to comply with these User Terms and Conditions. I understand that the Ministry will advise the Contracting Participant of the suspension and the reasons therefor.

9. Failure to comply

I understand that failure to abide by these Authorized User Terms will result in the withdrawal of access privileges to the Services, and may result in other actions or sanctions authorized by law.

10. Governing Law

These User Terms and Conditions will be governed by and construed in accordance with the laws of the Province of Ontario and the laws of Canada applicable in Ontario.

Attachment 6 – Service Schedule

1. Definition of Services

"**Services**" means all or part of the services or Equipment provided by the Ministry to the Contracting Participant and its Authorized Users as described in section 3 of this Service Schedule as amended from time to time, that comprise the ambulance dispatch services, as may be owned by, licensed or subscribed to by the Ministry from third parties, and includes any and all other information, data, documents, materials, works and other content, devices, methods, processes, hardware, software (including object and source code and related Documentation), and other technologies and inventions, and any technical or functional descriptions, instructions, requirements, plans, manuals or reports, that are provided or used by the Contracting Participant or its Authorized Users in connection with the installation, configuration, integration, operation, use, support or maintenance of the Services or otherwise comprise or relate to the Services, but expressly excludes: (i) PI; and (ii) information, data and other content that the Contracting Participant inputs into the Services

2. Participants and Contacts

A list of Participants and their Contacts can be accessed at the Ministry' website at: https://ontariogov.sharepoint.com/sites/EHPMDB/EHSPartnerSite/PDSSA

3. Services

The Ministry will provide the following information management, information systems and information technology services to the Participants as applicable, as amended from time to time.

Description of Ministry Services:

Services for Paramedic Services

I. Ambulance Dispatch Decision Support (ADDS)

Provides real time dashboards and reporting for live 911 operational decision support processes for Central Ambulance Communication Centre, Paramedic Service and Emergency Department stakeholders.

II. Ambulance Dispatch Reporting System (ADRS)

A web-based reporting system which provides historical reporting capability to query Ontario ambulance dispatch data for performance and trend analysis.

III. CAD Paging (SMS Texting)

Provides paramedic personnel with the ability to receive text messages on their mobile devices through business rules configured in the Computer Aided Dispatch (CAD) application.

IV. Real Time Data

A data service which enables medical 911 incident information to transfer in real-time from Central Ambulance Communication Centres (CACCs) to paramedic services. The Real Time Data (RTD) Service operates on a vendor-agnostic platform to enable the population of paramedic services

dashboards for situational awareness.

V. Real Time Data integration with Electronic Patient Care Record (ePCR)

A real-time data service which facilitates bi-directional 911 incident data exchanges between the Ministry's Computer Aided Dispatch (CAD) application and the paramedic services' ePCR solution. This service is vendor agnostic and automatically populates the CAD and the ePCR using a standardized data specification and electronic exchange.

VI. Real Time View (RTV)

The Real-Time View application provides a mobile application with a user interface for paramedic services supervisors to see real-time crew information such as location of vehicles, calls assigned and incident details.

VII. Mobile Computer Aided Dispatch (mCAD)

A mobile application that facilitates the digital exchange of real-time dispatch communications between Central Ambulance Communication Centres (CACC) and paramedics. mCAD enables CACCs to electronically notify paramedics of a call, provides routing functionality and allows paramedics to provide unit and incident status updates electronically back to the Computer Aided Dispatch (CAD) application.

VIII. Mobile Satellite (MSAT)

Provides primary and backup communication between CACCs and paramedics through a satellite push to talk radio system installed in an ambulance. Conversations via MSAT are recorded and become digital records.

IX. MOH Locator

An application available on ambulance computer notebooks, which takes an address (street name, number and municipality) entered by the user and generates a map of the area with a pointer marking the location.

X. Red Phone

A direct telephone service from dispatch centres to ambulance bases, used to reach the paramedic crews. It is also used as backup technology to notify crews of 911 calls in the event of an outage to the paging service. Conversations via red phone are recorded and become digital records.

XI. Trunked and Conventional FleetNet Radio, Hip and Base Paging (Legacy Radio network and equipment services)

Provides primary two-way radio communication between paramedics and CACCs. It includes in-ambulance radio services, mobile portable radio coverage via an ambulance as well as communication with hospital emergency departments. It also provides, base paging capability for CACCs to notify crews situated in an ambulance base. Conversations via the radio network are recorded and become digital records.

XII. New Public Safety Radio Network (PSRN) – Land Mobile Radio Services (PSRN network and radio equipment services)

Provides primary trunked and/or conventional (e.g. PCOM) two-way radio communication between paramedics and CACCs over the PSRN encrypted radio network. An air to ground solution is also included. It includes in-ambulance radio services, mobile portable radio coverage via an ambulance as well as communication with hospital emergency departments. It also provides, ambulance base call alerting (ABCA) capability for CACCs to notify crews situated in an ambulance base and in specific situations provides paramedic call back alerting (PCBA) solution. The new radio network is optimized to ensure the priority of communications for mission-critical public safety services. Conversations via the radio network are recorded and become digital records.

XIII. Automatic Vehicle Location (AVL) Aggregator

Receives and integrates into the Computer Aided Dispatch (CAD) system, real-time location information from Ambulance Service AVL software vendors to support 9-1-1 call dispatching by ACOs in CACCs. The Aggregator service operates on a vendor-agnostic platform to enable vehicle location integration in the CACC, regardless of the AVL vendors contracted locally by the ambulance service.