

## CONTRAT D'APPROVISIONNEMENT DE GRÉ À GRÉ

### DÉSIGNATION DES PARTIES

**ENTRE :** **LE MINISTRE DE LA SANTÉ ET DES SERVICES SOCIAUX**, pour et au nom du gouvernement du Québec, représenté par monsieur Luc Bouchard, sous-ministre associé, à la direction générale des technologies de l'information, dûment autorisé en vertu du Règlement 2 sur la signature de certains actes, documents ou écrits du ministère de la Santé et des Services sociaux (c. M-19.2, r.3), dont les bureaux d'affaires sont situés au 930, chemin Sainte-Foy, 6<sup>e</sup> étage, Québec (Québec) G1S 2L4;

ci-après appelé « le ministre »,

**ET :** **AKINOX SOLUTIONS INC.**, personne morale légalement constituée dont le numéro d'entreprise du Québec (NEQ) est 1166640020, ayant son siège au 2467, rue Bellevue, Lévis (Québec) G6W 2T8, représentée par monsieur Alexander Dahl, président, dûment autorisé tel qu'il le déclare;

ci-après appelée « le fournisseur ».

### LES PARTIES CONVIENNENT CE QUI SUIT :

1. Le fournisseur consent à fournir les biens et services ci-après décrits. Le présent contrat ainsi que les documents afférents constituent l'entente entre les parties à toutes fins que de droit. En cas d'incompatibilité, les stipulations du présent contrat auront préséance.
2. OBJET DU CONTRAT

Le 11 mars 2020, l'Organisation mondiale de la santé a déclaré une pandémie de la COVID-19. Le 13 mars 2020, le gouvernement du Québec a déclaré l'état d'urgence sanitaire. Par le décret numéro 177-2020 du 13 mars 2020 et par plusieurs décrets et arrêtés subséquents, le gouvernement et le ministre de la Santé et des Services sociaux ont pris différentes mesures pour protéger la santé de la population québécoise.

Le ministre retient les services du fournisseur qui accepte de livrer l'ensemble des biens et services suivants liés à la plateforme Trajectoire Santé Publique (TSP) :

- l'hébergement et l'infrastructure;
- l'abonnement annuel des licences;
- le soutien;
- les services professionnels de développement.

Cette plateforme a été développée afin de répondre à la situation d'urgence sanitaire provoquée par la pandémie de la COVID-19.

Pour davantage d'informations, veuillez-vous référer à l'annexe 2 « Description des besoins ».

**Définition :** « **Solution** » signifie (i) tous concepts, inventions, systèmes, procédés, techniques, méthodologie, savoir-faire, données, outils, maquettes, technologies (y compris les logiciels en codes exécutables et en codes sources), documentation ou tout autre information, données et matériels, et toute expression des précédents, développés par, propriétés de, habilités par le fournisseur avant la livraison/fourniture du Solution désigné dans le Contrat et (ii) toute amélioration, progrès ou dérivés développés par le fournisseur afin de fournir la Solution mentionnés dans le Contrat.

### 3. MONTANT DU CONTRAT

Le fournisseur sera rémunéré comme suit pour les biens fournis en vertu du présent contrat :

Le montant total à être versé pour l'exécution du présent contrat ne pourra être supérieur à dix millions deux cent dix mille dollars (10 210 000,00 \$) auquel s'ajoute les taxes de vente applicables.

	DESCRIPTION	QUAN -TITÉ	COÛT UNITAIRE	COÛT TOTAL
1)	Hébergement et infrastructure			
2)	Licences (abonnement annuel, entreprise – utilisation illimitée)			
3)	Support niveau 2			
4)	Services professionnels - développement			
Total				10 210 000,00\$

Pour l'exécution complète et entière des obligations prévues au présent contrat, sans autres frais, coûts ou dépens que ce soit et conformément aux modalités prévues à la clause 4 du présent contrat.

### 4. MODALITÉS DE PAIEMENT

	DESCRIPTION	FRÉQUENCE
1)	Hébergement et infrastructure	À la signature
2)	Licences (abonnement annuel, entreprise – utilisation illimitée)	À la signature
3)	Support niveau 2	À la signature
4)	Services professionnels – développement	À l'utilisation

Le fournisseur devra présenter au ministre, selon la fréquence mentionnée dans le tableau ci-dessus, pour les points 1 à 3, une facture contenant de façon générale l'information suivante : les dates, une description des biens rendus, le montant total de la facture ainsi que le numéro de contrat.

Le fournisseur devra présenter au ministre, mensuellement, pour la réalisation du point 4, une facture contenant de façon générale l'information suivante : les dates et les heures travaillées, la description des services rendus, le taux horaire, le montant total de la facture ainsi que le numéro de contrat.

Le ministre se réserve le droit de résilier ce contrat après six mois d'exécution s'il n'y a plus de situation d'urgence sanitaire. Pour ce faire, le ministre doit adresser un avis écrit de résiliation au fournisseur avec un préavis de 45 jours. Le fournisseur s'engage à rembourser le ministre au prorata d'utilisation, pour les points 1 à 3, en cas de résiliation sur la base du nombre de mois restants au contrat au moment de la résiliation, arrondi au nombre de mois restants le plus petit. Le remboursement sera effectué par chèque.

La facturation devra être acheminée à la personne désignée ci-après, à l'adresse suivante :

Direction des services administratifs – Informatique  
 Direction générale du financement, de l'allocation des ressources et du budget  
 Ministère de la Santé et des Services sociaux  
 1075, chemin Sainte-Foy, 16<sup>e</sup> étage  
 Québec (Québec) G1S 2M1  
 Téléphone : 418 266-6820  
 [REDACTED]

Après vérification, le ministre verse les sommes dues au fournisseur dans les 30 jours qui suivent la date de réception de la facture, accompagnée de tous les documents requis.

Le ministre règle normalement les demandes de paiement conformément aux dispositions prévues au Règlement sur le paiement d'intérêts aux fournisseurs du gouvernement (RLRQ, chapitre C-65.1, r.8).

Le ministre se réserve le droit de procéder à toute vérification des demandes de paiement déjà acquittées.

#### 5. DURÉE DU CONTRAT

Le présent contrat débute 3 avril 2021 et il prend fin à l'arrivée du premier des deux termes suivants: l'épuisement du montant maximal ou le 2 avril 2022.

#### 6. LIEU DE RÉALISATION DES TRAVAUX

Pour la réalisation des services professionnels du point 4, le fournisseur effectuera les travaux à distance.

#### 7. DOCUMENTS CONTRACTUELS

Les documents ci-annexés font partie intégrante du présent contrat comme s'ils y étaient au long récités. Le fournisseur reconnaît en avoir reçu une copie, les avoir lus et consent aux normes et aux conditions qui y sont énoncées.

Le présent contrat constitue la seule entente intervenue entre les parties et toute autre entente non reproduite au présent contrat est réputée nulle et sans effet.

#### 8. REPRÉSENTANTS DES PARTIES

Le ministre, aux fins de l'application du présent contrat, y compris pour toute approbation qui y est requise, désigne monsieur Luc Bouchard, sous-ministre associé, pour le représenter. Si un remplacement était rendu nécessaire, le ministre en avisera le fournisseur dans les meilleurs délais.

De même, le fournisseur désigne monsieur Alexander Dahl, président, pour le représenter. Si un remplacement était rendu nécessaire, le fournisseur en avisera le ministre dans les meilleurs délais.

#### 9. RESPONSABILITÉ DU MINISTRE

Sauf en cas de faute intentionnelle ou de faute lourde de la part du ministre, ce dernier n'assumera aucune responsabilité à l'égard de tous les dommages matériels subis par le fournisseur, ses employés, agents, représentants ou sous-contractants.

#### 10. OBLIGATIONS DES PARTIES

Le fournisseur s'engage envers le ministre à réaliser le mandat tel que décrit à la clause « OBJET DU CONTRAT ».

Le ministre s'engage à verser au fournisseur, moyennant les biens fournis, les montants visés à la clause « MONTANT DU CONTRAT », conformément aux modalités prévues à la clause « MODALITÉS DE PAIEMENT ».

#### 11. DÉFAUT D'EXÉCUTION DU CONTRAT

L'exécution du contrat devra cesser si le fournisseur est inscrit au Registre des entreprises non admissibles (RENA) en cours d'exécution et si le ministre n'obtient pas du Conseil du trésor dans les délais requis l'autorisation d'en poursuivre l'exécution.

Le cas échéant, le Conseil du trésor pourra notamment assortir son autorisation de conditions, dont celle demandant que le fournisseur soit soumis, à ses propres frais, à des mesures de surveillance et d'accompagnement.

Si le fournisseur ne peut poursuivre l'exécution du présent contrat en application du premier alinéa de l'article 21.3 de la Loi sur les contrats des organismes publics (RLRQ, chapitre C-65.1), il sera réputé en défaut d'exécuter ce contrat.

## 12. SOUS-CONTRAT

Lorsque la réalisation du présent contrat implique la participation de sous-contractants, sa réalisation et les obligations qui en découlent demeurent alors sous la responsabilité du fournisseur avec lequel le ministre a signé le contrat.

Le fournisseur doit, avant de conclure tout sous-contrat requis pour l'exécution du contrat, s'assurer que chacun de ses sous-contractants n'est pas inscrit au registre des entreprises non admissibles aux contrats publics (RENA) ou, s'il y est inscrit, que sa période d'inadmissibilité aux contrats publics est terminée. De plus, si le montant d'un sous-contrat est égal ou supérieur au seuil déterminé par le gouvernement, le fournisseur doit s'assurer que le sous-contractant est autorisé à contracter par l'Autorité des marchés financiers.

## 13. DROITS D'UTILISATION

En contrepartie du montant du contrat, le fournisseur accorde au ministre et au Réseau de la Santé et des Services sociaux (RSSS) un droit d'utilisation de la Solution non exclusif, irrévocable, transférable seulement aux établissements du RSSS, permettant une utilisation illimitée de la Solution que ce soit sans égard au nombre d'utilisateurs, au nombre d'établissements, d'installations, incluant les points de service, utilisant ladite Solution et à aucune limite territoriale.

L'accès par le public à la Solution, incluant le site web et autres outils, est limité dans le temps à la durée du Contrat, incluant les renouvellements, le cas échéant.

L'accès par le ministre et par le Réseau de la santé et des services sociaux aux rapports statistiques et extractions de données, fournis par le fournisseur pendant la durée du contrat, est valable pendant une année suivant la fin ou résiliation du contrat (incluant ses renouvellements) et doit être, ou selon le cas, demeurer indépendant du maintien d'un contrat d'entretien ou de maintenance actif, par exemple.

Toute considération pour ce droit d'utilisation de la Solution consenti en vertu du présent contrat est incluse dans le prix soumis. La contrepartie stipulée au Bordereau de prix tient lieu de toute redevance ou de toute royauté pour ces droits d'utilisation.

La documentation produite par le MSSS et transmise au fournisseur sur les processus, rapports statistiques et diagrammes sont et demeurent la propriété du ministre. La documentation produite par le fournisseur à la demande du ministre devient la propriété du ministre (Documents de gestion, M050, documents de formation sur la trajectoire, etc.).

Propriété des données : Le fournisseur reconnaît ne pas être propriétaire des données (saisies par les utilisateurs dans la Solution) et, ce faisant, il doit permettre au ministre ou, selon le cas, aux établissements et organismes du RSSS, d'y accéder selon les modalités prévues au Devis.

Nonobstant toute disposition contraire, aucune disposition du présent contrat ne modifie les droits du fournisseur quant à la propriété intellectuelle de la Solution, et le fournisseur n'accorde à l'autre partie le droit à la propriété intellectuelle de la Solution.

## 14. RESTRICTIONS D'UTILISATION

Le ministre, le réseau de la santé et des services sociaux et les établissements du RSSS ne doivent pas (i) concéder de sous licence, sous-licencier, vendre, revendre, transférer, céder, distribuer ou autrement exploiter commercialement ou mettre à la disposition de tout tiers



la Solution ou son contenu de quelque manière que ce soit; (ii) copier, reproduire, modifier ou créer des œuvres dérivées basées sur la Solution ou son contenu; (iii) «cadrer» ou «réfléter» tout contenu sur tout autre serveur ou appareil sans fil ou Internet (iv) « reverse engineer » la Solution; (v) créer un produit ou une Solution concurrentiel, (vi) construire un produit en utilisant des idées, des caractéristiques ou des fonctions similaires de la Solution ou (vii) «spider » la Solution ou autrement automatiser la collecte de données de la Solution par tout autre moyen que par le biais des utilisateurs, à l'insu du fournisseur.

#### 15. MODIFICATION DU CONTRAT

Toute modification au contenu du présent contrat devra faire l'objet d'une entente écrite entre les parties. Cette entente ne peut changer la nature du contrat et elle en fera partie intégrante.

#### 16. COMMUNICATIONS

Les communications et avis devant être transmis en vertu du présent contrat, pour être valides et lier les parties, doivent être donnés par écrit et être transmis par un moyen permettant de prouver la réception à un moment précis, aux coordonnées suivantes :

Pour le ministre :

Monsieur Luc Tremblay  
Directeur des mandats stratégiques  
Direction générale adjointe des licences et des systèmes d'information  
Direction générale des technologies de l'information  
Ministère de la Santé et des Services sociaux  
930, chemin Sainte-Foy, 6<sup>e</sup> étage  
Québec (Québec) G1S 2L4  
Téléphone : (581) 814-9100 poste 61797  
[REDACTED]

Pour le fournisseur :

Monsieur Alexander Dahl  
Président  
Akinox Solutions Inc.  
2467, rue Bellevue  
Lévis (Québec) G6W 2T8  
[REDACTED]  
[REDACTED]

Tout changement d'adresse de l'une des parties doit faire l'objet d'un avis à l'autre partie.

#### **LES PARTIES CONVIENNENT ÉGALEMENT CE QUI SUIT POUR LES SERVICES PROFESSIONNELS DE DÉVELOPPEMENT :**

#### 17. OBLIGATIONS DU FOURNISSEUR

Le fournisseur s'engage envers le ministre à :

- a) exécuter les travaux ou rendre l'ensemble des services décrits au présent contrat, ce qui inclut les travaux ou services qui, bien que non spécifiquement énumérés dans ce document, sont requis suivant la nature du présent contrat;
- b) collaborer entièrement avec le ministre dans l'exécution du contrat et tenir compte de toutes les instructions et recommandations du ministre relativement à la façon de préparer et d'exécuter le travail confié.

## 18. AUTORISATION DE CONTRACTER

En cours d'exécution du présent contrat, dans l'éventualité où le montant de la dépense est inférieur au montant déterminé par le gouvernement au regard de l'obligation de détenir une autorisation de contracter, ce dernier peut obliger le fournisseur et, dans le cas d'un consortium, les entreprises le composant ainsi que les entreprises parties à un sous-contrat rattaché directement ou indirectement à ce contrat, à obtenir une autorisation de contracter de l'Autorité des marchés publics dans les délais et selon les modalités particulières qu'il aura déterminés.

## 19. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

Le fournisseur, tel que stipulé au paragraphe 9) de l'article 15 des conditions générales décrites en annexe 1 du présent contrat, s'engage à :

**A.** ne conserver, à l'expiration du contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, en les retournant au ministre dans les 60 jours suivant la fin du contrat et remettre au ministre une confirmation que lui et les membres de son personnel ont retourné tous ces documents.

***Ou***

**B.** procéder, à ses frais, à la destruction des renseignements personnels et confidentiels en se conformant à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec ainsi qu'aux directives que lui remettra le représentant du ministre et transmettre à celui-ci, dans les 60 jours suivant la fin du contrat, l'Attestation de destruction des renseignements personnels et confidentiels jointe à l'annexe 6, signée par une personne autorisée qu'il aura désignée à cette fin.

***Ou***

**C.** confier la destruction des renseignements personnels et confidentiels à une entreprise de récupération, laquelle s'engage contractuellement à se conformer à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec ainsi qu'aux directives du ministre. Le fournisseur devra alors, dans les 60 jours suivant la fin du contrat de récupération, remettre au ministre l'Attestation de destruction des renseignements personnels et confidentiels jointe à l'annexe 6, signée par le responsable autorisé de cette entreprise.

Veuillez choisir une lettre (**A, B ou C**) :   **A**  .

## 20. CLAUSE FINALE

Tout engagement financier du gouvernement du Québec n'est valide que s'il existe, sur un crédit, un solde disponible suffisant pour imputer la dépense découlant de cet engagement conformément aux dispositions de l'article 21 de la Loi sur l'administration financière (RLRQ, chapitre A-6.001).

**EN FOI DE QUOI**, les parties ont signé le présent contrat en double exemplaire à la date indiquée ci-dessous :

**LE MINISTRE,**

**Luc Bouchard**

Signé avec ConsignO Cloud (12/04/2021)  
Vérifiez avec ConsignO ou Adobe Reader.



*Luc Bouchard, sous-ministre associé  
(Signature et date)*

**LE FOURNISSEUR,**

**Alexander Dahl**

Signé avec ConsignO Cloud (09/04/2021)  
Vérifiez avec ConsignO ou Adobe Reader.



*Alexander Dahl, président  
(Signature et date)*

**IMPORTANT : Le numéro de contrat doit être indiqué sur toutes les factures**

ANNEXE 1 – CONDITIONS GÉNÉRALES  
« Contrat de services de gré à gré »

1. LOIS ET RÈGLEMENTS APPLICABLES ET TRIBUNAL COMPÉTENT

Le fournisseur s'engage à respecter, dans l'exécution du présent contrat, les lois et règlements en vigueur au Québec applicables à l'exécution du présent contrat et en cas de contestation, les tribunaux du Québec seront seuls compétents.

2. ATTESTATION DE REVENU QUÉBEC

Tout fournisseur ayant un établissement au Québec doit, pour se voir octroyer un contrat de 25 000 \$ ou plus, transmettre au ministre une attestation délivrée par l'Agence du revenu du Québec, nommée « Attestation de Revenu Québec ». Cette attestation du fournisseur est valide jusqu'à la fin de la période de trois mois qui suit le mois au cours duquel elle a été délivrée.

De plus, l'attestation du fournisseur ne doit pas avoir été délivrée après la date et l'heure limites fixées pour la réception des soumissions.

Cette attestation indique que, à sa date de délivrance, le fournisseur a produit les déclarations et les rapports qu'il devrait produire en vertu des lois fiscales et qu'il n'a pas de compte payable en souffrance à l'endroit du ministre du Revenu du Québec, notamment lorsque son recouvrement a été légalement suspendu ou lorsque des dispositions ont été convenues avec lui pour en assurer le paiement et qu'il n'est pas en défaut à cet égard.

Un fournisseur ne peut transmettre une attestation de Revenu Québec qui contient des renseignements faux ou inexacts, produire pour lui-même l'attestation d'un tiers ou faussement déclarer qu'il ne détient pas l'attestation requise.

Il est interdit d'aider une personne, par un acte ou une omission, à contrevenir aux dispositions du paragraphe précédent ou, par un encouragement, un conseil, un consentement, une autorisation ou un ordre, de l'amener à y contrevenir.

**La violation des dispositions des deux paragraphes précédents constitue une infraction suivant le Règlement sur les contrats de services des organismes publics (chapitre C-65.1, r. 4) et rend son auteur passible d'une amende de 5 000 \$ à 30 000 \$ dans le cas d'une personne physique et de 15 000 \$ à 100 000 \$ dans les autres cas. En cas de récidive dans les cinq ans, le montant des amendes minimales et maximales prévues est doublé.**

3. DÉCLARATION CONCERNANT LES ACTIVITÉS DE LOBBYISME EXERCÉES AUPRÈS DE L'ORGANISME PUBLIC RELATIVEMENT À L'ATTRIBUTION D'UN CONTRAT DE GRÉ À GRÉ

Avant la signature du contrat de gré à gré, tout fournisseur doit produire le formulaire « Déclaration concernant les activités de lobbyisme exercées auprès de l'organisme public relativement à l'attribution d'un contrat de gré à gré » joint à l'annexe 3 et dûment signé pour se voir octroyer le contrat. Dans ce formulaire, le contractant déclare notamment qu'au sens de la Loi sur la transparence et l'éthique en matière de lobbyisme (RLRQ, chapitre T-11.011) et des avis émis par le Commissaire au lobbyisme :

- soit que personne n'a exercé pour son compte, que ce soit à titre de lobbyiste d'entreprises ou de lobbyiste-conseil ou de lobbyiste d'organisation, des activités de lobbyisme, préalablement à la déclaration;

- ou que des activités de lobbyisme ont été exercées pour son compte et qu'elles l'ont été en conformité avec cette loi, avec ces avis ainsi qu'avec le Code de déontologie des lobbyistes (RLRQ, chapitre T-11.011, r.2).

De plus, le contractant reconnaît que, si l'organisme public a des motifs raisonnables de croire que des communications d'influence non conformes à la Loi sur la transparence et l'éthique en matière de lobbyisme et au Code de déontologie des lobbyistes ont eu lieu pour obtenir le contrat, une copie de la déclaration pourra être transmise au Commissaire au lobbyisme par l'organisme public.

Ce formulaire doit être celui du ministre ou contenir les mêmes dispositions. Le défaut de produire cette déclaration pourra entraîner la non-conclusion du contrat.

#### 4. RESPONSABILITÉ DU FOURNISSEUR

Le fournisseur sera responsable de tous les dommages causés par lui, ses employés, agents, représentants ou sous-contractants dans le cours ou à l'occasion de l'exécution du présent contrat, y compris le dommage résultant d'un manquement à un engagement pris en vertu du présent contrat.

Le fournisseur s'engage à indemniser, protéger et prendre fait et cause pour le ministre contre tout recours, toute réclamation, toute demande, toute poursuite et toute autre procédure pris par toute personne en raison de dommages ainsi causés.

Nonobstant toute autre clause de ce contrat, l'entière responsabilité de chaque partie envers l'autre en cas de dommage, quelle qu'en soit la cause, et, quelle qu'en soit la forme d'action ou la cause d'action, que ce soit dans le contrat ou à tort (y compris par négligence), une responsabilité stricte, violation d'une condition essentielle au contrat, violation fondamentale ou tout autre violation, ne devrait pas dépasser 50% de la valeur du contrat.

En aucun cas, une des parties n'est redevable à l'autre pour des dommages particuliers indirects, punitifs, accidentels ou consécutifs, y compris, sans limitation, la perte de profits ou de revenus ou d'opportunités, les frais généraux, la perte de clientèle, la perte de données, le coût du capital, quelle qu'en soit la cause, même si de tels dommages sont prévisibles ou que les parties ont été avisées de la possibilité de tels dommages.

#### 5. REGISTRE DES ENTREPRISES NON ADMISSIBLES AUX CONTRATS PUBLICS (RENA)

Le fournisseur ne doit pas être inscrit au registre des entreprises non admissibles aux contrats publics (RENA) ou, s'il y est inscrit, sa période d'inadmissibilité aux contrats publics doit être terminée.

Par contre, le Conseil du trésor peut, lors de circonstances exceptionnelles, permettre à un organisme public ou à un organisme visé à l'article 7 de conclure un contrat avec une entreprise inadmissible aux contrats publics ou permettre à une entreprise de conclure un sous-contrat rattaché directement à un contrat public avec un sous-contractant inadmissible aux contrats publics. Le Conseil du trésor peut assortir cette permission de conditions, notamment celle que l'entreprise ou le sous-contractant inadmissible soit soumis, à ses frais, à des mesures de surveillance et d'accompagnement.

En outre, lorsqu'un organisme public ou un organisme visé à l'article 7 constate qu'il y a urgence et que la sécurité des personnes ou des biens est en cause, le dirigeant de cet organisme peut permettre de conclure un contrat avec une entreprise inadmissible aux contrats publics ou permettre à une entreprise de conclure un sous-contrat rattaché directement à un contrat public avec un sous-contractant inadmissible aux contrats publics. Le dirigeant de l'organisme doit toutefois en aviser par écrit le président du Conseil du trésor dans les 15 jours.

Les dispositions des deux paragraphes précédents s'appliquent également, avec les adaptations nécessaires, lorsqu'il s'agit de permettre la conclusion d'un contrat public ou d'un sous-contrat rattaché directement à un contrat public avec une entreprise qui ne détient pas une autorisation de contracter alors qu'une telle autorisation est requise.

## 6. COMPUTATION DES DÉLAIS

Aux fins de la computation des délais fixés au contrat, lorsque les délais prévus pour remplir une obligation expirent un jour non juridique, cette obligation pourra être valablement remplie le premier jour juridique suivant.

## 7. RÉSILIATION

7.1 Le ministre se réserve le droit de résilier ce contrat pour l'un des motifs suivants :

- a) le fournisseur fait défaut de remplir l'un ou l'autre des termes, conditions ou obligations qui lui incombent en vertu du présent contrat;
- b) le fournisseur cesse ses opérations de quelque façon que ce soit, y compris en raison de la faillite, liquidation ou cession de ses biens;
- c) le fournisseur lui a présenté des renseignements faux ou trompeurs ou lui a fait de fausses représentations;
- d) le fournisseur est déclaré coupable d'une infraction à la Loi sur la concurrence (L.R.C. (1985), c. C-34) édictée par le gouvernement fédéral relativement à un appel d'offres public ou à un contrat conclu avec une administration publique au Canada, sans toutefois avoir encore été inscrit au registre des entreprises non admissibles aux contrats publics (RENA).

Pour ce faire, le ministre adresse un avis écrit de résiliation au fournisseur énonçant le motif de résiliation. S'il s'agit d'un motif de résiliation prévu au paragraphe a), le fournisseur devra remédier au défaut énoncé dans le délai prescrit à cet avis, à défaut de quoi ce contrat sera automatiquement résilié, la résiliation prenant effet de plein droit à l'expiration de ce délai. S'il s'agit d'un motif de résiliation prévu au paragraphe b), c) ou d), la résiliation prendra effet de plein droit à compter de la date de la réception de l'avis par le fournisseur.

Le fournisseur aura alors droit aux frais, déboursés et sommes représentant la valeur réelle des biens fournis jusqu'à la date de la résiliation du contrat, conformément au présent contrat, sans autre compensation ni indemnité que ce soit (en considérant l'avance reçue, s'il y a lieu), et ce, à la condition qu'il remette au ministre tous les travaux déjà effectués au moment de la résiliation.

Le fournisseur sera par ailleurs responsable de tous les dommages subis par le ministre du fait de la résiliation du contrat.

En cas de poursuite du contrat par un tiers, le fournisseur devra notamment assumer toute augmentation du coût du contrat pour le ministre.

7.2 Le ministre se réserve également le droit de résilier ce contrat sans qu'il soit nécessaire pour lui de motiver la résiliation.

Pour ce faire, le ministre doit adresser un avis écrit de résiliation au fournisseur. La résiliation prendra effet de plein droit à la date de la réception de cet avis par le fournisseur.

Le fournisseur aura alors droit aux frais, déboursés et sommes représentant la valeur réelle des biens fournis jusqu'à la date de résiliation du contrat, conformément au présent contrat, sans autre compensation ou indemnité que ce soit et, notamment, sans compensation ni indemnité pour la perte de tous profits escomptés.

## 8. CESSION DE CONTRAT

Les droits et obligations contenus au présent contrat ne peuvent, sous peine de nullité, être cédés, en tout ou en partie, sans l'autorisation du ministre.

## 9. LANGUE FRANÇAISE

Le fournisseur doit respecter les dispositions de la Charte de langue française et ses règlements quant au statut et à la qualité du français, notamment pour tout ce qui touche :

- les inscriptions sur les produits, le matériel traitant du fonctionnement de l'appareil et de son entretien, les touches de fonction et les consignes, les inscriptions sur les contenants et sur les emballages (article 51);
- la documentation de base, incluant les modes d'emploi, les modes d'entretien, les consignes de sécurité et les certificats de garantie (article 51);
- les documents de formation à l'utilisation du produit et les documents relatifs aux appareils (article 52);
- l'assistance technique et tout document qui y est relié (article 141).

Lorsque les documents de référence ne sont pas disponibles en français, le ministre peut exiger que certains documents soient traduits, et ce, aux frais du fournisseur.

## 10. APPLICATION DE LA TPS ET DE LA TVQ

Ceci est pour certifier que les biens retenus en vertu du présent contrat sont requis et payés par le ministère de la Santé et des Services sociaux avec les deniers publics pour son utilisation propre et sont assujettis aux taxes de vente applicables (taxe de vente du Québec (TVQ) et taxe sur les produits et services (TPS) ou, le cas échéant, taxe de vente harmonisée (TVH)) et, par conséquent, ces taxes doivent être facturées.

## 11. REMBOURSEMENT DE LA DETTE FISCALE

L'article 31.1.1 de la Loi sur l'administration fiscale (RLRQ, chapitre A-6.002) et l'article 53 de la Loi facilitant le paiement des pensions alimentaires (RLRQ, chapitre P-2.2) s'appliquent lorsque le fournisseur est redevable d'un montant exigible en vertu d'une loi fiscale ou alimentaire. Ainsi, le ministre pourra transmettre tout ou partie du montant payable en vertu du présent contrat au ministre du Revenu, à sa demande, afin que ce montant soit affecté au paiement de cette dette.

## 12. CONFLITS D'INTÉRÊTS

Le fournisseur doit éviter toute situation qui mettrait en conflit soit son intérêt propre, soit d'autres intérêts, notamment, mais sans limiter la généralité de ce qui précède, l'intérêt d'une de ses ressources, d'une de ses filiales ou d'une personne liée; dans le cas d'un consortium, l'intérêt d'une des constituantes versus l'intérêt du ministre. Si une telle situation se présente ou est susceptible de se présenter, le fournisseur doit immédiatement en informer le ministre qui pourra, à sa seule discrétion, émettre une directive indiquant au fournisseur comment remédier à ce conflit d'intérêts ou résilier le contrat.

Le présent article ne s'applique pas à un conflit pouvant survenir sur l'interprétation ou l'application du contrat.

## 13. CONFIDENTIALITÉ

Le fournisseur s'engage à ne révéler ni ne faire connaître, sans y être dûment autorisé par le ministre, quoi que ce soit dont il aurait eu connaissance dans l'exécution du contrat.

## **LES CONDITIONS GÉNÉRALES SUIVANTES S'APPLIQUENT POUR LES SERVICES PROFESSIONNELS DE DÉVELOPPEMENT :**

## 14. RESPONSABILITÉS DU FOURNISSEUR

Malgré la clause 4 de l'annexe 1, la responsabilité du fournisseur aux termes de ce contrat est toutefois limitée à cinq fois la valeur du contrat jusqu'à concurrence de 3 000 000 \$.

Cette limite financière de responsabilité ne s'applique pas au préjudice corporel ou moral ni au préjudice matériel causé par une faute intentionnelle ou une faute lourde.

## 15. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

### 15.1 Définitions

« Renseignement personnel » : tout renseignement qui concerne une personne physique et qui permet de l'identifier.

« Renseignement confidentiel » : tout renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par la Loi sur l'accès, notamment un renseignement ayant des incidences sur les relations intergouvernementales, sur les négociations entre organismes publics, sur l'économie, sur l'administration de la justice et la sécurité publique, sur les décisions administratives ou politiques ou sur la vérification.

15.2 Le fournisseur s'engage envers le ministre à respecter chacune des dispositions applicables aux renseignements personnels et confidentiels ci-dessous énumérées; que ces renseignements lui soient communiqués dans le cadre de la réalisation de ce contrat ou soient générés à l'occasion de sa réalisation.

- 1) Informer son personnel des obligations stipulées aux présentes dispositions et diffuser à cet égard toute l'information pertinente.
- 2) Rendre accessibles les renseignements personnels, au sein des membres de son personnel, uniquement à ceux qui ont qualité pour les recevoir, lorsqu'ils sont nécessaires à l'exercice de leurs fonctions et sont utilisés aux fins pour lesquelles ils ont été recueillis ou que la loi autorise leur utilisation.
- 3) Faire signer aux membres de son personnel, préalablement à l'accès à des renseignements personnels et confidentiels, des engagements au respect de la confidentialité de ces renseignements selon l'annexe 4 du présent document et les transmettre aussitôt au ministre, sous peine de se voir refuser l'accès aux locaux, à l'équipement du ministre ou aux données à être transmises par celui-ci, le cas échéant.
- 4) Ne pas communiquer les renseignements personnels, sans le consentement de la personne concernée, à qui que ce soit, sauf dans le cadre d'un sous-contrat et selon les modalités prévues au paragraphe 19).
- 5) Soumettre à l'approbation du ministre le formulaire de consentement à la communication de renseignements personnels de la personne concernée.
- 6) Utiliser les renseignements personnels uniquement pour la réalisation du contrat.
- 7) Recueillir un renseignement personnel au nom du ministre, dans les seuls cas où cela est nécessaire à la réalisation du contrat, et informer préalablement toute personne visée par cette cueillette de l'usage auquel ce renseignement est destiné, ainsi que des autres éléments mentionnés à l'article 65 de la Loi sur l'accès.
- 8) Prendre toutes les mesures de sécurité propres à assurer la confidentialité des renseignements personnels et confidentiels à toutes les étapes de la réalisation du contrat et, le cas échéant, les mesures identifiées à l'annexe 4 – Engagement de confidentialité, jointe au présent document.
- 9) **Le fournisseur devra, au moment de la signature du contrat, faire un choix parmi les trois options suivantes :**
  - ne conserver, à l'expiration du contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, en les retournant au ministre dans les 60 jours suivant la fin du contrat et remettre au ministre une confirmation que lui et les membres de son personnel ont retourné tous ces documents;



- procéder, à ses frais, à la destruction des renseignements personnels et confidentiels en se conformant à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec ainsi qu'aux directives que lui remettra le ministre et transmettre à celui-ci, dans les 60 jours suivant la fin du contrat, l'Attestation de destruction des renseignements personnels et confidentiels jointe à l'annexe 6, signée par une personne autorisée qu'il aura désignée à cette fin;
  - confier la destruction des renseignements personnels et confidentiels à une entreprise de récupération, laquelle s'engage contractuellement à se conformer à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec ainsi qu'aux directives du ministre. Le fournisseur devra alors, dans les 60 jours suivant la fin du contrat de récupération, remettre au ministre l'Attestation de destruction des renseignements personnels et confidentiels jointe à l'annexe 6, signée par le responsable autorisé de cette entreprise.
- 10) Informer, dans les plus brefs délais, le ministre de tout manquement aux obligations prévues aux présentes dispositions ou de tout événement pouvant risquer de porter atteinte à la sécurité ou à la confidentialité des renseignements personnels ou confidentiels.
  - 11) Fournir, à la demande du ministre, toute l'information pertinente au sujet de la protection des renseignements personnels et confidentiels et donner accès, à toute personne désignée par le ministre, à la documentation, aux systèmes, aux données et aux lieux physiques relatifs au contrat afin de s'assurer du respect des présentes dispositions.
  - 12) Se conformer aux objectifs et aux exigences de sécurité de l'information définis par le ministre.
  - 13) Obtenir l'autorisation écrite du ministre avant de communiquer ou de transférer quelque donnée que ce soit, même à des fins techniques, hors du Québec.
  - 14) Lorsque la réalisation du présent contrat est confiée, en tout ou en partie, à un sous-contractant et qu'elle comporte la communication de renseignements personnels et confidentiels par le fournisseur au sous-contractant ou la cueillette de renseignements personnels et confidentiels par le sous-contractant :
    - soumettre à l'approbation du ministre la liste des renseignements personnels et confidentiels communiqués au sous-contractant;
    - conclure un contrat avec le sous-contractant stipulant les mêmes obligations que celles prévues aux présentes dispositions;
    - exiger du sous-contractant qu'il s'engage à ne conserver, à l'expiration du sous-contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, et à remettre au fournisseur, dans les 60 jours suivant la fin de ce contrat, un tel document.
  - 15) Transmettre de façon sécuritaire les renseignements personnels ou confidentiels lorsque ceux-ci sont communiqués par courriel ou Internet. Ces renseignements doivent nécessairement faire l'objet d'un chiffrement ou être protégés par un dispositif de sécurité éprouvé. Si les renseignements personnels ou confidentiels sont acheminés par télécopieur, l'émetteur du document doit s'assurer que le récepteur est habilité à le recevoir et qu'il prendra toutes les mesures nécessaires à la protection de ces renseignements. Toutefois, les parties peuvent convenir entre elles de tout autre moyen, telle la remise en mains propres, la messagerie ou la poste recommandée en indiquant toujours sur l'enveloppe la mention « personnel et confidentiel ».

- 15.3 La fin du contrat ne dégage aucunement le fournisseur et le sous-contractant de leurs obligations et engagements relatifs à la protection des renseignements personnels et confidentiels. Les principales dispositions applicables se retrouvent notamment, mais non limitativement, aux articles 1, 9, 18 à 41.3, 53 à 60.1, 62, 64 à 67.2, 83, 89, 158 à 164.

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels peut être consultée à l'adresse suivante : [www.publicationsduquebec.gouv.qc.ca](http://www.publicationsduquebec.gouv.qc.ca).

## ANNEXE 2 – DESCRIPTION DES BESOINS

**APPROVISIONNEMENT ET SERVICES EN MATIÈRE DE TECHNOLOGIES DE  
L'INFORMATION**

**Annexe 2 - DEVIS TECHNIQUE**

**Acquisition d'une solution visant à soutenir l'implantation de la télésanté dans le  
cadre de la pandémie causée par la COVID19**

## Table des matières

Table des matières .....	2
ACRONYMES ET DÉFINITIONS.....	5
1. Objectifs et portée du projet .....	8
1.1. Objectif .....	8
1.2. Portée .....	8
1.3. Mise en place de la solution .....	9
1.4. Éléments sur demande .....	10
1.5. Processus d'acceptation .....	10
2. Contexte organisationnelle .....	11
2.1. Gestion de la solution .....	11
2.2. Rôle attendu du fournisseur .....	11
3. Définition des besoins .....	12
3.1. Questionnaires médicaux .....	12
3.1.1. Spécifications .....	12
3.2. Redirection / Trajectoire .....	13
3.2.1. Spécifications .....	13
3.3. Systèmes de webconférence .....	13
3.3.1. Spécifications .....	13
3.4. Suivis et statistiques .....	14
3.4.1. Spécifications .....	14
4. Définition des besoins génériques .....	14
4.1. Convivialité de la solution .....	14
4.2. Gestion des rôles et privilèges .....	14
5. Exigences technologiques .....	15
5.1. Parc informatique .....	15
5.2. Télécommunications .....	15
5.3. Environnements .....	15
5.4. Gestion des fuseaux horaires .....	16
5.5. Ergonomie et accessibilité .....	16
5.6. Hébergement/exploitation .....	16
5.6.1. Niveaux de service .....	17

5.6.2. Arrêts planifiés.....	17
5.7. Performances .....	18
5.7.1. Exigence sur l'exécution .....	18
5.7.2. Surveillance.....	18
5.8. Données.....	18
5.9. Interopérabilité des systèmes .....	18
5.10. Cadre normatif de la gestion de l'identification de l'utilisateur (GIU).....	18
5.11. Interfaces applicatives.....	18
5.12. Évolution de la solution .....	19
5.12.1. Rehaussement des infrastructures.....	19
5.12.2. Mise à jour de la solution .....	19
5.12.3. Processus de rehaussement des versions .....	19
5.13. Certification .....	19
5.14. Service fournisseur (Service « F »).....	19
5.15. Sécurité.....	19
5.15.1. Sécurité hébergement .....	20
5.15.2. Déclaration des incidents de sécurité .....	20
5.15.3. Gestion des accès .....	21
5.15.4. Journalisation .....	22
6. Services d'entretien.....	23
6.1. Besoins.....	23
6.2. Exigences en matière de soutien .....	23
6.3. Services de maintenance.....	25
7. Organisation du projet .....	25
7.1. Le chargé de projet de l'organisme public .....	25
7.2. Chargé de projet du fournisseur.....	26
7.3. Reddition de compte .....	26
7.4. Échéancier des travaux et disponibilité des services.....	26
8. Gestion du changement et formation.....	26
8.1. Gestion du changement .....	26
8.2. Formation .....	26
Super utilisateurs.....	26

Ressources TI .....	27
8.3 Matériel de formation et de soutien.....	27
9. Services sur demande : Interfaces.....	27
10. Services sur demande : Banque d'heures .....	27
11. Modalités de décaissement.....	28
12. Liste préliminaire des demandes de changement 2021-2022 .....	29

## ACRONYMES ET DÉFINITIONS

Terme	Abréviation / Définition
Acquisition	Acquisition d'un droit d'utilisation de la solution
Agent	Désigne tout utilisateur du système. Un agent peut être un agent ccc, un agent administratif ou un agent superviseur.
Agent administratif	Désigne toute personne soutenant les responsables cliniques pour l'ensemble des tâches administratives liées au dépistage (code d'accès, communication avec répondant, suivi des relances, etc.)
Agent d'intégration (AI)	Solution intergicielle conçue pour permettre à des applications hétérogènes de gérer leurs échanges. Cette solution offre des fonctionnalités allant au-delà de celles offertes par les engins d'interfaces en facilitant l'intégration, l'orchestration et la gestion de ceux-ci.
ANS	Accords de niveau de services
Appelant	Partenaire qui appelle les services du 8-1-1
Assignataire	Désigne toute personne ayant la charge d'assigner un questionnaire à un répondant. Typiquement, un assignataire est un agent administratif, mais peut également être un professionnel de la santé et des services sociaux
CISSS	Centre intégré de santé et de services sociaux
CIUSSS	Centre intégré universitaire de santé et de services sociaux
Engin d'interface (EI)	Un engin d'interface est conçu pour simplifier la connexion, le maintien, le suivi et le partage des données entre les interfaces. Un engin d'interface peut prendre les données transmises par une application, les filtrer ou modifier leur format afin de satisfaire les besoins de chaque application individuelle.
Épisode de soins	Durée pendant laquelle un patient reçoit un ensemble de soins donnés en fonction d'un diagnostic (aussi appelé période de traitement).
Établissement	Entité juridique dotée de capacités et responsabilités légales, titulaire d'un permis délivré par le ministre de la Santé et des Services sociaux pour gérer des services.
Fournisseur	Désigne tout SOUMISSIONNAIRE choisi comme ADJUDICATAIRE au terme du processus de l'appel d'offres.
GIU	Gestion de l'identification de l'utilisateur
Hébergeur	Désigne l'organisme mandaté par l'organisme public pour héberger la solution
Installation	Lieu physique maintenu par un établissement où sont dispensés des soins de santé et de services sociaux à la population du Québec, dans le cadre d'une ou de plusieurs missions. Un établissement comporte généralement plusieurs installations.
Interopérabilité	L'interopérabilité est la capacité que possède un système informatique à fonctionner avec d'autres produits ou systèmes informatiques, existants ou futurs, sans restriction d'accès ou de mise en œuvre (ISO/IEC 2382-18:1999).
ITIL	Information Technology Infrastructure Library

LGGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
Licence	Désigne le droit d'utilisation du logiciel octroyé par le FOURNISSEUR en faveur des établissements du RSSS.
Licence d'utilisation concurrente	Licence octroyant un droit d'utilisation du logiciel partagé par plusieurs utilisateurs, mais limité quant au nombre d'utilisateurs accédant en même temps au logiciel. Ce type de licence nécessite de posséder autant de licences que d'utilisateurs susceptibles d'utiliser simultanément le logiciel. Cette licence permet d'utiliser le logiciel à partir de tout matériel compatible, pourvu qu'une licence d'utilisation soit disponible. Le droit d'utilisation est limité au nombre d'utilisations concurrentes du logiciel et non au nombre de matériels ayant le potentiel d'accès.
Licence par utilisateur nommé	Licence octroyant un droit d'utilisation pour un utilisateur identifié, lui permettant d'utiliser le logiciel à partir de tout matériel compatible. Le droit d'utilisation est limité à l'utilisateur et non au nombre de matériels ayant le potentiel d'accès.
LMOGRSSS	Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales
LMRSSS	Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales
LPCRS	Loi concernant le partage de certains renseignements de santé
LSSSS	Loi sur les services de santé et les services sociaux
MSSS	Ministère de la Santé et des Services sociaux.
NAM	Numéro d'assurance maladie
NIU	Numéro d'identification unique
NIU-U	Numéro d'identification unique de l'utilisateur attribué par la RAMQ
Organismes	Désigne les organismes du réseau de la santé et des services sociaux relevant de l'autorité du ministre.
PDF	Portable Document Format
Professionnel de la santé et des services sociaux (PSSS)	Désigne toute personne devant accéder aux questionnaires complétés par le (ou les) répondant(s) ainsi qu'aux rapports. Un PSSS peut aussi effectuer d'autres tâches dans la solution telles que l'analyse des questionnaires.
Questionnaire	Le questionnaire est un outil méthodologique comportant un ensemble de questions qui s'enchaînent d'une manière structurée.
RAMQ	Régie de l'assurance maladie du Québec
Référent	Désigne toute personne qui réfère un usager ou un requérant dans la solution
Référent	Désigne toute personne qui a initié une investigation de la situation de l'utilisateur (ex. parent, médecins, tuteurs, PSSS)
Registre des usagers	Contient des renseignements sur l'identité des personnes assurées ou ayant déjà été assurées aux régimes d'assurance maladie ou d'assurance médicaments et autres programmes confiés à la RAMQ.



Répondant	Désigne une personne identifiée pour répondre minimalement à un questionnaire concernant un usager. Un répondant peut être typiquement le parent de l'usager, mais peut être aussi une personne en lien avec l'usager, à titre d'exemple un éducateur en garderie ou encore, dans certains cas, un professionnel de la santé et des services sociaux, ou encore l'usager lui-même.
Responsable clinique	Désigne toute personne devant accéder aux données complétées par le répondant dans le questionnaire
RITM	Réseau intégré de télécommunication multimédia
RSSS	Réseau de la santé et des services sociaux
RSSS	Réseau de la santé et des services sociaux
RTSS	Réseau de Télécommunications Socio-Sanitaire
RU	Registre des usagers
Services Web	Office québécois de la langue française. Le grand dictionnaire terminologique. «Le service Web se définit comme un ensemble de fonctionnalités accessibles sur Internet et permettant la communication ainsi que l'échange automatique et en temps réel de données entre applications et systèmes hétérogènes, dans des environnements distribués.» [En ligne]. <a href="http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26506475">http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26506475</a> . (page consultée le 11 mars 2016).
SSSS	Désigne le système de la santé et des services sociaux composé du RSSS et des autres organisations oeuvrant dans le domaine au Québec.
Usager	Désigne une personne qui a reçu, aurait dû recevoir, reçoit ou requiert des services de santé ou des services sociaux d'un établissement, d'une ressource intermédiaire ou d'une ressource de type familial ou de tout autre organisme, société ou personne auxquels l'établissement recourt
Utilisateur	Désigne toute personne autorisée par l'établissement à utiliser la solution en fonction des droits d'accès qui lui ont été attribués.
XML	eXtensible Markup Language
XSL	eXtensible Stylesheet Language

## 1. Objectifs et portée du projet

---

### 1.1. Objectif

---

Le contrat vise l'acquisition et l'utilisation d'une plateforme provinciale permettant la gestion de trajectoires cliniques dans le contexte de la pandémie de la COVID-19.

À ce titre, la plateforme soutient la trajectoire des patients atteints de la covid-19 ou à risque de l'être, en intégrant le processus de triage clinique par l'évaluation des usagers, l'orientation des patients vers les cliniques attirées de dépistage et l'intégration des résultats de laboratoire (PCR et tests rapides) ainsi que tout autre besoin en lien avec la pandémie actuelle, selon l'évolution de la situation épidémiologique

### 1.2. Portée

---

Le FOURNISSEUR met à la disposition de l'ORGANISME PUBLIC la trajectoire de suivi des cas et des contacts (TSP) de la COVID-19, incluant les éléments et travaux suivants :

- La licence
- Les services professionnels (composés d'une équipe de projet sénior)
- Les travaux de paramétrisation de la plateforme

La portée de la TSP prévoit :

- Le maintien de la trajectoire TSP développée et utilisée pendant la première année de la pandémie (avril 2020 à mars 2021), incluant les tableaux de bords et les interfaces avec les systèmes complémentaires, notamment Nosotech pour les résultats de laboratoire
- Le développement et l'évolution de la trajectoire TSP selon la liste des biens livrables (voir la section 12 : liste préliminaire des demandes de changement) estimés nécessaires par les autorités de santé publique, ainsi que les tableaux de bords associés
- La modification de cette liste de livrables pour s'adapter au besoin à l'évolution de la pandémie Covid-19

Les critères d'acceptation des livraisons sont décrits à la section [1.5 Processus d'acceptation](#).

Le FOURNISSEUR met à la disposition de l'ORGANISME PUBLIC la trajectoire de dépistage (TDD) COVID-19, incluant les éléments et travaux suivants :

- Le maintien de la solution Clinique désignée de dépistage CDD développée et utilisée au début de la pandémie (avril 2020 à mars 2021), et sa remise en opération (incluant les tableaux de bord) le cas échéant. Le maintien de la requête web pour les tests rapides développée et utilisée dans le cadre de trajectoire TDD pendant la première année de la pandémie (avril 2020 à mars 2021), incluant les tableaux de bords et les interfaces avec les systèmes complémentaires, notamment Nosotech pour l'envoi des résultats des EBMD.
- Le développement et l'évolution de la trajectoire TDD selon la liste des biens livrables (voir la section 12 : liste préliminaire des demandes de changement) estimés nécessaires par les autorités de santé publique, ainsi que les tableaux de bords associés
- La modification de cette trajectoire pour s'adapter au besoin à l'évolution de la pandémie Covid-19

La portée de la trajectoire TDD prévoit :

- L'utilisation d'une licence provinciale de la trajectoire TDD et de son déploiement dans un contexte d'urgence, sur demande
- Le cas échéant, la banque d'heures devrait être utilisée pour la remise en opération de la solution CDD
- Le tableau de bord

Les critères d'acceptation des livraisons sont décrits à la section [1.5 Processus d'acceptation](#).

Le FOURNISSEUR met à la disposition de l'ORGANISME PUBLIC la trajectoire Clinique désignée d'évaluation (CDÉ) COVID-19, incluant les éléments et travaux suivants :

- Le maintien de la trajectoire CDÉ développée et utilisée pendant la première année de la pandémie (avril 2020 à mars 2021), et sa remise en opération (incluant les tableaux de bord) le cas échéant
- La modification de cette trajectoire pour s'adapter au besoin à l'évolution de la pandémie Covid-19

La portée de la trajectoire CDÉ prévoit :

- L'utilisation d'une licence provinciale de la trajectoire CDÉ et de son déploiement dans un contexte d'urgence, sur demande
- Le cas échéant, la banque d'heures devrait être utilisée pour la remise en opération de la trajectoire CDÉ
- Le tableau de bord

Les critères d'acceptation des livraisons sont décrits à la section [1.5 Processus d'acceptation](#).

Le FOURNISSEUR met à la disposition de l'ORGANISME PUBLIC la trajectoire d'auto-évaluation (TAE) COVID-19, incluant les éléments et travaux suivants :

- La licence
- Les services professionnels (composés d'une équipe de projet sénior)
- ☑ Les travaux de paramétrisation de la plateforme

La portée de la trajectoire TAE prévoit :

- Le maintien de la trajectoire TAE développée et utilisée pendant la première année de la pandémie (avril 2020 à mars 2021)
- Le développement et l'évolution de la trajectoire TAE selon la liste des biens livrables (voir la section 12 : liste préliminaire des demandes de changement) estimés nécessaires par les autorités de santé publique, ainsi que les tableaux de bords associés
- La modification de cette trajectoire pour s'adapter au besoin à l'évolution de la pandémie Covid-19

Les critères d'acceptation des livraisons sont décrits à la section [1.5 Processus d'acceptation](#).

Le FOURNISSEUR met à la disposition de l'ORGANISME PUBLIC la trajectoire Alerte Covid, incluant les éléments et travaux suivants :

- La licence
- Les services professionnels (composés d'une équipe de projet sénior)
- ☑ Les travaux de paramétrisation de la plateforme

La portée de la trajectoire TAE prévoit :

- Le maintien de la trajectoire Alerte Covid développée et utilisée pendant la première année de la pandémie (avril 2020 à mars 2021)
- La modification de cette trajectoire pour s'adapter au besoin à l'évolution de la pandémie Covid-19

Les critères d'acceptation des livraisons sont décrits à la section [1.5 Processus d'acceptation](#).

### [1.3. Mise en place de la solution](#)

Le FOURNISSEUR prend en charge tous les éléments liés à l'hébergement de la solution, l'ORGANISME PUBLIC désirant une solution de type « clé en main ». Ceci inclut :

- Un hébergement Cloud (de base)
- Les services Cloud de communication (de type SMS, courriels), impliquant des parties tierces
- Le support de niveau 2 (décrit à la section [5.6.1 Niveaux de service](#))

#### 1.4. Éléments sur demande

Une liste de biens livrables (voir la section 12 : liste préliminaire des demandes de changement) anticipés par les différentes unités d'affaires impliquées a permis d'estimer les efforts requis pour le développement de nouvelles fonctionnalités nécessaires pendant la durée du contrat. Il est essentiel de permettre le remplacement de certains livrables de cette liste par d'autres livrables, afin de répondre de façon agile à l'urgence sanitaire et aux priorités cliniques provinciales et de s'adapter à l'épidémiologie changeante de la pandémie actuelle.

#### 1.5. Processus d'acceptation

À la mise en ligne des livrables de paramétrisation selon les requis entendus au courant des ateliers de travail, l'ORGANISME PUBLIC procède à l'acceptation du livrable, dans un délai de cinq (5) jours ouvrés.

Toute demande de changement adressée par l'ORGANISME PUBLIC sera évaluée mutuellement par l'ORGANISME PUBLIC et le FOURNISSEUR. Les efforts sous-jacents aux changements demandés seront encourus à travers la banque d'heure prévue au présent contrat. Le FOURNISSEUR s'engage à déployer les efforts raisonnables pour implanter les changements.



Dans un contexte d'évolution constante des recommandations émises par la Santé Publique et des besoins évolutifs sur l'interprétation des textes, les demandes de changement de libellés seront également encourues à travers la banque d'heure prévue au présent contrat.

Dans un contexte de gestion de crise et de changements de priorité, l'ORGANISME PUBLIC peut avoir à annuler un livrable sur lequel le FOURNISSEUR a investi des efforts à la demande de l'ORGANISME PUBLIC, mais sans aboutir à une livraison. Dans un tel cas, l'ORGANISME PUBLIC s'engage à couvrir les frais encourus par le FOURNISSEUR, sous réserve de la présentation de preuve relative aux efforts investis.

Dans le cas où un livrable annulé est repriorisé pendant la durée du contrat, les efforts pouvant être récupérés seront entendus entre l'ORGANISME PUBLIC et le FOURNISSEUR et les travaux supplémentaires nécessaires à la mise en place du livrable seront encourus à travers la banque d'heure prévue au présent contrat.

De la même façon, suivant l'évolution de la pandémie, une trajectoire peut être rendue non-disponible à la demande de l'organisme public (hors production) et, toujours à la demande de l'organisme public, peut être rendue de nouveau disponible au cours du contrat, sans frais additionnels. Tous travaux hormis l'activation ou désactivation, par exemple des demandes de changements, manipulations de données, communications en lots aux utilisateurs pour les aviser d'une désactivation, etc. seront encourus à travers la banque d'heure prévue au présent contrat.

## 2. Contexte organisationnelle

Le RSSS est constitué de 34 établissements. Chacun des établissements peut offrir des services dans plusieurs installations qu'il maintient et qui sont des lieux physiques où sont dispensés les soins de santé et des services sociaux. En plus des services offerts par les établissements publics, la population bénéficie des services des établissements privés qui offrent notamment des services en hébergement et des soins de longue durée. Les établissements privés ne sont pas visés par le présent appel d'offres.

Au Québec, les services de santé et les services sociaux sont intégrés au sein d'une même administration. Cette particularité québécoise offre l'avantage de répondre à l'ensemble des besoins de santé et de bien-être des personnes et elle représente un défi majeur à relever comme mode d'organisation des soins et services.

### 2.1. Gestion de la solution

L'ORGANISME PUBLIC, pour l'acquisition, le déploiement et l'exploitation de la solution pour tout le Québec est en charge des activités suivantes :

- Gestion de la relation avec le FOURNISSEUR
- Planification de projet et gestion des démarches d'autorisation de mise en œuvre
- Reddition de comptes aux instances concernées, incluant un bilan de projet
- Validation des besoins et des livrables

### 2.2. Rôle attendu du fournisseur

Le fournisseur, a la responsabilité d'assurer, notamment :

- Gestion de projets
- Analyse d'affaires
  - Collecte et analyse des besoins
  - Collaboration avec l'ORGANISME PUBLIC dans le processus de paramétrisation de la solution
- Reddition de compte
  - La production périodique de rapports et biens livrables selon la méthodologie Macroscopie de Fujitsu ou autre à la demande de l'ORGANISME PUBLIC
- Architecture technologique, hébergement et intégration
  - La mise en place et l'exploitation de l'architecture technologique, incluant :
    - Acquisition
    - Installation
    - Virtualisation des serveurs et des infrastructures

- L'infrastructure d'hébergement
- Le déploiement de licences requises pour le fonctionnement de la solution
- L'installation et mise en production de la solution et des interfaces
- Les travaux en capacité de traitement et en performance
- La gestion de la performance opérationnelle
- La gestion des copies de sécurité et sauvegarde (la manipulation, le transport, l'entreposage des copies) et récupération des données
- L'administration, l'entretien, l'évolution, le soutien et la coordination des
- Le volet Communication avec des parties tierces pour l'envoi de SMS et courriels
- Maintenance
  - La gestion des changements de versions, de la maintenance et des mises à jour technologiques et fonctionnelles (solution)
- Collaboration avec l'ORGANISME PUBIC pour la gestion du changement et la formation :
  - La formation de pilotes désignés de l'ORGANISME PUBIC
  - L'accompagnement des pilotes à la production du matériel de formation
- Soutien technique
  - Le soutien de niveau 2
  - La gestion des niveaux de services
  - La gestion des incidents et des problèmes

### 3. Définition des besoins

---

#### 3.1. Questionnaires médicaux

---

Dans le cadre de la pandémie qui sévit actuellement, les usagers doivent avoir accès rapidement et ce, facilement à des professionnels de la santé. Il est important de limiter les déplacements des usagers et ainsi protéger la population. Les établissements doivent pouvoir rapidement diriger un usager pour des soins de leur région selon différents critères (ex. : symptômes) ou situation.

##### 3.1.1. Spécifications

---

Pour répondre à ce besoin, la solution doit :

- Permettre la création de questionnaires avec différents types de réponses :
  - Questions ouvertes (pas de limitation du nombre de caractères)
  - Réponses ouvertes (avec possibilité de limitation du nombre de caractère)
  - Réponses fermées, encadrées selon une liste fournie
    - unitaire,
    - multiple,
    - avec une quantité de sélection configurable
  - Réponses mixtes (fermées et avec une possibilité de champs ouverts)
  - Réponse de type classement (ordre de préférence)
  - Selon une échelle de mesure (sémantique, numérique, mixte échelle de Lickert, échelle avec ou sans point de neutralité, sémantique différentielle, etc.
  - Assignation d'une valeur à chaque réponse (valeur par défaut)
- Permettre à un usager de le remplir via un accès web (page web) sans créer un compte utilisateur (pour l'usager)
- Offrir un portail patient, au besoin qu'il sera nécessaire de paramétrer selon le contexte
- Permettre, à l'usager d'inscrire ses données d'identification; Donc, la solution doit être en mesure de supporter les données telles que:
  - Nom
  - Prénom
  - Sexe
  - Date de naissance
  - Nom de la mère
  - Prénom de la mère
  - Langue d'usage

- De plus, la solution doit permettre l'ajout de champs propres aux besoins éventuel de l'ORGANISME PUBLIC telles que :
  - NAM, lorsque disponible
  - Établissement (saisie à partir d'une liste), au besoin
  - Installation (saisie à partir d'une liste)
  - Région administrative (saisie à partir d'une liste)
  - Adresse postale, etc.
- Permettre de développer des questionnaires complémentaires selon les réponses données par l'utilisateur
- Permettre l'utilisation de règles de paramétrisation permettant de renvoyer à des questions subséquentes à l'intérieur d'un même questionnaire. Les règles minimales attendues permettant ce type de renvoi sont les suivantes :
  - Dépendamment d'une réponse obtenue
  - Dépendamment d'un score obtenu à l'intérieur d'une même section ou sous-section
  - Dépendamment d'une quantité de réponses de même type obtenu, à l'intérieur d'une même section ou sous-section
  - Dépendamment d'un comparatif de quantité de réponses de même type obtenu, à l'intérieur d'une même section ou sous-section
- Proposer des questionnaires selon la langue choisie par le répondant lors de son identification. Néanmoins, il doit être possible pour un répondant, lors de la complétion d'un questionnaire, de passer du français à l'anglais (ou inversement) en gardant les réponses données, pour les questionnaires qui le permettent
- Intégrer un processus de consentement de l'utilisateur
- Permettre la production de rapports
- Permettre l'envoi de notification selon différentes modalités
- Permettre l'intégration avec des outils de communication ou téléconsultation qu'il sera nécessaire de paramétrer selon le contexte

### 3.2. Redirection / Trajectoire

Suite aux réponses fournies dans le ou les questionnaire(s), la solution doit pouvoir diriger l'utilisateur vers des services externes.

#### 3.2.1. Spécifications

Pour répondre aux besoins, la solution doit permettre de s'interfacer à des systèmes externes (e.g. Carnet Santé Québec, DSQ pour le dépôt de documents à partir de Akinox, DCI, DMÉ). Ces éléments devront être assumés à partir de la banque d'heures selon les besoins qui émergeront, le cas échéant, en cours de contrat.

### 3.3. Systèmes de webconférence

Suite aux réponses fournies dans le ou les questionnaire(s), la solution peut orienter l'utilisateur vers un outil de webconférence externe (e.g. Reacts, Zoom, MS Teams), selon les travaux d'interfaçage requis et réalisés à la section 3.3.1. Les outils de webconférence permettent à un professionnel de la santé de faire un suivi (consultation) avec l'utilisateur ou d'échanger avec un autre professionnel de la santé.

La plateforme doit être agnostique par rapport à la solution de webconférence retenue par l'ORGANISME PUBLIC. Les licences des outils de webconférence sont exclues du présent contrat.

#### 3.3.1. Spécifications

Pour répondre à ce besoin, la solution doit permettre :

- Un suivi (consultation) en temps réel et en temps différé, via une interface avec le ou les systèmes de webconférence requis et disponibles suite à la réalisation des travaux décrit à la section [3.3 Systèmes de webconférence](#)
- L'utilisation de caméras, casque d'écoute et haut-parleurs



- Un échange bidirectionnel entre l'utilisateur et le professionnel de la santé
- L'usage d'un compte utilisateur (professionnel de la santé), au besoin

### 3.4. Suivis et statistiques

Des statistiques sont nécessaires pour évaluer la performance, la nécessité et l'adaptation des usagers en vue d'ajuster l'offre de soins et services des établissements. Ils seront produits par le FOURNISSEUR à la demande de l'ORGANISME PUBLIC.

#### 3.4.1. Spécifications

La portée prévoit le maintien et l'évolution des tableaux de bord déjà existants. Par ailleurs, le fournisseur permettra l'exploitation de rapports statistiques par trajectoire, selon les données et indicateurs requis par l'ORGANISME PUBLIC, permettant en outre de comptabiliser des statistiques telles que :

- Nombre d'utilisateurs ayant utilisé le service
- Nombre d'utilisateurs ayant été dirigé vers le système RVSQ
- Nombre d'utilisateurs ayant été dirigé vers le 811
- Nombre d'utilisateurs ayant utilisé un système de webconférence
- Quantité de réponses d'un même type (ex. « réussite » / « échec »)
- Comparaison entre des quantités de réponses d'un même type (plus grande
- quantité de réponse « échec » que de réponse « réussite »)
- Quantité minimale de réponse d'un type donné (ex. si au moins une
- réponse « échec », alors.)
- Quantité maximale de réponse d'un type donné (ex. si toutes les réponses
- sont « échecs », alors...)

On devra aussi permettre l'extraction de données brutes par le FOURNISSEUR à la demande de l'ORGANISME PUBLIC

## 4. Définition des besoins génériques

### 4.1. Convivialité de la solution

Le niveau de littératie attendu de la solution est de niveau 1 pour l'utilisation du questionnaire médical : <http://www.education.gouv.qc.ca/adultes/references/litteratie/peica/resultats-2012/niveau-1/>

### 4.2. Gestion des rôles et privilèges

La solution doit permettre une gestion des rôles et privilèges.



La détermination des rôles et privilèges doit pouvoir être réalisée en fonction de tâches, de fonctions spécifiques, de processus ou d'expertise. Alors que les rôles permettent d'avoir accès à des modules ou champs spécifiques de la solution, les privilèges, quant à eux, sont attribués en fonction des données auxquelles l'utilisateur peut avoir accès.

La solution doit permettre d'octroyer les privilèges selon les éléments de la structure hiérarchique et doit permettre d'ajouter ou de soustraire des informations à ces éléments.

Par ailleurs, l'accès aux données doit pouvoir être fait en fonction de champs spécifiques, jusqu'à la donnée brute. La solution doit également permettre le paramétrage du type d'accès aux données : en création, en visualisation, en modification ou en suppression.

La solution doit également permettre la modification des rôles et privilèges attribués à un poste, par le FOURNISSEUR, à la demande de l'ORGANISME PUBLIC.



## 5. Exigences technologiques

Le FOURNISSEUR doit s'assurer que sa solution ou les modules de sa solution sont compatibles avec le parc informatique des postes de travail du RSSS ainsi que les différentes versions de navigateur web supportées par les fabricants.

### 5.1. Parc informatique

L'ensemble du parc informatique des postes de travail du RSSS utilise une version du système d'exploitation Windows. Les postes de travail de type bureautique comprennent notamment la suite bureautique Microsoft Office et les produits assignés à chaque utilisateur, selon son secteur d'activité. Les postes de travail de type allégé comprennent Windows de base sans la suite Microsoft Office. Enfin, les postes de travail de type commun (poste sans utilisateur assigné) sont principalement des postes partagés et sont configurés selon les besoins du secteur d'activités. Environ 30 % des postes clients utilisent des technologies de virtualisation, notamment : Citrix, Remote Desktop Services (RDS) de Microsoft et VMware. La solution doit être capable d'utiliser des périphériques installés sur les postes locaux.

Les téléphones intelligents déployés utilisent les systèmes d'exploitation de type iOS et Android. La solution doit pouvoir être utilisée sur ces systèmes d'exploitation.

Les versions des systèmes d'exploitation et des logiciels installés sont des versions supportées par le fabricant de ceux-ci.

Les établissements possèdent plusieurs milliers de systèmes d'information, dont plusieurs instances et versions pour un même système d'information.

La plateforme doit être web et ne nécessiter aucune installation du côté de l'utilisateur. Ceci exclut les systèmes avec lesquels la solution est intégrée.

### 5.2. Télécommunications

Le réseau de télécommunications utilisé pour les communications inter-établissements et inter-installation d'un établissement est actuellement de type IP/MPLS privé. Une migration vers un réseau de type SD WAN hybride (IP/MPLS et internet) est aussi prévue pendant l'exécution du présent contrat.

La solution doit être fonctionnelle sur les infrastructures de télécommunications de l'ORGANISME PUBLIC et des infrastructures internet de la population. La solution doit être optimisée pour une utilisation minimale de bande passante et supporter une latence variant de 1 milliseconde à 60 millisecondes.

L'ORGANISME PUBLIC est responsable d'assurer la performance et les niveaux de services des liens de télécommunications de ses installations.

### 5.3. Environnements

La solution doit disposer minimalement de deux environnements (pour la gestion des questionnaires) :

- « Production »
- « Pré-Production » : permet de valider les nouvelles versions de l'application sans impacter les environnements de production et de formation avant le moment prévu

Dans le cas de l'implantation de correctifs et mises à jour, ceux-ci doivent toujours être testés à la satisfaction de l'ORGANISME PUBLIC dans l'environnement de pré-production avant de pouvoir être installés dans l'environnement de production et de démonstration. Les processus de gestion des correctifs doivent être en conformité avec les bonnes pratiques de l'industrie en matière de gestion des configurations et sont sujets à vérification et approbation de l'ORGANISME PUBLIC.

La solution doit disposer d'une procédure pour basculer (copier) les paramètres ou les données des divers environnements entre eux pour s'assurer d'une synchronisation entre ces environnements. La solution doit permettre aux équipes TI d'être en mesure, de manière autonome, en suivant une procédure établie, de procéder aux bascules. Il est aussi acceptable

que le FOURNISSEUR s'engage, sur demande, à basculer les paramètres ou les données des environnements, et ce dans un délai imposé par l'ORGANISME PUBLIC.

Ces environnements sont dédiés exclusivement aux besoins de l'ORGANISME PUBLIC. Le FOURNISSEUR ne peut en aucun cas disposer de ces environnements pour ses besoins de tests ou autres.

#### 5.4. Gestion des fuseaux horaires

---

La solution doit assurer la gestion et le fonctionnement sur plusieurs fuseaux horaires simultanément.

#### 5.5. Ergonomie et accessibilité

---

Les portails web accessibles par les usagers doivent respecter les normes d'accessibilité du Web du Conseil du Trésor du Québec.

<https://www.tresor.gouv.qc.ca/ressources-informationnelles/architecture-dentreprise-gouvernementale/standards-et-normes/standards-sur-laccessibilite-du-web/>

La solution devra aussi être accessible et en respect des normes du site web du gouvernement du Québec.

#### 5.6. Hébergement/exploitation

---

Le FOURNISSEUR prend en charge tous les éléments liés à l'hébergement de la solution, l'ORGANISME PUBLIC désirant une solution de type « clé en main ».

Par « clé en main », il est entendu que le FOURNISSEUR assume l'ensemble des dépenses liées à la mise en place et au maintien de la solution. Ceci inclut, sans s'y limiter :

- Un hébergement par le FOURNISSEUR, dans ses installations physiques, en colocation ou par une tierce partie sous sa responsabilité
- Les mises à jour et l'entretien de la solution sont de la responsabilité du FOURNISSEUR
- Les dispositions pour atteindre les niveaux de disponibilité sont de la responsabilité du FOURNISSEUR

Les infrastructures et tout logiciel ou composante requis pour le fonctionnement sécuritaire de la solution conformément aux exigences décrites dans le présent devis sont fournies et hébergées par le FOURNISSEUR, incluant notamment:

- L'infrastructure
- Les environnements
- Les serveurs
- Les logiciels tiers (exemple : licences SGBD, système d'exploitation, etc.)
- Les bases de données
- La sauvegarde et récupération des données
- La redondance et relève géographique
- Le lien internet reliant son infrastructure à l'internet, **le lien entre Internet et chacun des sites de l'ORGANISME PUBLIC et de la population est hors portée**
- L'ensemble des droits et licences sans limites de nombre d'utilisateurs et serveurs pour répondre aux besoins exprimés

Conséquemment, il doit répondre aux exigences suivantes :

- La solution et l'**ensemble des données cliniques** (collectée dans la plateforme) doivent demeurer au Canada
- Les données doivent être cryptées lors des échanges et du stockage
- La maintenance et l'entretien des serveurs ne doivent pas interférer à la disponibilité et la performance de la solution, hors des périodes convenues

Concernant les données, si l'hébergement n'est pas prévu au Canada, la solution doit avoir un chiffrement prévu avec des clés de chiffrement entreposées au Québec, autrement, les données ne doivent que transiter par le système, sans qu'il y ait d'entreposage.

Le FOURNISSEUR est responsable de l'installation ainsi que des mises à jour de la solution.

La solution doit être capable de soutenir tous les utilisateurs concurrents du RSSS incluant :

- Les utilisateurs (environ 10 000), dans le contexte actuel de la pandémie, ce nombre est approximatif. Il pourrait y avoir un besoin plus élevé.
- Les interfaces
- Toute autre connexion « machine » nécessaire au fonctionnement de la solution

La solution doit répondre aux exigences d'hébergement suivantes :

- Permet une exécution dans un environnement résilient (balancement de charge) afin d'assurer une disponibilité élevée;
- Supporte un rééquilibrage de la plate-forme d'hébergement (ex : v-motion) sans causer un arrêt de service de la solution.

Base de données (le cas échéant) :

- Doit pouvoir être distante des serveurs Web et protégée par un bastion de sécurité (coupe-feu)

#### 5.6.1. Niveaux de service

Les niveaux de service suivants doivent être respectés par la solution :

- Environnement de production :
  - Taux de disponibilité : **99,5%**, excluant les arrêts planifiés sur un service 24/7, soit une indisponibilité par année de 1,83 jours équivalent à 3,60 heures/mois ou 50,4 minutes/semaine ou 7,2 minutes par jour et ce globalement pour la province.
  - Perte de données maximale admissible (Recovery Point Objective – RPO) ; délai durant lequel les mises à jour des données par les utilisateurs avant la panne majeure sont perdues : **4 heures**.
  - Délai de reprise attendu (Recovery Time Objective – RTO) ; délai maximum nécessaire pour rendre disponibles les services à l'utilisateur après la décision d'activer la relève à la suite d'une panne majeure : **4 heures**.
  - Le taux de rétention exigé est de : 16 derniers jours, 1 mensuel et 1 annuel par année pour la durée du contrat incluant les renouvellements, le cas échéant.
  - Les entretiens planifiés doivent être convenus avec l'ORGANISME PUBLIC, en dehors des heures de service et sont exclus du calcul de la disponibilité.
- Environnements de pré-production et de démo :
  - Niveau de disponibilité : 90 %, ceci est l'équivalent d'un potentiel de non-disponibilité de 36.5 jours par année, sur les heures normales d'affaires.

Le service offert est de 6 heures à minuit, excluant les fins de semaine et les jours fériés.

#### 5.6.2. Arrêts planifiés

Afin d'exécuter des travaux d'entretien, d'amélioration et de rehaussement, le FOURNISSEUR peut effectuer des arrêts planifiés, en tenant compte du fait que les arrêts planifiés :

- S'effectuent sur approbation préalable de l'ORGANISME PUBLIC
- Peuvent s'effectuer hors des heures normales d'affaires, selon un horaire à convenir avec l'ORGANISME PUBLIC, mais préférablement entre 21H30 et 6:00 du matin
- Peuvent s'effectuer exceptionnellement la fin de semaine
- Habituellement, sont planifiés minimalement 2 semaines à l'avance. Dans un contexte d'urgence, un préavis minimal de 48h est exigé. Un calendrier annuel doit être soumis pour approbation à l'ORGANISME PUBLIC, étant entendu que des arrêts peuvent s'ajouter en cours d'année, au besoin.



## 5.7. Performances

---

### 5.7.1. Exigence sur l'exécution

---

L'utilisation de la solution par un utilisateur ne doit en aucun temps empêcher le fonctionnement de la solution pour les autres utilisateurs.

### 5.7.2. Surveillance

---

Le FOURNISSEUR dispose d'un mécanisme de notification et d'escalade des alertes sur le dépassement des seuils acceptables des différents indicateurs de service et de performance. Les seuils seront définis conjointement entre l'ORGANISME PUBLIC et le FOURNISSEUR lors du déploiement de la solution.

## 5.8. Données

---

L'accès et l'exploitation des données doivent être permis et soutenus par le FOURNISSEUR à tous les paliers d'agrégation.

La solution permet l'interrogation des données à partir d'une méthodologie convenue entre le FOURNISSEUR et l'ORGANISME PUBLIC. Les données sont accessibles selon les paramètres entendus dans la portée, par les mécanismes d'accès aux rapports entendus.

Le FOURNISSEUR doit mettre en place un processus par lequel l'ORGANISME PUBLIC peut visualiser de façon autonome les données nécessaires, et ce en n'affectant pas les performances de la production (ex. : réplique de la base de données de production, etc.).

## 5.9. Interopérabilité des systèmes

---

La solution doit rendre disponible par des interfaces (ex. : service Web, connecteurs, vues, etc.) les données nécessaires aux échanges avec les autres systèmes du RSSS et de ses partenaires. Des interactions bidirectionnelles avec certaines interfaces, pour insérer ou extraire des données, sont requises. À la demande et à la satisfaction de l'ORGANISME PUBLIC, le transfert des données effectués par ces services doivent être chiffré et assurer la sécurité des échanges d'information. L'ensemble des coûts des services d'interopérabilité requis, incluant la documentation et la configuration, dans le cadre de l'interopérabilité de la solution avec les systèmes actuels et à venir pour toute la durée du contrat. Les spécifications détaillées des services à mettre en place sont fournies en cours du contrat et au fur et à mesure des déploiements.

Le FOURNISSEUR doit s'assurer de fournir les interfaces requises dans sa solution, de les documenter et de collaborer avec l'ORGANISME PUBLIC dans la création des connecteurs. L'ORGANISME PUBLIC prend en charge les interfaces des systèmes à connecter.

### 5.10. Cadre normatif de la gestion de l'identification de l'utilisateur (GIU)

---

Le FOURNISSEUR doit respecter le cadre normatif de la gestion de l'identification de l'utilisateur.

### 5.11. Interfaces applicatives

---

Le FOURNISSEUR doit pouvoir fournir les interfaces applicatives pour les échanges avec différents systèmes externes identifiés par l'ORGANISME PUBLIC.

La solution doit permettre l'envoi des données ciblées de façon granulaire vers un système distant.

## 5.12. Évolution de la solution

### 5.12.1. Rehaussement des infrastructures

Tout au long du contrat, le FOURNISSEUR doit procéder au rehaussement de ses infrastructures pour répondre au niveau de service demandé. De plus, l'ensemble de la solution doit être et demeurer compatible, tout au long du contrat, avec les logiciels utilisés sur les postes de travail incluant les mises à jour (autant mineure [ex. rustine de sécurité] que majeure [ex. Windows 10]).

### 5.12.2. Mise à jour de la solution

La solution doit être dans sa version la plus à jour (version stable), et doit être maintenue à jour en tout temps.

Le processus de déploiement d'une mise à jour doit être convenu avec l'ORGANISME PUBLIC, mais doit inclure minimalement, une phase d'approbation par l'ORGANISME PUBLIC incluant un test en pré-production, ainsi que la formation des pilotes de chaque établissement, sur la plateforme.

### 5.12.3. Processus de rehaussement des versions

Le fournisseur doit rendre disponible un processus de rehaussement des versions. Ce processus doit, entre autres, respecter les cibles suivantes :

- Minimiser le temps de non-disponibilité du système, le cas échéant
- Être exécuté en dehors des heures normales d'affaires ou selon un calendrier sujet à l'approbation de l'ORGANISME PUBLIC
- Doit comprendre en tout temps un plan de retour arrière en cas d'anomalie

Le fournisseur doit publier un registre des changements avec chaque version déployée et collaborer avec l'ORGANISME PUBLIC pour supporter la mise à jour de toute la documentation pertinente en conformité avec les changements induits (aide en ligne, guides d'utilisation de la plateforme, guides de formation sur la plateforme, etc.).

## 5.13. Certification

Une certification de la solution, effectuée par un organisme auditeur indépendant, doit également être réalisée à la demande du MSSS. Le fournisseur doit prévoir déboursier un maximum de 25 000 \$ pour obtenir cette certification. Les informations pour l'obtention de cette certification sont disponibles à l'adresse suivante : <http://ti.msss.gouv.qc.ca/Familles-de-services/Bureau-de-certification-et-d-homologation/Certification.aspx>

Les efforts investis par le fournisseur dans le processus de certification et pour les corrections nécessaires à l'obtention de cette dernière sont à ses frais. Le fournisseur doit s'assurer que la certification est maintenue tout au long du contrat pour toutes les nouvelles versions déployées de la solution.

La certification n'est exceptionnellement pas un prérequis au déploiement.

## 5.14. Service fournisseur (Service « F »)

Le FOURNISSEUR doit utiliser le service « F » (service fournisseur) de l'ORGANISME PUBLIC pour le soutien à distance. Les modalités d'accès sont disponibles pour les fournisseurs du RSSS à l'adresse suivante: <http://ti.msss.gouv.qc.ca/Familles-de-services/Infrastructures/Service-F.aspx>.

## 5.15. Sécurité

La solution doit adopter une architecture respectant les exigences légales et réglementaires du cadre normatif du RSSS en sécurité de l'information. La disponibilité, l'intégrité et la confidentialité des informations liées à la solution doivent être assurées tout au long de leur cycle de vie.

Afin d'assurer la protection des renseignements personnels et leur sécurité, le FOURNISSEUR doit déposer une architecture de sécurité, et la maintenir à jour pour l'ensemble du contrat, à la satisfaction de l'ORGANISME PUBLIC et qui respecte le cadre normatif du RSSS en matière de

sécurité.

Le FOURNISSEUR doit utiliser les standards de l'industrie pour renforcer la sécurité du système dans toutes les phases de son cycle de vie (ex. : BSIMM, OWASP, NIST, etc). Le cas échéant, le FOURNISSEUR doit assurer une protection des applications Web relativement au TOP 10 d'OWASP selon la version la plus récente publiée et maintenir à jour la protection de la solution tout au long du contrat en concertation avec l'ORGANISME PUBLIC.

Le FOURNISSEUR doit effectuer un « durcissement » (hardening) approprié de son infrastructure pour ne fournir uniquement que les ports, protocoles et services nécessaires pour répondre aux besoins de l'ORGANISME PUBLIC. Il doit présenter un plan de durcissement à l'ORGANISME PUBLIC.

La méthode de gestion des erreurs (tel que les messages d'erreur générés par l'application) contenant des données sensibles (l'ID de session, les versions de logiciel et les informations personnelles) doit les traiter comme des données confidentielles.

La solution doit chiffrer toutes les communications circulant sur le réseau de télécommunications excluant les solutions de l'ORGANISME PUBLIC qui ne le permettent pas. Les données confidentielles doivent être chiffrées lors de l'entreposage.

Le FOURNISSEUR doit assurer la sécurité afin de prévenir l'accès non autorisé, les fuites et les vols d'informations, selon un effort raisonnable. Les lieux physiques d'hébergement de la solution doivent être protégés de l'intrusion de personnes non autorisées. Des mécanismes d'identification, de surveillance, d'audits des accès aux serveurs locaux doivent être mis en place. La solution est accessible via une multitude d'appareils intelligents disparates, de niveaux de sécurité très variables. Pour ces considérations, l'application doit résister aux tentatives de cyberattaques de type, injection de codes ou autres pouvant compromettre son intégrité. Le système de BD sur lequel elle repose doit être à jour, dépourvu de toute faille de sécurité connue.

La solution doit être exempte de programmes malicieux (ex. : virus, cheval de Troie, programmes-espions, vers, etc.) et ne pas propager ceux-ci.

#### 5.15.1. Sécurité hébergement

Le fournisseur doit préciser le lieu d'hébergement des données.

L'ORGANISME PUBLIC se réserve le droit de réaliser un audit de sécurité des services infonuagiques, et ce, avec un préavis de 30 jours. Dans le cas où le FOURNISSEUR présente un rapport d'audit, l'ORGANISME PUBLIC se réserve le droit de confirmer les résultats de cet audit par une firme indépendante.

#### 5.15.2. Déclaration des incidents de sécurité

Le FOURNISSEUR doit déposer un processus documenté de gestion des incidents de sécurité. L'ORGANISME PUBLIC reconnaît les niveaux de sévérité suivants pour les incidents de sécurité :

Niveaux de sévérité	Caractéristiques
Mineur	<ul style="list-style-type: none"> <li>Affecte un secteur d'activité d'une des parties prenantes</li> </ul>
Modéré	<ul style="list-style-type: none"> <li>Affecte plusieurs secteurs d'une des parties prenantes</li> </ul>
Important	<ul style="list-style-type: none"> <li>Affecte plusieurs des parties prenantes</li> <li>Affecte de manière significative la qualité de services indispensables à la population</li> <li>Possède un potentiel fort de nuire à la réputation de l'organisme</li> <li>Affecte le respect des droits fondamentaux des personnes à la protection de leurs renseignements personnels et de leur vie privée, sans porter atteinte à la santé, à la vie ou au bien-être de ces personnes</li> </ul>



Critique	<ul style="list-style-type: none"> <li>• Un ou plusieurs services indispensables à la population ne peuvent être rendus</li> <li>• Mets en danger la santé, la vie ou le bien-être de personnes</li> <li>• Affecte le respect des droits fondamentaux des personnes à la protection de leurs renseignements personnels et de leur vie privée et, de ce fait, met en danger la santé, la vie ou le bien-être de ces personnes</li> <li>• Affecte la réputation d'une des parties prenantes, avec ou sans médiatisation</li> </ul>
----------	--

L'ORGANISME PUBLIC reconnaît la classification suivante pour la déclaration des incidents de sécurité. Le FOURNISSEUR doit utiliser cette classification.

1. Atteinte à la sécurité physique : Incident caractérisé par un accès non autorisé à un périmètre physique contrôlé (ex. : centres de traitement) et résultant en des accès non autorisés à de l'information ou une perturbation de la disponibilité des infrastructures technologiques.
2. Code malicieux : Incident caractérisé par l'installation ou l'exécution réussie (infection) d'un code malicieux sur un système, une application ou un environnement. Les codes malicieux mis avec succès en quarantaine, notamment par un antivirus, ne doivent pas être rapportés.
3. Comportement inapproprié : Incident caractérisé par une négligence, une erreur, une omission ou le non-respect des règles de sécurité.
4. Cyberattaque : Incident caractérisé par un accès non autorisé et mal intentionné visant principalement à compromettre la confidentialité, l'intégrité ou la disponibilité de l'information ou des infrastructures technologiques.
5. Dysfonctionnement technologique : Incident ayant pour cause des configurations déficientes de sécurité ou des pannes de l'infrastructure technologique ou application ayant des impacts sur la sécurité de l'information.
6. Vol ou perte d'information : Incident caractérisé par la perte ou le vol d'information sur support papier ou électronique (ex. : clé USB, ordinateur portable).

La prise en charge des incidents de sécurité doit :

1. Identifier, signaler et enregistrer les incidents de sécurité.
2. Évaluer le niveau de sévérité et classer les incidents de sécurité selon les échelles reconnues par l'ORGANISME PUBLIC.
3. Mettre en place une équipe d'intervention opérationnelle apte à prendre en charge et traiter les incidents de sécurité.
4. Mettre en place une procédure d'escalade administrative et opérationnelle qui tient compte du niveau de sévérité et de la classification des Incidents de sécurité.
5. Mettre en place une démarche d'amélioration continue assurant notamment la prévention, la détection et la réaction.
6. Transmettre un bilan des incidents de sécurité ou rendre compte d'incidents de sécurité spécifiques sur demande de l'ORGANISME PUBLIC.

L'ORGANISME PUBLIC doit être informé immédiatement des incidents de sécurité.

#### 5.15.3. Gestion des accès

De plus, la solution doit permettre une authentification de niveau N2 pour les utilisateurs (professionnels de la santé) (identifiant + mot de passe). Des mesures doivent être mises en place pour contrôler et protéger les mots de passe des utilisateurs, notamment :

- La solution doit mitiger les attaques des champs mot de passe par « brute force »
- La solution doit protéger la confidentialité des mots de passe des utilisateurs en empêchant, entre autres, l'affichage et l'impression de ces informations
- La composition du mot de passe doit être paramétrable :
  - Comprendre des lettres, des chiffres et des caractères spéciaux
  - Spécifié une longueur minimale (ex. au moins huit (8) caractères)

- Spécifié un délai d'expiration (ex. 90 jours), après lequel l'utilisateur a l'obligation de changer son mot de passe. De plus, l'historique des derniers mots de passe (nombre configurable) doit être conservé afin de s'assurer que les nouveaux mots de passe diffèrent des précédents

- La solution doit permettre la récupération ou le changement de mot de passe oublié par l'utilisateur, de façon sécuritaire, sans intervention humaine autre que l'utilisateur lui-même

La solution doit disposer d'une interface pour la création automatique des comptes utilisateurs avec des informations minimales (notamment : Nom, Prénom, Code utilisateurs, Mot de Passe, Courriel).

La solution doit permettre le chargement en bloc pour la création de comptes utilisateurs avec des informations minimales (notamment : Nom, Prénom, Code utilisateurs, Mot de Passe, Courriel). Ceci peut être réalisé par l'importation de fichier (ex. .csv).

La solution doit permettre le contrôle des accès des utilisateurs par profil et par établissement, en respectant les principes de l'accès minimal et de la séparation des tâches. La gestion des profils doit pouvoir être faite centralement. Un utilisateur doit pouvoir cumuler plusieurs profils.

Le FOURNISSEUR doit mettre en place des contrôles pour empêcher l'accès non autorisé aux applications, programmes ou codes sources, et s'assurer qu'ils sont réservés uniquement au personnel autorisé. Il doit appliquer des mécanismes d'autorisation afin d'empêcher toute manipulation non autorisée.

#### 5.15.4. Journalisation

La solution doit permettre la journalisation des accès, des modifications de données ainsi que des actions effectuées, de toutes les composantes. Cette journalisation doit être de façon exploitable par l'ORGANISME PUBLIC.

La journalisation et la gestion des journaux de sécurité doivent inclure la journalisation :

- Des accès des utilisateurs, des administrateurs et des services (ex. accès réussis et échoués, paramètres de la connexion, etc.)
- Des activités d'administration (ex. gestion des comptes, gestion des privilèges d'accès, changement d'un paramètre d'administration du progiciel, etc.);
- Des événements de sécurité (ex. alertes de sécurité du progiciel, changement à un paramètre de sécurité, défaillance d'un contrôle de sécurité, etc.).

De plus, la solution doit prendre en charge la synchronisation automatisée par horodatage au moyen du protocole de synchronisation réseau (NTP). La confidentialité et l'intégrité des journaux de sécurité doivent être protégées. En particulier, les journaux de sécurité sont protégés des modifications, maintenant le principe « d'immutabilité » de ces derniers.

Les données de journalisation doivent être conservées pendant toute la durée du contrat. La solution doit permettre la sauvegarde des données de journalisation pour permettre de restaurer les données en cas de perte.

La solution doit avoir la capacité d'alimenter les systèmes de surveillance de l'ORGANISME PUBLIC. Le FOURNISSEUR doit déposer le format (syslog, etc.), la méthode de transmission (temps réel, aux deux jours, etc.) ainsi que le protocole utilisé (SFTP, FTPS, etc.) pour alimenter les systèmes de journalisation de l'ORGANISME PUBLIC aux fins de surveillance.



## 6. Services d'entretien

### 6.1. Besoins

Le fournisseur doit inclure les services d'entretien de la solution pour la durée du contrat, incluant les renouvellements le cas échéant.

Le fournisseur s'engage à un soutien selon les heures de service entendues, avec une prise en charge des problèmes critiques par du personnel qualifié. Un problème est jugé critique s'il compromet les soins et/ou la sécurité des usagers.

Le centre de support doit être capable de fournir des numéros de billets (incidents, requêtes, etc.) lors de l'ouverture d'appels. Le fournisseur doit fournir le processus de prise en charge des appels et sa façon d'assurer la disponibilité de ses ressources spécialisées afin d'assurer une résolution efficace des problèmes. Il doit également fournir son modèle de soutien.

### 6.2. Exigences en matière de soutien

#### Services de soutien :

Désigne un service de soutien technique permettant de répondre aux questions des utilisateurs et de résoudre les problèmes rencontrés lors de l'opération et de l'exploitation de la solution.

L'ORGANISME PUBLIC assume le soutien de niveau 1. Il procède au tri des demandes d'assistance et à la résolution des incidents mineurs. Il escalade les demandes d'assistance non résolues auprès du FOURNISSEUR, qui agit à titre de deuxième et dernier niveau, pour les éléments l'impliquant.

Tous les coûts relatifs à l'offre de services en matière de soutien doivent être inclus dans les coûts des services d'entretien.

#### Résolution des problèmes :

La résolution des problèmes implique nécessairement le retour à un « fonctionnement et à des performances normales ». Le fournisseur atteste qu'il s'engage à :

- Intervenir rapidement afin de régler le problème et sa cause
- Prendre en charge les problèmes rencontrés et mettre en œuvre toutes les ressources humaines et matérielles nécessaires pour obtenir le rétablissement complet des services dans les meilleurs délais
- Maintenir l'intégrité de la configuration de la solution durant l'intervention visant la résolution du problème
- Faire en sorte que les correctifs apportés n'entraînent pas de diminution de service ou de nouveaux problèmes

Le fournisseur doit donc prévoir des méthodes d'intervention en cas de problème ou de panne permettant de continuer à fonctionner tout en corrigeant la situation rapidement.

#### Couverture du soutien

Le fournisseur s'engage à fournir un support téléphonique ainsi qu'un système de billets d'assistance sur les heures entendues, soit de 6:00 à minuit, excluant les fins de semaine et jours fériés, en français, selon les modalités suivantes :

- La couverture durant les heures d'activités prévues : le fournisseur offre un soutien pour traiter les requêtes de toute priorité.
- La couverture en dehors des heures d'activités prévues, incluant les jours de fin de semaine et les jours fériés : le fournisseur offre un service d'urgence ainsi qu'un service de support téléphonique et par billets d'assistance pour prendre en note les requêtes de toute priorité. Les requêtes non urgentes déposées seront alors réputées l'être au prochain jour ouvrable. La réponse aux requêtes soumises sera ensuite traitée dès la prochaine période d'heures d'activités prévues, en respectant les délais de réponse et de résolution établis ci-après. Les requêtes urgentes (priorité 1) doivent être répondues selon la grille ci-dessous. Néanmoins, en raison de la situation pandémique, l'organisme public pourrait demander une intervention pour des requêtes de priorité 2, 3 ou 4, auquel cas, la banque d'heures pourrait

être utilisée pour y répondre.

#### Niveau de priorité des requêtes

Un niveau de priorité est assigné à chacune des requêtes de soutien reçues par le fournisseur. L'assignation du niveau de priorité se fait conjointement par le fournisseur et l'organisme public en tenant compte de la sévérité et de l'impact sur les opérations. Si l'organisme public se trouve en désaccord avec la priorité assignée, il doit en référer immédiatement au fournisseur selon la procédure d'escalade. Les niveaux de priorité sont définis comme suit :

##### Priorité de niveau 1

Problème rapporté sur l'environnement de production faisant en sorte que la solution dans son ensemble, ou qu'une ou des fonctions critiques de la solution, (a) sont non opérationnelles ou (b) opèrent d'une manière qui peut compromettre l'intégrité des données de production ou (c) opèrent d'une manière qui peut compromettre la sécurité des soins aux patients.

##### Priorité de niveau 2

Problème rapporté sur l'environnement de production faisant en sorte qu'une ou des fonctions non critiques du système sont (a) non opérationnelles et (b) opèrent d'une manière qui peut compromettre l'intégrité des données de production ou causent de sérieux inconvénients à l'établissement.

##### Priorité de niveau 3

Problème rapporté sur l'environnement de production faisant en sorte qu'une ou des fonctions de la solution sont (a) non opérationnelles ou opèrent d'une manière non conforme aux spécifications ou à la documentation et (b) pour lequel il existe une procédure de contournement manuel, acceptable pour l'établissement, pendant le temps de résolution.

##### Priorité de niveau 4

Problème rapporté sur un environnement autre que production, demande d'information ou demande de changement.

#### Temps de réponse et temps de résolution

Le fournisseur s'engage à offrir le service de soutien dans un temps inférieur ou égal à :

Pour les utilisateurs :

Priorité	Temps de réponse		Temps de résolution	
	Du lundi au vendredi selon les heures d'activités prévues 6:00 à 00:00	En dehors de ces heures	Du lundi au vendredi selon les heures d'activités prévues 6:00 à 00:00	En dehors de ces heures
1	1 heure	1 heure	16 heures	16 heures
2	4 heures	N/A	32 heures	N/A
3	8 heures	N/A	14 jours	N/A
4	16 heures	N/A	30 jours	N/A

##### Définition du temps de réponse

Désigne le temps entre l'appel initial par L'ORGANISME PUBLIC ou l'envoi initial du courriel et le retour d'appel par un expert logiciel qualifié du fournisseur. Pour les requêtes qui sont soumises en dehors des heures de services prévues, le calcul du temps de réponse débute à la prochaine heure normale d'ouverture suivant l'appel initial ou l'envoi initial du courriel.

##### Définition du temps de résolution

Signifie le temps entre le moment utilisé pour débiter le calcul du temps de réponse et celui où le problème est résolu selon une des avenues suivantes :

- Un correctif est installé dans l'environnement de production et l'organisme public certifie que le problème est résolu

- Le fournisseur livre une procédure de contournement durable à long terme acceptable pour l'organisme public
- L'organisme public reçoit une réponse satisfaisante à sa demande d'information
- Le fournisseur confirme que la requête est une demande de changement et que cette dernière sera considérée pour inclusion dans une des deux prochaines versions de la solution

#### Procédure d'escalade

Le fournisseur doit fournir une procédure d'escalade téléphonique. Cette procédure est disponible pour l'organisme public. Si le fournisseur est dans l'incapacité d'établir la cause du problème et/ou de déterminer la période de temps nécessaire pour le régler, il doit immédiatement en informer l'organisme public qui peut alors avoir recours à la procédure d'escalade.

#### Exigences sur l'offre de services en matière de soutien

Le soutien technique par téléphone est accessible aux employés de l'organisme public ayant été désignés par ce dernier pour agir comme interlocuteurs en ce qui a trait à l'installation ou à l'utilisation de la solution. Il n'y a pas de limite quant au nombre d'appels pouvant être effectués par ces ressources pour obtenir le soutien technique.

Le fournisseur doit inclure un processus de prise en charge des appels et les mécanismes permettant d'assurer la disponibilité de ses ressources spécialisées pendant la période de couverture du soutien afin d'assurer une résolution efficace des problèmes.

#### 6.3. Services de maintenance

Le fournisseur doit inclure les services de maintenance de la solution pour la durée du contrat. La maintenance inclut tout rehaussement ainsi que toute amélioration à la solution dont notamment, la correction des erreurs empêchant le logiciel de fonctionner selon les spécifications (problème), ainsi que mises à jour de la solution, incluant les fonctionnalités génériques que le fournisseur peut ajouter de temps à autre au logiciel.

Les procédures de maintenance doivent permettre de décomposer les tâches entre conception, spécification détaillée, tests unitaires et d'intégration, avec attribution au personnel de maintenance en fonction de profils correspondant aux tâches à réaliser.

Une procédure formelle de maintenance corrective (correction des erreurs dans le logiciel) doit être établie, documentée et suivie. Elle doit prévoir les moyens de revenir à la situation antérieure en cas de problème.

Le fournisseur doit rendre disponibles les nouvelles versions de sa solution en temps opportun. Il doit livrer des versions qui s'adaptent aux modifications des logiciels tiers (systèmes sources) afin de maintenir la compatibilité. Il doit rendre disponibles les correctifs (rustines) dans un délai acceptable (8 semaines maximum pour se conformer à la sécurité et pour l'adaptation aux changements dans le système d'exploitation). La distribution des correctifs doit être automatisée autant que possible.

Le produit doit inclure l'ensemble des outils et des processus nécessaires à la maintenance, à la gestion des versions et à la graduation des composantes afin de mettre en place un processus de contrôle des versions.

Tous les coûts relatifs à l'offre de services en matière de maintenance doivent être inclus dans les coûts des services d'entretien.

## **7. Organisation du projet**

### 7.1. Le chargé de projet de l'organisme public

Le chargé de projet de l'organisme public doit notamment :

- Prendre en charge les communications liées au projet
- S'assurer du suivi des échéanciers, autant auprès du fournisseur
- Assurer le suivi des orientations



- Suivre l'ensemble des travaux liés au projet
- Approuver les différents livrables
- Approuver, lorsque requis, des demandes d'intervention visant l'utilisation de la banque d'heures
- Effectuer le suivi des points en suspens

Il s'assure de la disponibilité des ressources internes et des expertises nécessaires pour soutenir l'exécution du contrat.

#### 7.2. Chargé de projet du fournisseur

Le chargé de projet du fournisseur est responsable de la réalisation de tous les travaux et services requis du fournisseur dans le cadre de la mise en œuvre de la solution. Parmi les activités qu'il doit réaliser, il doit notamment :

- Produire et mettre à jour sur une base mensuelle, les rapports d'avancement
- En collaboration avec l'organisme public, voir à l'assignation d'un nombre suffisant de ressources possédant l'expérience et les expertises requises afin de réaliser tous les travaux confiés dans les délais demandés
- Prendre en charge promptement la réalisation, soit personnellement ou par les membres de son équipe, de toutes les demandes de services et d'informations qui lui seront adressées par l'organisme public (dans les délais entendus avec l'organisme public)
- Assurer la planification et le suivi des travaux
- Informer l'organisme public de toute préoccupation, tout enjeu et tout risque pouvant compromettre l'atteinte d'une solution intégrée, disponible, stable et performante
- S'assurer que les travaux confiés soient exécutés dans le respect des échéanciers
- Réaliser la reddition de compte auprès de l'organisme public
- Être disponible durant la mise en œuvre et le déploiement

#### 7.3. Reddition de compte

La méthodologie Macroscope sera utilisée pour la reddition de compte et le suivi du projet entre le FOURNISSEUR et l'ORGANISME PUBLIC (M050).

#### 7.4. Échéancier des travaux et disponibilité des services

Le fournisseur doit prévoir toutes les ressources humaines, matérielles et financières requises afin de respecter les échéanciers des travaux demandés par l'organisme public dans le cadre du présent appel d'offres.

### **8. Gestion du changement et formation**

#### 8.1. Gestion du changement

Les activités liées à la gestion du changement sont prises en charge par l'organisme public, excluant les éléments de formation énumérés à la section Formation. Le fournisseur doit néanmoins soutenir l'organisme public dans l'élaboration du plan de gestion du changement, en mettant à profit ses expériences antérieures dans la mise en place de la solution. À ce titre, le fournisseur a un rôle-conseil auprès de l'organisme public.

#### 8.2. Formation

##### *Super utilisateurs*

Le nombre de ressources à former est à évaluer selon le besoin dans le contexte actuel.

##### **Objectifs de formation**

Les objectifs de formation sont les suivants :

- Au terme de la formation, les super-utilisateurs doivent être autonomes dans l'utilisation de fonctions qui leur sont attribuées de la solution
- Ils doivent à ce titre être en mesure et ce, de manière autonome, de former les ressources de l'organisme public sur la plateforme
- Ils doivent également être en mesure de former les agents administratifs sur la plateforme

#### *Ressources TI*

Le nombre de ressources à former est à évaluer selon le besoin dans le contexte actuel.

#### **Objectifs de formation**

Les objectifs de formation sont les suivants :

- Les ressources TI doivent acquérir une connaissance suffisante, d'un point de vue technologique, de la solution pour assurer un niveau de soutien aux utilisateurs et aux répondants le cas échéant.

#### **8.3 Matériel de formation et de soutien**

Le FOURNISSEUR doit collaborer avec l'ORGANISME PUBLIC pour la production du matériel de formation adapté à la solution et aux différents profils, tout en tenant compte d'un arrimage aux processus d'affaires de l'organisme public.

Le matériel de formation est à rendre disponible en français et en anglais.

Le FOURNISSEUR collabore avec l'organisme public pour la mise à jour du matériel de formation sur la plateforme pendant toute la durée du contrat.

La formation est axée sur l'utilisation de la plateforme. Elle exclue toute formation clinique ou toute autre formation en lien avec le processus d'affaires de l'ORGANISME PUBLIC.

#### **Matériel didactique**

Le matériel didactique pour les différents profils est élaboré en collaboration avec l'ORGANISME PUBLIC et le FOURNISSEUR.

#### **Guide d'utilisation**

Un guide d'utilisation est rendu disponible par le fournisseur. Ce guide doit refléter toutes les améliorations et mises à jour de la solution en temps réels. La reproduction du guide est autorisée, notamment à des fins de formation.

### **9. Services sur demande : Interfaces**

En plus des livrables présents dans la liste préliminaire décrite à la section 12, il est possible qu'en cours de contrat, l'organisme public ait besoin de mettre en place de nouvelles interfaces.

Tous les travaux nécessaires pour la mise en place de nouvelles interfaces seront encourus dans la banque d'heures.

### **10. Services sur demande : Banque d'heures**

Le montant identifié pour les trajectoires COVID-19 est une banque d'heures à utilisation sur demande estimée pour la réalisation des biens livrables annexés. Ce montant inclut tous les travaux requis jusqu'à la mise en place des biens livrables attendus.

La banque d'heures est prévue pour la gestion des risques et de complexité de trajectoires cliniques spécifiées au moment de l'évaluation des priorités et des besoins. En cas de dépassement anticipé du coût prévu, le fournisseur doit informer l'organisme public pour procéder à une entente mutuelle de planification de l'utilisation de la banque d'heures, telle que décrit dans la section [1.4 Besoins optionnels](#), **avant** l'utilisation de celle-ci.

La banque d'heures peut aussi être sollicitée en cas de demande de changement ou selon la clause d'annulation de livrables, tel que décrit dans la section [1.5 Processus d'acceptation](#).

#### **11. Modalités de décaissement**

---

Le fournisseur peut facturer les coûts d'infrastructure, d'hébergement, de licences et de support niveau 2 dès la signature du contrat.

La banque d'heures est facturable mensuellement sur présentation des justificatifs d'utilisation par le fournisseur et sur approbation de l'organisme public, en respect du plan d'utilisation de la banque d'heures.

## 12. Liste préliminaire des demandes de changement 2021-2022

Note : Cette liste n'est pas complète et sera validée en temps opportun entre les parties prenantes afin de prioriser, annuler ou même ajouter de nouvelles demandes.

Elle a pour objectif de donner une idée au prestataire de services un aperçu des besoins à combler.

Volet	No	Description de la demande
<b>1 -</b>		<b>Adapter le questionnaire d'enquête des cas</b>
	1.1	Prendre en charge les lieux Hors QC pour section Contacts, Endroits et Exposition
	1.2	Distinguer les valeurs sans réponses versus les valeurs Inconnues
	1.3	Acquisition probable: Hypothèse du cas et de l'enquêteur + synchronisation V10
	1.4	Gérer manuellement l'affichage automatique des dates (Q2)
	1.5	Ajout de la date premier et dernier contact (Q3)
	1.6	Identifier Exposition continue (Q3)
	1.7	Ajout de questions sur la gestion du risque (port du masque, ...)
	1.8	Ajout de champs texte libre dans le questionnaire (pour les enquêteurs seulement)
<b>2 -</b>		<b>Gérer des épisodes multiples de l'infection ou contact pour une personne</b>
	2.1	Ajustements structure de données pour avoir la notion d'épisodes dans les vues INSPQ
<b>3 -</b>		<b>Gérer les doublons de façon robuste à la création d'un citoyen (FIPA)</b>
	3.1	Fonction de recherche de doublons (améliorations)
	3.2	Intégration au registre FIPA pour l'intégrité des données (et adresses)
	3.3	Fusion de citoyen (outils de "ménage" pour usage autonome et traçabilité)

<b>4 -</b>	<b>Intégrer les résultats de laboratoire (PCR) dans TSP</b>
4.1	Laboratoires TSP: Automatiser l'association au citoyen quand il y a une identification non ambiguë
4.2	Récupération des résultats négatifs pour traiter les faux positifs
4.3	Interface Dépistage Deloitte (Reporting généralisé)
4.4	Synchroniser le lieu de prélèvement et le laboratoire d'analyse dans la fiche signalétique (Q1) + mise à jour des référentiels
4.5	Réceptionner les amendements aux résultats de laboratoire - notion d'avertissement
4.6	Voir l'information du résultat dans la liste Requêtes/questionnaire associée au cycle labo
4.7	Identifier le cycle source qui a généré le cycle labo ou le cycle cas
<b>5 -</b>	<b>EBMD (Tests rapides)</b>
5.1	Autres demandes d'améliorations de la requête
5.2	Pilotage des données (CDD - prescripteurs, laboratoires, NS des appareils)
5.3	Requête web Labos privés
5.4	Intégration avec Nosotech
5.5	Alimentation au DSQ ou service web pour accéder aux données de laboratoires EBMD
5.6	Adaptation des accès de la recherche FIPA pour les utilisateurs EBMD
5.7	Étiquette nominative du citoyen pour le prélèvement
<b>6 -</b>	<b>Outil d'auto-évaluation pour le dépistage</b>
6.1	Mettre l'outil aux normes graphiques PVI
6.2	Évolution selon les recommandations de la SP
<b>7 -</b>	<b>Intelligence d'affaires et gestion de la donnée</b>
7.1	Accès direct aux données TSP pour les régions (Rapports comparatifs automatisés)
7.2	Optimisation Architecture Phase 2: Structure de données pour le reporting
7.3	Dictionnaire de données d'équivalences entre les systèmes (TSP, V10, Infocentre)
7.4	PowerBI Embedded pour accéder aux données de reporting via la plateforme



<b>8 -</b>	<b>Soutenir et faciliter la gestion des opérations en Direction de santé publique</b>
8.1	Automatisation CAS - CONTACT (nouvelles améliorations aux travaux antérieurs)
8.2	Donner accès à tous les utilisateurs en modification à l'ensemble des cas/contacts
8.3	Optimiser le tableau de bord dans TSP pour, entre autres, faciliter le suivi, l'assignation et la communication des dossiers à l'aide de statuts calculés ou attribués par le personnel.
8.4	Produire des listes filtrées de cas et contacts (ex:statuts des dossiers cas/contacts)
8.5	Produire des indicateurs de gestion opérationnels.
8.6	Rendre les notes évolutives disponibles à l'infocentre et ajout de champs notes dans le questionnaire pour l'enquêteur seulement (à synchroniser également)
8.7	Pilotage des actions à entreprendre
8.8	Automatiser le chargement, la modification de données en lot (ex. : code d'éclosion / statut rétabli).
<b>9 -</b>	<b>Autres travaux</b>
9.1	Amélioration de la qualité des données
9.2	Gestion des éclosions - Intégration dans le TB de gestion PowerBI
-	9.3 Journalisation et suivi des communications aux citoyens (courriels, rappels, contacts, levée isolement - pour EBMD, Contacts, Fiche signalétique)
	9.4 Historique complet des modifications
	9.5 Gestion des référentiels
	9.6 Gestion des variants et autres MADO
-	9.7 Travaux d'amélioration aux différentes trajectoires mises en place
<b>10 -</b>	<b>Adaptations d'interfaces</b>
10,1	Travaux additionnels d'interfaces (DDC ou ajouts)

**ANNEXE 3 - DECLARATION CONCERNANT LES ACTIVITES DE LOBBYISME  
EXERCEES AUPRES DE L'ORGANISME PUBLIC RELATIVEMENT A  
L'ATTRIBUTION DU CONTRAT DE GRE A GRE**

**TITRE DU PROJET** : MAINTIEN, HEBERGEMENT, SOUTIEN ET EVOLUTION DE LA PLATEFORME DE TRAJECTOIRE SANTE  
PUBLIQUE (TSP) N° : 21-0074-COVID

JE, SOUSSIGNE(E), **ALEXANDER DAHL**, PRESIDENT

PRESENTE AU MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX, ATTESTE QUE LES DECLARATIONS CI-APRES SONT  
VRAIES ET COMPLETES A TOUS LES EGARDS, AU NOM DE :

**AKINOX SOLUTIONS INC.**

*(NOM DU CONTRACTANT)*

(CI-APRES APPELE LE « CONTRACTANT »).

JE DECLARE CE QUI SUIIT :

1. J'AI LU ET JE COMPRENDS LE CONTENU DE LA PRESENTE DECLARATION.
2. JE SUIS AUTORISE(E) PAR LE CONTRACTANT A SIGNER LA PRESENTE DECLARATION.
3. LE CONTRACTANT DECLARE (COCHER L'UNE OU L'AUTRE DES DECLARATIONS SUIVANTES) :
  - A.** QUE PERSONNE N'A EXERCE POUR SON COMPTE, QUE CE SOIT A TITRE DE LOBBYISTE D'ENTREPRISE OU DE LOBBYISTE-CONSEIL OU DE LOBBYISTE D'ORGANISATION, DES ACTIVITES DE LOBBYISME, AU SENS DE LA LOI SUR LA TRANSPARENCE ET L'ETHIQUE EN MATIERE DE LOBBYISME (RLRQ, CHAPITRE T-11.011) ET DES AVIS EMIS PAR LE COMMISSAIRE AU LOBBYISME\*, PREALABLEMENT A CETTE DECLARATION RELATIVEMENT A LA PRESENTE ATTRIBUTION DU CONTRAT;
  - B.** QUE DES ACTIVITES DE LOBBYISME, AU SENS DE LA LOI SUR LA TRANSPARENCE ET L'ETHIQUE EN MATIERE DE LOBBYISME ET DES AVIS EMIS PAR LE COMMISSAIRE AU LOBBYISME\*, ONT ETE EXERCEES POUR SON COMPTE ET QU'ELLES L'ONT ETE EN CONFORMITE AVEC CETTE LOI, AVEC CES AVIS AINSI QU'AVEC LE CODE DE DEONTOLOGIE DES LOBBYISTES\*, PREALABLEMENT A CETTE DECLARATION RELATIVEMENT A LA PRESENTE ATTRIBUTION DU CONTRAT (RLRQ, CHAPITRE T-11.011, R.2).

VEUILLEZ CHOISIR UNE LETTRE (A OU B) : **A**\_\_\_\_\_.

4. JE RECONNAIS QUE, SI L'ORGANISME PUBLIC A DES MOTIFS RAISONNABLES DE CROIRE QUE DES COMMUNICATIONS D'INFLUENCE NON CONFORMES A LA LOI SUR LA TRANSPARENCE ET L'ETHIQUE EN MATIERE DE LOBBYISME ET AU CODE DE DEONTOLOGIE DES LOBBYISTES\* ONT EU LIEU POUR OBTENIR LE CONTRAT, UNE COPIE DE LA PRESENTE DECLARATION POURRA ETRE TRANSMISE AU COMMISSAIRE AU LOBBYISME PAR L'ORGANISME PUBLIC.

**Alexander Dahl**

Signé avec ConsignO Cloud (09/04/2021)  
Vérifiez avec ConsignO ou Adobe Reader.

notarius

ET J'AI SIGNE, \_\_\_\_\_  
(SIGNATURE ET DATE)

\* LA LOI, LE CODE ET LES AVIS EMIS PAR LE COMMISSAIRE AU LOBBYISME SONT DISPONIBLES A CETTE ADRESSE :  
[WWW.COMMISSAIRELOBBY.OC.CA](http://WWW.COMMISSAIRELOBBY.OC.CA).

#### ANNEXE 4 – ENGAGEMENT DE CONFIDENTIALITÉ

Je, soussigné(e), Alexander Dahl, exerçant mes fonctions au sein d'Akinox Solutions Inc., déclare formellement ce qui suit :

1. Je suis un(e) employé(e) de cette entreprise et, à ce titre, j'ai été affecté(e) à l'exécution du mandat faisant l'objet du contrat de services concernant le maintien, l'hébergement, le soutien et l'évolution de la plateforme de Trajectoire Santé Publique (TSP) entre le ministre de la Santé et des Services sociaux et mon employeur en date du **2021-04-01** ;
2. Je m'engage, sans limites de temps, à garder le secret le plus entier, à ne pas communiquer ou permettre que soit communiqué à quiconque quelque renseignement ou document, quel qu'en soit le support, qui me sera communiqué ou dont je prendrai connaissance dans l'exercice ou à l'occasion de l'exécution de mes fonctions, à moins d'avoir été dûment autorisé à le faire par le ministre de la Santé et des Services sociaux ou par l'un de ses représentants autorisés;
3. Je m'engage également, sans limites de temps, à ne pas faire usage d'un tel renseignement ou document à une fin autre que celle s'inscrivant dans le cadre des rapports contractuels entretenus entre mon employeur et le ministre de la Santé et des Services sociaux;
4. J'ai été informé(e) que le défaut par le (la) soussigné(e) de respecter tout ou partie du présent engagement de confidentialité m'expose ou expose mon employeur à des recours légaux, des réclamations, des poursuites et toute autre procédure en raison du préjudice causé pour quiconque est concerné par le contrat précité;
5. Je confirme avoir lu les termes du présent engagement et en avoir saisi toute la portée.

**Alexander Dahl**

Signé avec ConsignO Cloud (09/04/2021)  
Vérifiez avec ConsignO ou Adobe Reader.



---

*(Signature du déclarant ou de la déclarante)*



## ANNEXE 5 – FICHE D'INFORMATION SUR LA DESTRUCTION DES DOCUMENTS CONTENANT DES RENSEIGNEMENTS PERSONNELS

Tout organisme ou toute entreprise privée qui recueillent, détiennent, utilisent ou communiquent des renseignements personnels doivent mettre en place des mesures de sécurité propres à préserver le caractère confidentiel de ces données. Cette obligation découle à la fois de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels dans le secteur privé*. À la suite d'incidents majeurs qui lui ont été signalés, la Commission d'accès à l'information a réfléchi sur les moyens à prendre pour assurer la protection du caractère confidentiel des renseignements personnels au moment de leur destruction.

Au sein de l'organisme ou de l'entreprise, il est important que chaque employé, à son poste de travail, se sente responsable d'assurer la protection des renseignements personnels qu'il traite. C'est ainsi qu'il ne doit pas jeter au rebut les documents, cartes de mémoire flash, clés USB, disques durs d'ordinateur, CD, DVD, etc. qui en contiennent, sans s'être assuré au préalable que leur contenu ne peut être reconstitué.

La Commission suggère aux organismes et entreprises de désigner une personne qui sera responsable de mettre en place et de surveiller l'application d'une politique sur la destruction de documents contenant des renseignements personnels.

Le déchiquetage de documents sur support papier, le formatage de médias numériques réutilisables et la destruction physique de médias numériques non réutilisables demeurent les meilleures méthodes de destruction des documents confidentiels. Si les spécifications techniques de la déchiqueteuse de l'entreprise ne répondent pas au volume des documents sur support papier à détruire, il faut les entreposer dans un endroit fermé à clef avant de les confier à une entreprise spécialisée de récupération de papier.

La Commission voit mal comment la destruction des documents contenant des renseignements personnels puisse s'effectuer sur la foi d'une simple entente verbale. Aussi, un contrat en bonne et due forme concernant la destruction des documents devrait-il contenir au moins des clauses spécifiant :

- le procédé utilisé pour la destruction des documents;
- la nécessité d'un accord préalable entre les parties avant de confier la destruction des documents confidentiels à un sous-contractant;
- les pénalités aux dépens de l'entreprise de récupération si elle ne respecte pas ses engagements.

En outre, dans ce même contrat, la Commission est d'avis que l'entreprise de récupération devrait :

- reconnaître que les renseignements personnels contenus dans les documents sont de nature confidentielle;
- faire signer un engagement à la confidentialité à toute personne qui aura à manipuler ces documents;
- s'engager à ce que les documents soient entreposés dans des locaux sécuritaires et qu'ils soient toujours sous bonne garde jusqu'à leur destruction;
- veiller à limiter de façon très stricte l'accès aux lieux où les documents sont entreposés ou transformés;
- s'engager à ne pas céder les documents en sa possession à des tiers à des fins autres que la transformation du papier préalablement et obligatoirement déchiqueté;
- assurer à son client le droit d'avoir accès en tout temps à ses installations, toute la durée du contrat;
- voir à la destruction totale des documents qui ne font pas l'objet d'une transformation;
- faire rapport à son client lors de la destruction des documents reçus.

**ANNEXE 6 – ATTESTATION DE DESTRUCTION DES RENSEIGNEMENTS  
PERSONNELS ET CONFIDENTIELS**

Je, soussigné(e), \_\_\_\_\_  
*(Prénom et nom de l'employé(e))*  
 exerçant mes fonctions au sein de \_\_\_\_\_  
 dont le bureau principal est situé à l'adresse \_\_\_\_\_  
 \_\_\_\_\_,  
 déclare solennellement que je suis dûment autorisé(e) à certifier que les renseignements personnels  
 et confidentiels communiqués par le ministre ou toute autre personne dans le cadre du projet octroyé à  
 \_\_\_\_\_  
*(Nom du fournisseur)*  
 et qui prend fin le \_\_\_\_\_, ont été détruits selon les méthodes suivantes :  
*(Date)*

**Cochez les cases appropriées :**

<input type="checkbox"/>	par déchiquetage : renseignements sur support papier
<input type="checkbox"/>	par destruction logique et effacement physique en utilisant un logiciel de réécriture : renseignements sur support informatique
<input type="checkbox"/>	par un autre mode de destruction : préciser le support et le mode de destruction _____ _____ _____ _____ _____

EN FOI DE QUOI, J'AI SIGNÉ À \_\_\_\_\_, CE \_\_\_\_\_ JOUR  
 DU MOIS DE \_\_\_\_\_ DE L'AN \_\_\_\_\_.

\_\_\_\_\_  
*(Signature de l'employé(e))*

**À remplir seulement après la destruction des renseignements. Cependant, vous devez cocher une  
des cases de l'article 19 du contrat, au moment de sa signature.**