eHealth Ontario
www.ehealthontario.on.ca

Guide des normes d'interaction avec les services

Gestion des incidents, des problèmes et des changements

Version : 3

Date : Le 7 novembre 2017

ID du document : 4164

Ontario
eHealth Ontario

Avis de droit d'auteur

Tous droits réservés

Marques de commerce

Contrôle de document

La version électronique du présent document est reconnue comme étant la seule version valide.

Niveau de sensibilité du document

Renseignements qui sont généralement mis à la disposition du personnel, des conseillers et des fournisseurs de cyberSanté Ontario, ainsi que des personnes autorisées qui ne travaillent pas pour cyberSanté Ontario. Une fuite de tels renseignements n'aurait qu'une incidence minimale.

Historique des révisions

N° DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS
3	Le 2017-11-07	Nouvelle publication de l'examen trimestriel – Mises à jour des organigrammes pour la protection de la vie privée compte tenu de l'ajout de points de contact, soit Service Ontario et le Bureau d'accès à l'information et de la protection de la vie privée du MSSLD, selon le cas, en consultation avec le personnel du ministère. Le 2018-02-07: Traduit en Français. (Translated to French.)
2	Le 2016-09-30	Nouvelle publication de l'examen trimestriel - Correction des heures d'ouverture du service d'assistance de cyberSanté Ontario; exigence supplémentaire relativement à l'approbation du propriétaire du service pour les changements de la fenêtre d'entretien régulière; modifications au format. En fonction de la version de l'ébauche 1.01_20160930
1	Le 2016-02-19	Premier Guide des normes d'interaction avec les services, établir à partir de la version provisoire 0.03

Table des matières

Liste des figures

Liste des tableaux

1.0 Introduction

1.1 Objectif du document

Le présent Guide des normes d'interaction avec les services vise à garantir une communication adéquate entre les organismes en ce qui a trait à la gestion des incidents, des problèmes et des changements en lien avec les services de cyberSanté Ontario, pour qu'un organisme partenaire puisse comprendre, adopter et communiquer les points d'interaction qui le lient à cyberSanté Ontario. Ce document présente les normes de cyberSanté Ontario qui s'appliquent à l'interaction entre cyberSanté Ontario et un organisme partenaire dans le domaine opérationnel et technique de cyberSanté Ontario et pendant la durée de vie d'un service de cyberSanté Ontario. Les activités particulières du processus de gestion des incidents, des problèmes et des changements de cyberSanté Ontario entrant dans le cadre du rôle de l'organisme partenaire sont décrites pour permettre de résoudre les incidents de manière efficace, de répondre aux demandes de service, d'éviter les problèmes récurrents et les tendances indésirables en matière d'incidents, et de gérer efficacement les changements touchant l'environnement réel du service.

1.2 Portée

Les aspects du processus interne de gestion des incidents, des problèmes et des changements de cyberSanté Ontario ne sont pas décrits dans le présent document. L'adoption de ce guide ne correspond pas à l'examen ou l'approbation des processus internes de cyberSanté Ontario. Ce document décrit les normes relatives aux points de contact de cyberSanté Ontario avec les organismes partenaires, pour que les processus soient appliqués de manière uniforme d'un bout à l'autre de la chaîne de soutien.

1.3 Destinataires du document

Ce document est destiné aux équipes de gestion des incidents, des problèmes et des changements appartenant à l'une des catégories d'organisme externe ci-après qui conclut un partenariat direct avec cyberSanté Ontario dans un domaine opérationnel ou technique pour permettre le bon déroulement d'un service de cyberSanté Ontario, ci-après désigné sous le nom d'« organisme partenaire ».

- Partenaires de mise en œuvre
- Prestataires de services
- Clients
- Clientèle
- Fournisseurs[1]

[1] Les relations de fournisseur entre cyberSanté Ontario et les vendeurs tiers sont régis par des contrats en vigueur conclus entre cyberSanté Ontario et le fournisseur. Toutes modalités acceptées, tous moyens de rejoindre cyberSanté

Il s'adresse également aux employés du service à la clientèle et de la prestation de services de cyberSanté Ontario qui sont chargés de répondre aux demandes de service, aux incidents et aux demandes d'information liées aux incidents.

Les organismes partenaires qui ont conclu des partenariats directs avec des prestataires de services tiers ou des fournisseurs tiers qui participent à la chaîne de soutien de tout service de cyberSanté Ontario ont la responsabilité de communiquer les normes de cyberSanté Ontario figurant dans le présent guide à leurs prestataires de services tiers et à leurs fournisseurs tiers.

> **Note:** Le Guide des normes d'interaction avec les services de cyberSanté Ontario est soumis au processus de gestion des changements. Il est considéré comme un élément de configuration et appartient à cyberSanté Ontario.

2.0 Gestion des incidents

Cette section vise à offrir un cadre de référence pour les interactions d'un organisme partenaire avec cyberSanté Ontario aux fins de la gestion des incidents. Le processus de gestion des incidents de cyberSanté Ontario suit la pratique exemplaire ITIL (Information Technology Infrastructure Library) V3. La gestion des incidents est le processus reproductible utilisé par cyberSanté Ontario pour rétablir un service normal le plus rapidement possible et en nuisant le moins possible aux activités. Cela permet de maintenir les meilleurs niveaux de disponibilité et de service possibles, comme le stipulent les normes en matière d'objectifs de niveau de service de cyberSanté Ontario.

Pour garantir une communication adéquate entre les organismes en ce qui a trait à la gestion des incidents, la présente section décrit les points d'intégration avec un organisme partenaire et la façon dont ils seront activés le cas échéant pour contribuer aux activités de gestion des incidents de cyberSanté Ontario.

2.1 Services de dépannage

2.1.1 cybersanté Ontario Bureau des services

Le Service de dépannage de cyberSanté Ontario est composé d'un service de dépannage et d'un service d'assistance. Le Service de dépannage de cyberSanté Ontario est le point de contact pour les rapports d'incidents et les demandes de service. Il assure l'enregistrement et la gestion du cycle de vie de tous les incidents qui touchent le service opérationnel offert aux clients, notamment la coordination du soutien technique dans les groupes d'activités, et l'utilisation et la mise en œuvre des produits et des services d'infrastructure de cyberSanté Ontario en lien avec tout service de cyberSanté Ontario.

Le Service de dépannage de cyberSanté Ontario accepte les appels signalant des incidents de priorité élevée (niveaux de priorité 1 et 2) et des incidents de priorité peu élevée (niveaux de priorité 3 et 4) nuisant

---

Ontario, ainsi que les ENS et ONS qui sont énoncés dans lesdits contrats ont préséance sur l'ensemble des points de contact et des modalités énoncées dans le *Guide des normes d'interaction avec les services.*

au rendement du service de cyberSanté Ontario, et toutes les demandes de service liées à tout service de cyberSanté Ontario.

Ces appels peuvent être émis par les tiers suivants :

- Utilisateurs finaux;
- Patients ou mandataires spéciaux;
- Équipes techniques externes;
- Services de soutien externes de niveau 1;
- Services de soutien locaux;
- Services de soutien des organismes partenaires;
- Autorités locales d'enregistrement (ALE);
- Agents d'enregistrement express (AEE);
- Agents de protection de la vie privée externes;
- Agents de sécurité externes;
- Services de soutien des fournisseurs;
- ServiceOntario;
- Ministère de la Santé et des Soins de longue durée et Bureau de l'accès à l'information et de la protection de la vie privée;
- Programmes publics de médicaments de l'Ontario (PPMO);
- Direction des stratégies et des politiques de gestion de l'information (DSPGI).

Voici les coordonnées du Service de dépannage de cyberSanté Ontario :

Coordonnées	Courriel :* servicedesk@ehealthontario.on.ca Téléphone :* 1 866 250-1554 Télécopieur : 416 586-4040 (Veuillez appeler le Service de dépannage de cyberSanté Ontario si vous souhaitez envoyer une télécopie contenant des renseignements relatifs à un incident ou à une demande de service.) ** Remarque : Le téléphone est le moyen privilégié de communication du Service de dépannage de cyberSanté Ontario. À l'heure actuelle, il n'existe aucune entente de niveau de service (ENS) pour les demandes de service ou les incidents ouverts par courriel au Service de dépannage de cyberSanté Ontario. Il existe en revanche des objectifs de niveau de service (ONS). Consulter la section « Niveaux de service » du présent document pour en savoir plus.*

Heures d'ouverture	**Service de dépannage :** Le Service de dépannage de cyberSanté Ontario reçoit les appels signalant un incident 24 heures sur 24, 7 jours sur 7, 365 jours par an. **Service d'assistance :** De 8 h à 17 h, heure de l'Est (HE)

Le service d'assistance de cyberSanté Ontario dispose d'un système de secours assuré par le Service de dépannage de cyberSanté Ontario en dehors des heures d'ouverture.

2.1.2 Service de dépannage de l'organisme partenaire

Un organisme partenaire ne doit communiquer avec le Service de dépannage de cyberSanté Ontario qu'après avoir mené une enquête préliminaire et après avoir déterminé que la source du problème était liée aux services offerts par cyberSanté Ontario.

Les coordonnées du service de dépannage des organismes partenaires seront indiquées durant la phase de projet du service. Si ces coordonnées sont modifiées durant la durée de vie du service, il faut en informer le Service de dépannage de cyberSanté Ontario. Les nouvelles coordonnées sont ensuite transmises sous forme de demande de service au chef de service de cyberSanté Ontario désigné.

Les points de réacheminement et le nom des personnes-ressources en dehors des heures d'ouverture pour l'organisme partenaire doivent être établis pour la durée de vie du service et transmis au chef de service de cyberSanté Ontario désigné. Ces personnes-ressources seront contactées pour clarifier les niveaux de priorité, en cas de problème de dépannage durant le processus de résolution, pour faire un suivi sur le règlement rapide d'incidents de priorité élevée et pour faire un suivi sur le rendement du service de dépannage de l'organisme partenaire et son respect des organigrammes de soutien établis par cyberSanté Ontario.

2.2 Priorité des incidents et objectifs de niveau de service

Un incident est un événement qui ne fait pas partie du fonctionnement normal d'un service et qui entraîne ou qui peut entraîner une interruption du service ou une diminution de sa qualité. Le niveau de priorité sert à déterminer l'importance relative d'un incident en fonction de son impact et de son urgence, pour ensuite établir l'ENS du ticket. cyberSanté Ontario suit son processus normalisé de gestion des incidents pour classer les incidents touchant ses services de cyberSanté Ontario et pour leur attribuer un niveau de priorité.

Ces niveaux de priorité vont de 1 à 4 et sont attribués en fonction de l'importance du service et du nombre d'utilisateurs et de sites touchés par l'incident, c'est-à-dire en fonction de l'impact et de l'urgence :

- Les incidents de priorité 1 et 2 sont pris en charge 24 heures sur 24, 7 jours sur 7, 365 jours par an.
- Les incidents de priorité 3 et 4 sont pris en charge durant les heures d'ouverture de cyberSanté Ontario, de 8 h à 17 h, heure de l'Est (HE).

Si le service de dépannage d'un organisme partenaire qui possède ou gère des éléments permettant de mener à bien un service de cyberSanté Ontario, ainsi que les groupes de soutien associés à ces éléments, n'a pas les mêmes heures d'ouverture que cyberSanté Ontario (24 heures sur 24, 7 jours sur 7, 365 jours par an pour les incidents majeurs), l'ENS de cyberSanté Ontario n'est pas réalisable pour le service en question.

Tous les incidents doivent être signalés par téléphone au Service de dépannage de cyberSanté Ontario. Ce dernier procède ensuite à l'attribution d'un niveau de priorité, à l'enquête et à la résolution de l'incident.

Des mises à jour sur l'état de l'incident sont envoyées automatiquement par courriel à l'auteur de la déclaration par l'intermédiaire du système de tickets de cyberSanté Ontario. L'envoi de mises à jour a lieu lorsque l'incident porte l'un des états suivants : *En cours*, *En attente* ou *Résolu*.

Consulter l'annexe B pour connaître les normes de cyberSanté Ontario en matière de niveaux de priorité et d'objectifs de niveau de service pour les incidents.

2.3 Priorité des demandes de service et objectifs de niveau de service

Une demande de service est une question, une demande d'information, une plainte ou une demande d'aide liée aux services de soutien de cyberSanté Ontario. En satisfaisant à une demande de service, on appuie le rendement du service de cyberSanté Ontario concerné puisqu'on respecte l'ENS indirectement, par exemple en réinitialisant le mot de passe d'un compte d'administrateur technique.

Les niveaux de priorité normalisés de cyberSanté Ontario pour les demandes de service vont de 1 à 4. Toutes les demandes de service sont prises en charge durant les heures d'ouverture de cyberSanté Ontario, de 8 h à 17 h, heure de l'Est (HE).

Toutes les demandes de service doivent être acheminées au Service de dépannage de cyberSanté Ontario.

Consulter l'annexe C pour connaître les normes de cyberSanté Ontario en matière de niveaux de priorité et d'objectifs de niveau de service pour les demandes de service.

2.4 Classification des tickets

Les définitions des priorités d'incident figurent dans l'entente de prestataire de service conclue durant la phase de projet du cycle de vie du service de cyberSanté Ontario.

2.4.1 Incidents normaux

L'ouverture d'un ticket peut se faire de différentes manières :

1. Lors de la réception d'un appel émis par le service de dépannage de l'organisme partenaire pour signaler un incident ou présenter une demande de service en lien avec le domaine opérationnel ou technique de cyberSanté Ontario touchant le service de cyberSanté Ontario, le Service de dépannage de cyberSanté Ontario ouvre un ticket.
2. Lors de la réception d'une alerte provenant d'un système de surveillance, le groupe de soutien de cyberSanté Ontario responsable de la réception des alertes crée un ticket et l'attribue à un autre groupe de soutien de cyberSanté Ontario qui prendra les mesures appropriées.
3. Lors de la réception d'un courriel envoyé par le service de dépannage de l'organisme partenaire pour signaler un incident ou présenter une demande de service en lien avec le domaine opérationnel ou technique de cyberSanté Ontario

touchant le service de cyberSanté Ontario, le Service de dépannage de cyberSanté Ontario crée un ticket[2].

Une fois créé, le ticket de cyberSanté Ontario contiendra des renseignements relatifs à l'incident. Consulter la section « Attribution d'un ticket » du présent document pour en savoir plus. Voir l'information ci-dessous.

Lors de l'ouverture d'un ticket normal, les équipes de soutien opérationnel de l'organisme partenaire peuvent être invitées à collaborer avec les équipes de soutien de cyberSanté Ontario au moyen de ponts de conférence mis en place par cyberSanté Ontario.

2.4.2 Incidents majeurs

cyberSanté Ontario fait appel au processus d'incident majeur lorsqu'un service essentiel est considéré comme indisponible ou détérioré au point d'être inutilisable. Deux niveaux de priorité peuvent être attribués à un incident majeur : P1-Critique ou P2-Élevé.

cyberSanté Ontario désigne un coordonnateur d'incident pour assurer la gestion de l'incident majeur en vue de sa résolution, au moyen d'un pont de téléconférence et de WebEx, au besoin, et en utilisant les ressources internes et externes le cas échéant. Lors de l'ouverture d'un ticket d'incident majeur, les équipes de soutien de l'organisme partenaire et celles du fournisseur peuvent être amenées à collaborer avec les équipes de soutien de cyberSanté Ontario au moyen de ponts de conférence mis en place par cyberSanté Ontario.

cyberSanté Ontario informe les organismes partenaires et les utilisateurs finaux concernés si un incident nuit à l'accessibilité et à la disponibilité des services de cyberSanté Ontario en leur transmettant un avis d'interruption de service par l'intermédiaire de son Service de dépannage de cyberSanté Ontario. Lorsque le service est rétabli, un avis de rétablissement du service est transmis à ces mêmes organismes partenaires et utilisateurs finaux. Ils sont également appelés « arrêts imprévus » au sein de cyberSanté Ontario.

2.4.2.1 Examen d'incident majeur

À la suite d'un incident majeur, cyberSanté Ontario effectue un examen d'incident majeur et, au besoin, une analyse des causes fondamentales pour repérer et corriger les éventuelles lacunes relatives aux processus ou à la conception technique. L'équipe de gestion des incidents de cyberSanté Ontario programme l'examen d'incident majeur dans les deux jours ouvrables suivant l'incident (objectif) et met au point le rapport d'incident majeur dans un délai de cinq jours ouvrables (objectif). Dans la plupart des cas, l'organisme partenaire peut obtenir un exemplaire du rapport d'incident majeur s'il en fait la demande.

Les résultats de l'examen d'incident majeur sont également étudiés lors d'une réunion d'examen du service à horaire fixe qui s'inscrit dans le cadre du processus de gestion des incidents de cyberSanté Ontario.

[2] Les tickets ouverts par courriel ne sont pas rattachés à une ENS.

> **Note:** cyberSanté Ontario se réserve le droit d'exclure les renseignements sensibles (adresses IP, noms des serveurs, etc.) du rapport d'incident majeur pour garantir la sécurité et l'intégrité de ses systèmes de DME.

2.4.3 Atteinte à la sécurité

cyberSanté Ontario coordonne la gestion des incidents de sécurité qui touchent les services qu'il possède et qu'il gère. Si un incident de sécurité est détecté par cyberSanté Ontario et signalé par l'organisme partenaire ou par tout autre tiers, le Service de dépannage de cyberSanté Ontario ouvre un ticket et le processus d'intervention en cas d'incident de sécurité de cyberSanté Ontario est déclenché.

Le Service de dépannage de cyberSanté Ontario informe l'organisme partenaire, par l'intermédiaire du service de dépannage, au sujet des incidents de sécurité et de leur résolution.

L'organisme partenaire informe cyberSanté Ontario, par l'intermédiaire de son Service de dépannage de cyberSanté Ontario, des incidents de sécurité qui ne sont pas liés au domaine de soutien opérationnel et technique de cyberSanté Ontario et de la résolution de ces incidents.

2.4.4 Incidents et violations touchant la protection de la vie privée

Les incidents touchant la protection de la vie privée doivent être traités différemment en fonction du service mis en cause et si la partie en cause est un membre du grand public (patient, mandataire spécial, ou autre), un utilisateur final (clinicien) ou un agent de protection de la vie privée local.

Tout incident possible touchant la protection de la vie privée signalé par des membres du grand public ou des utilisateurs finaux doit être traité en tant que demande d'opérations liées à la protection de la vie privée (une plainte liée à la protection de la vie privée) jusqu'à ce qu'elle soit validée par une partie appropriée,
c. -à-d. l'agent de protection de la vie privée local ou un clinicien compétent. Ainsi, le grand public doit signaler les incidents touchant la protection de la vie privée aux cliniciens (utilisateurs finaux) et les utilisateurs finaux doivent signaler les incidents ou les violations soupçonnés touchant la protection de la vie privée à cyberSanté Ontario par l'intermédiaire d'un agent de protection de la vie privée local. Les agents de protection de la vie privée locaux doivent faire appel à cyberSanté Ontario pour un soutien de niveau 1 pour tous les incidents et violations touchant la protection de la vie privée. Ces incidents et violations doivent être communiqués à cyberSanté Ontario par l'intermédiaire de son Service de dépannage de cyberSanté Ontario. Le Service de dépannage de cyberSanté Ontario crée alors un ticket et le processus de gestion des incidents et des violations touchant la protection de la vie privée de cyberSanté Ontario est déclenché. Voir les figures 2 et 3 pour consulter les organigrammes de soutien de haut niveau en ce qui a trait aux demandes d'opérations liées à la protection de la vie privée et à la gestion des incidents et des violations touchant la protection de la vie privée.

Pour les utilisateurs finaux n'ayant pas suivi de programme de sensibilisation sur les violations touchant la protection de la vie privée, les plaintes liées à la protection de la vie privée soumises à cyberSanté Ontario par les utilisateurs finaux directement ou au nom d'un patient doivent être tout d'abord validées par un agent de protection de la vie privée local, lorsqu'il y en a un.

Lorsqu'il n'y a pas d'agent de protection de la vie privée local sur les lieux, et dans les cas où la demande d'information ou la plainte liée à la protection de la vie privée a trait à ConnexionOntario ou aux services

d'images diagnostiques, le grand public doit alors soumettre les demandes d'information ou les plaintes directement à cyberSanté Ontario par l'entremise du Service de dépannage de cyberSanté Ontario, pouvant être ensuite validées et classées par le bureau de protection de la vie privée de cyberSanté Ontario à titre d'incident ou de violation touchant la protection de la vie privée, ce qui entraînerait la mise en œuvre du processus de gestion des incidents et des violations touchant la protection de la vie privée de cyberSanté Ontario. Voir la figure 2 pour consulter les organigrammes de soutien de haut niveau en ce qui a trait aux demandes d'opérations liées à la protection de la vie privée et à la gestion des incidents et des violations touchant la protection de la vie privée.

Le grand public utilise ServiceOntario en tant que premier point de contact pour soumettre une demande d'information ou une plainte liée à la protection de la vie privée pour les services du VPPP et du RNM. À ce titre, toute demande d'information ou plainte liée à la protection de la vie privée validée et qui a fait l'objet d'une enquête par le secteur de programme approprié du ministère (PPMO) est ensuite dirigée à cyberSanté Ontario par l'entremise du Service de dépannage de cyberSanté Ontario pour confirmation d'un incident ou d'une violation touchant la protection de la vie privée. Voir la figure 2 pour consulter les organigrammes de soutien de haut niveau en ce qui a trait aux demandes d'opérations liées à la protection de la vie privée et à la gestion des incidents et des violations touchant la protection de la vie privée.

Le grand public doit faire appel au Bureau de l'accès à l'information et de la protection de la vie privée du ministère de la Santé et des Soins de longue durée (MSSLD) en tant que premier point de contact pour déposer une plainte liée à la protection de la vie privée pour le service du SILO. À ce titre, toute plainte liée à la protection de la vie privée validée et qui a fait l'objet d'une enquête par le secteur de programme du ministère approprié (DSPGI) est ensuite dirigée à cyberSanté Ontario par l'entremise de son Service de dépannage de cyberSanté Ontario pour confirmation d'un incident ou d'une violation touchant la protection de la vie privée. Voir la figure 2 pour consulter les organigrammes de soutien de haut niveau en ce qui a trait aux demandes d'opérations liées à la protection de la vie privée et à la gestion des incidents et des violations touchant la protection de la vie privée.

Les incidents liés à la protection de la vie privée signalés au Service de dépannage de cyberSanté Ontario ne doivent pas contenir de renseignements personnels ou de renseignements personnels sur la santé. Si, dans le cadre du partenariat avec le bureau de la protection de la vie privée de cyberSanté Ontario, lors du processus de gestion des incidents et des violations touchant la protection de la vie privée, des renseignements personnels ou des renseignements personnels sur la santé doivent être échangés entre cyberSanté Ontario et un organisme partenaire, et s'il est impossible de régler le ticket sans procéder à cet échange, les normes de cyberSanté Ontario en matière de livraison électronique sont les suivantes :

1. Courriel : Comme suit, selon que l'organisme partenaire utilise ou non le service ONE MailMD de cyberSanté Ontario :

    a. Si l'organisme est abonné au service ONE Mail de cyberSanté Ontario, les renseignements doivent être transmis à l'adresse privacy.operations@ehealthontario.on.ca par l'intermédiaire du compte ONE Mail;

    b. Si l'organisme n'est pas abonné au service ONE Mail de cyberSanté Ontario, les renseignements doivent être transmis par courriel sous forme de documents compressés, chiffrés et protégés par mot de passe.

2. Téléphone : Appeler directement le bureau de la protection de la vie privée de cyberSanté Ontario au 416 946-4767.

3. Télécopieur sécurisé : Envoyer les renseignements par télécopie en composant le 416 586-4397 (service de télécopie du Service d'assistance de cyberSanté Ontario).

Pour la gestion des incidents et des violations touchant la protection de la vie privée, l'organisme partenaire doit fournir un soutien de niveau 2 comme suit (et selon le domaine de soutien de l'organisme) :

- Lancer une enquête à la suite d'une plainte;
- Maîtrise l'incident ou la violation;
- Informer les personnes touchées;
- Coopérer durant l'enquête sur la violation;
- Diriger l'enquête sur la violation si cyberSanté Ontario estime que c'est la procédure à suivre;
- Remédier à l'incident ou à la violation.

2.4.5 Demandes d'opérations liées à la protection de la vie privée

Les demandes d'opérations liées à la protection de la vie privée sont les suivantes :

- Blocage ou déblocage du dossier d'un patient (directive de consentement);
- Rapport du dossier d'un patient;
- Rapport de vérification d'accès au dossier d'un patient, incluant les rapports sur l'historique des directives en matière de consentement;
- Rapport de vérification pour un agent de protection de la vie privée;
- Correction de données cliniques dans le dossier d'un patient;
- Demande d'information liée à la protection de la vie privée;
- Plainte liée à la protection de la vie privée[3].

Les demandes d'opérations liées à la protection de la vie privée doivent être traitées différemment en fonction du service mis en cause et si le tiers faisant la demande est un membre du grand public, un utilisateur final ou un agent de protection de la vie privée.

Le Service de dépannage de cyberSanté Ontario est le premier point de contact pour les demandes d'opérations liées à la protection de la vie privée en provenance du grand public pour les services d'ID et

[3]Le Service de dépannage de cyberSanté Ontario achemine directement les demandes d'opérations liées à la protection de la vie privée au bureau de la protection de la vie privée de cyberSanté Ontario lorsque les demandes d'information et les plaintes ont été validées et ont fait l'objet d'une enquête de la part d'un agent de protection de la vie privée ou du secteur de programme du ministère. Ces plaintes ou demandes d'information liées à la protection de la vie privée doivent ensuite être traitées comme des incidents ou des violations soupçonnées de la protection de la vie privée jusqu'à ce qu'elles soient validées par le bureau de la protection de la vie privée de cyberSanté Ontario.

ConnexionOntario[4]. cyberSanté Ontario est chargé de remplir les demandes d'opérations liées à la protection de la vie privée, d'enquêter sur les demandes d'information et les plaintes et, après le classement et la validation d'un incident touchant la protection de la vie privée, de lancer le processus de gestion des violations de sécurité, le cas échéant, ou de demander aux organismes partenaires de répondre aux demandes ou de prendre des mesures en collaboration pour la gestion des violations, le cas échéant. Voir la figure 2 pour consulter les organigrammes de soutien de haut niveau en ce qui a trait aux demandes d'opérations liées à la protection de la vie privée et à la gestion des incidents et des violations touchant la protection de la vie privée.

ServiceOntario est le premier point de contact pour les demandes d'opérations liées à la protection de la vie privée provenant du grand public pour le service du RNM, le service du VPPP, ainsi que les demandes relatives aux directives en matière de consentement pour le service du SILO. ServiceOntario prend les mesures sous-jacentes pour les directives en matière de consentement du SILO et attribue l'achèvement de la demande au bureau de la protection de la vie privée de cyberSanté Ontario. Pour les demandes de rapport d'accès concernant le RNM (y compris les demandes de rapports sur l'historique des directives en matière de consentement), les demandes d'information ou les plaintes sont attribuées par ServiceOntario au programme du ministère, PPMO. Le PPMO prend les mesures sous-jacentes nécessaires pour ces demandes d'accès et travaille directement avec l'Unité du soutien opérationnel du RNM de cyberSanté pour régler les demandes. Pour les demandes de rapport d'accès concernant le VPPP (y compris les demandes de rapports sur l'historique des directives en matière de consentement), les demandes d'information ou les plaintes sont attribuées par ServiceOntario au programme du ministère, PPMO. Le PPMO prend les mesures sous-jacentes nécessaires pour ces demandes d'accès et travaille directement avec le Groupement ITI pour les services de santé pour régler les demandes. Si la demande vise à corriger les RPS/RP dans le dossier d'un patient, ServiceOntario avise le demandeur qu'il doit communiquer avec le point d'entrée des données (le bureau local de ServiceOntario, le praticien de soins de santé ou le pharmacien) pour qu'il effectue la correction des données à la source. Le PPMO mène les enquêtes sur les demandes d'information et les plaintes liées à la protection de la vie privée. Si celles-ci sont validées, elles sont alors signalées au Service de dépannage de cyberSanté Ontario qui lancera le processus de gestion des violations de sécurité. Voir la figure 2 pour consulter les organigrammes de soutien de haut niveau en ce qui a trait aux demandes d'opérations liées à la protection de la vie privée et à la gestion des incidents et des violations touchant la protection de la vie privée.

Pour toute autre demande d'opérations liée à la protection de la vie privée en provenance du grand public pour le service du SILO, le Bureau de l'accès à l'information et de la protection de la vie privée du ministère de la Santé et des Soins de longue durée (MSSLD) est le premier point de contact. Le BAIPVP du MMSLD attribue au SILO les demandes de rapport d'accès (y compris les demandes de rapports sur l'historique des directives en matière de consentement), les demandes d'informations ou les plaintes au programme du ministère, DGSPI. La DGSPI prend les mesures sous-jacentes nécessaires pour ces demandes et travaille directement avec le bureau de protection de la vie privée de cyberSanté Ontario pour régler les demandes. Si la demande vise à corriger les RPS/RP dans le dossier d'un patient, le BAIPVP du MMSLD avise le demandeur qu'il doit communiquer avec le point d'entrée des données (le bureau local de ServiceOntario, le praticien de soins de santé ou le pharmacien) pour qu'il effectue la correction des données à la source. La DGSPI mène les enquêtes sur les demandes d'information et les plaintes liées à la protection de la vie

[4] ConnexionOntario donne l'accès clinique aux données du SILO et du RNM. De cette façon, les demandes relatives à la protection de la vie privée ou les préoccupations liées au RNM et au SILO qui découle de l'utilisation du service de ConnexionOntario doit suivre les moyens énoncés pour chacun de ces services (tel que souligné ici).

privée. Si celles-ci sont validées, elles sont alors signalées au Service de dépannage de cyberSanté Ontario qui lancera le processus de gestion des violations de sécurité. Voir la figure 2 pour consulter les organigrammes de soutien de haut niveau en ce qui a trait aux demandes d'opérations liées à la protection de la vie privée et à la gestion des incidents et des violations touchant la protection de la vie privée.

Pour les demandes d'opérations liées à la protection de la vie privée provenant d'un agent de protection de la vie privée, en son nom, au nom d'un patient ou au nom d'un utilisateur final, l'agent de protection de la vie privée doit utiliser le Service de dépannage de cyberSanté Ontario comme premier point de contact. cyberSanté Ontario communique alors avec les organismes partenaires pour qu'ils prennent les mesures sous-jacentes ou qu'ils collaborent dans le cadre du processus de gestion des violations de sécurité, le cas échéant. Voir la figure 3 pour obtenir les détails sur les organigrammes de soutien lorsque l'agent de protection de la vie privée interagit avec cyberSanté Ontario.

> **Note:** Les demandes d'information et les plaintes liées à la protection de la vie privée signalées à d'autres points de contact sont considérées comme étant des demandes d'opérations liées à la protection de la vie privée jusqu'à ce qu'elles soient validées en tant qu'incident ou violation touchant la protection de la vie privée, après quoi le Service de dépannage de cyberSanté Ontario devient le premier point de contact pour tous les services en ce qui a trait au signalement de tout incident ou violation, tel qu'indiqué dans la section précédente.

Les demandes d'opérations liées à la protection de la vie privée adressée au Service de dépannage de cyberSanté Ontario ne doivent pas contenir de renseignements personnels ou de renseignements personnels sur la santé.

L'organisme partenaire peut être invité par le bureau de la protection de la vie privée de cyberSanté Ontario à fournir de plus amples renseignements au besoin.

L'agent de protection de la vie privée de l'organisme partenaire est en mesure de satisfaire à plusieurs types de demande :

- Directive de consentement au nom d'un patient;
- Demande d'accès si celle-ci ne concerne que les dossiers de l'organisme, incluant les demandes de rapports sur l'historique des directives en matière de consentement (voir la figure 4);
- Demande de correction;
- Demande d'information si celle-ci ne concerne que l'organisme ou s'il est en mesure d'y répondre;
- Plainte, si celle-ci ne concerne que l'organisme ou s'il est en mesure d'y répondre.

Si, dans le cadre du partenariat avec le bureau de la protection de la vie privée de cyberSanté Ontario, lors d'une demande d'opérations liée à la protection de la vie privée, des renseignements personnels ou des renseignements personnels sur la santé doivent être échangés entre cyberSanté Ontario et l'organisme partenaire, et s'il est impossible de satisfaire à la demande sans procéder à cet échange, les normes de cyberSanté Ontario en matière de livraison électronique sont les suivantes :

1. Courriel : Comme suit, selon que l'organisme partenaire utilise ou non le service ONE MailMD de cyberSanté Ontario :

    a. Si l'organisme est abonné au service ONE Mail de cyberSanté Ontario, les renseignements doivent être transmis à l'adresse privacy.operations@ehealthontario.on.ca par l'intermédiaire du compte ONE Mail;

    b. Si l'organisme n'est pas abonné au service ONE Mail de cyberSanté Ontario, les renseignements doivent être transmis par courriel sous forme de documents compressés, chiffrés et protégés par mot de passe.

2. Téléphone : Appeler directement le bureau de la protection de la vie privée de cyberSanté Ontario au 416 946-4767.

3. Télécopieur sécurisé : Envoyer les renseignements par télécopie en composant le 416 586-4397, à l'intention du service de télécopie du service d'assistance de cyberSanté Ontario.

2.4.6 Fonction de dérogation et rapports sur les dérogations pour les directives en matière de consentement

La fonction de dérogation pour une directive en matière de consentement (DMC) nécessite une interaction directe entre l'utilisateur final et une interface d'un visualiseur. Lorsque la fonction est déployée par l'utilisateur final, le visualiseur envoie alors l'information vers l'application du Système d'information aux entreprises (SIE)[5]. Le SIE envoie alors un avis automatisé, soit au bureau de protection de la vie privée de cyberSanté Ontario, soit à ServiceOntario, selon le service pour lequel la directive en matière de consentement a été envoyée (voir la figure 4). La partie chargée d'envoyer une lettre à l'intervenant concerné dépend du service mis en cause, soit :

- ConnexionOntario et visualiseur d'imagerie diagnostique – le bureau de la protection de la vie privée de cyberSanté Ontario envoie une lettre à l'agent de protection de la vie privée local, qui enverra à son tour une lettre au patient;

- SILO – le bureau de la protection de la vie privée de cyberSanté Ontario envoie une lettre au patient;

- RNM/VPPP – ServiceOntario envoie une lettre au patient.

Pour le service du RNM, les agents de protection de la vie privée locaux emploient une section libre-service dans l'application du SIE pour examiner les rapports sur les dérogations pour les directions en matière de consentement. Au cours de l'examen de ces rapports, l'agent de protection de la vie privée local peut lancer le processus de GVS en signalant la validation d'un incident touchant la protection de la vie privée au Service de dépannage de cyberSanté Ontario.

Voir la figure 4 pour obtenir les organigrammes de l'entrée des dérogations pour les directives en matière de consentement et les rapports sur les dérogations.

[5] L'application du SIE est accessible sur le portail de cyberSanté Ontario.

2.5 Attribution des tickets

Chaque organisme doit conserver, dans son outil de référence de gestion des incidents, une référence au numéro de ticket de l'autre organisme.

2.5.1 Du service de dépannage de l'organisme partenaire au Service de dépannage de cyberSanté Ontario

En cas d'incident lié au domaine de soutien opérationnel et technique de cyberSanté Ontario, le service de dépannage de l'organisme partenaire appelle le Service de dépannage de cyberSanté Ontario et procède comme suit :

- Le correspondant autorisé se présente comme membre du service de dépannage et nomme l'organisme partenaire;
- Il donne le numéro de ticket de l'organisme partenaire;
- Il décrit l'impact du problème sur le service;
- Il décrit l'impact du problème sur l'utilisateur final;
- Il donne la date et l'heure auxquelles le problème est survenu pour la première fois;
- Priorité;
- Il décrit les activités de dépannage entreprises par l'organisme partenaire pour écarter les problèmes relevant de son domaine opérationnel ou technique;
- Il indique s'il existe une solution de rechange et, s'il y en a une, la décrit.
    - Il enregistre la mention « aucune solution de rechange » ou la « solution de rechange » actuelle (le cas échéant)

> **Note:** Comme mentionné plus haut, le téléphone est le premier moyen de création de tickets auprès du Service de dépannage de cyberSanté Ontario. Les incidents signalés par courriel ne sont pas rattachés à une ENS.

2.5.2 De l'équipe de soutien de cyberSanté Ontario au service de dépannage de l'organisme partenaire

En cas d'incident lié au domaine de soutien opérationnel et technique de cyberSanté Ontario, le Service de dépannage de cyberSanté Ontario communique avec le service de dépannage de l'organisme partenaire et procède comme suit :

- Le correspondant autorisé se présente comme membre de l'équipe de soutien de cyberSanté Ontario;
- Il indique le numéro de ticket de cyberSanté Ontario;
- Il décrit l'impact du problème sur le service;
- Il décrit l'impact du problème sur l'utilisateur final;

- Il donne la date et l'heure auxquelles le problème est survenu pour la première fois;
- Priorité;
- Il indique s'il existe une solution de rechange et, s'il y en a une, la décrit.
    - Il enregistre la mention « aucune solution de rechange » ou la « solution de rechange » actuelle (le cas échéant)

2.5.3 Communication

2.5.3.1 Communication avec les utilisateurs finaux

cyberSanté Ontario ne communique pas directement avec les utilisateurs finaux dans le cas d'incidents techniques et de demandes qui relèvent uniquement de la responsabilité de l'organisme partenaire. Si un utilisateur final tente de communiquer directement avec cyberSanté Ontario pour connaître l'état d'un incident de ce type ou pour obtenir de l'aide, il sera redirigé vers le service de dépannage de l'organisme partenaire.

cyberSanté Ontario communique directement avec les utilisateurs finaux pour satisfaire aux demandes d'opérations liées à la protection de la vie privée et dans le cadre des enquêtes liées à la gestion des incidents et des violations touchant la protection de la vie privée, ainsi qu'avec le grand public, les patients et toute autre personne ou entité présentant une telle demande ou signalant un incident ou une violation, comme le décrit le schéma ci-après présentant l'organigramme de soutien de haut niveau en ce qui a trait aux demandes d'opérations de protection de la vie privée et à la gestion des incidents et des violations touchant la protection de la vie privée. Tout correspondant qui présente une telle requête ou qui signale un incident ou une violation touchant la protection de la vie privée, par l'intermédiaire du service de dépannage de l'organisme partenaire ou d'un autre point de communication central au sein de l'organisme partenaire, sera redirigé vers le Service de dépannage de cyberSanté Ontario.

Dans certains cas, l'agent de protection de la vie privée de l'organisme partenaire peut servir de premier point de triage pour une demande d'opérations liée à la protection de la vie privée ou pour le signalement d'un incident ou d'une violation touchant la protection de la vie privée. L'agent de protection de la vie privée doit ensuite informer cyberSanté Ontario par l'intermédiaire du Service de dépannage de cyberSanté Ontario.

2.5.3.2 Mises à jour

Les groupes de soutien de cyberSanté Ontario et le service de dépannage de l'organisme partenaire doivent communiquer entre eux pour faire le point sur l'état du ticket et indiquer les numéros de ticket correspondants dans leur outil de ticket respectif, et ce, assez fréquemment pour respecter l'ENS qui a été conclue.

2.5.3.3 Résolution et fermeture d'un ticket

cyberSanté Ontario et l'organe directeur de l'organisme partenaire doivent communiquer entre eux au sujet de la fermeture du ticket, au besoin, et pour indiquer les numéros de ticket correspondants une fois la résolution confirmée, comme suit :

- cyberSanté Ontario transmet un avis de fermeture de ticket au service de dépannage de l'organisme partenaire;

- L'organisme partenaire transmet un avis de fermeture de ticket au Service de dépannage de cyberSanté Ontario.

2.6 Processus d'intégration

2.6.1 Démarcation du soutien

Le point de démarcation opérationnel et technique entre cyberSanté Ontario et un organisme partenaire correspond à la frontière entre les éléments de configuration des composants détenus et gérés par l'organisme partenaire et les éléments de configuration des services de cyberSanté Ontario.

2.6.1.1 Surveillance et niveau 1 – Organigramme de soutien pour les incidents techniques et les enjeux touchant la protection de la vie privée

Le schéma suivant montre la communication de haut niveau entre cyberSanté Ontario et l'organisme partenaire en ce qui a trait aux incidents techniques.

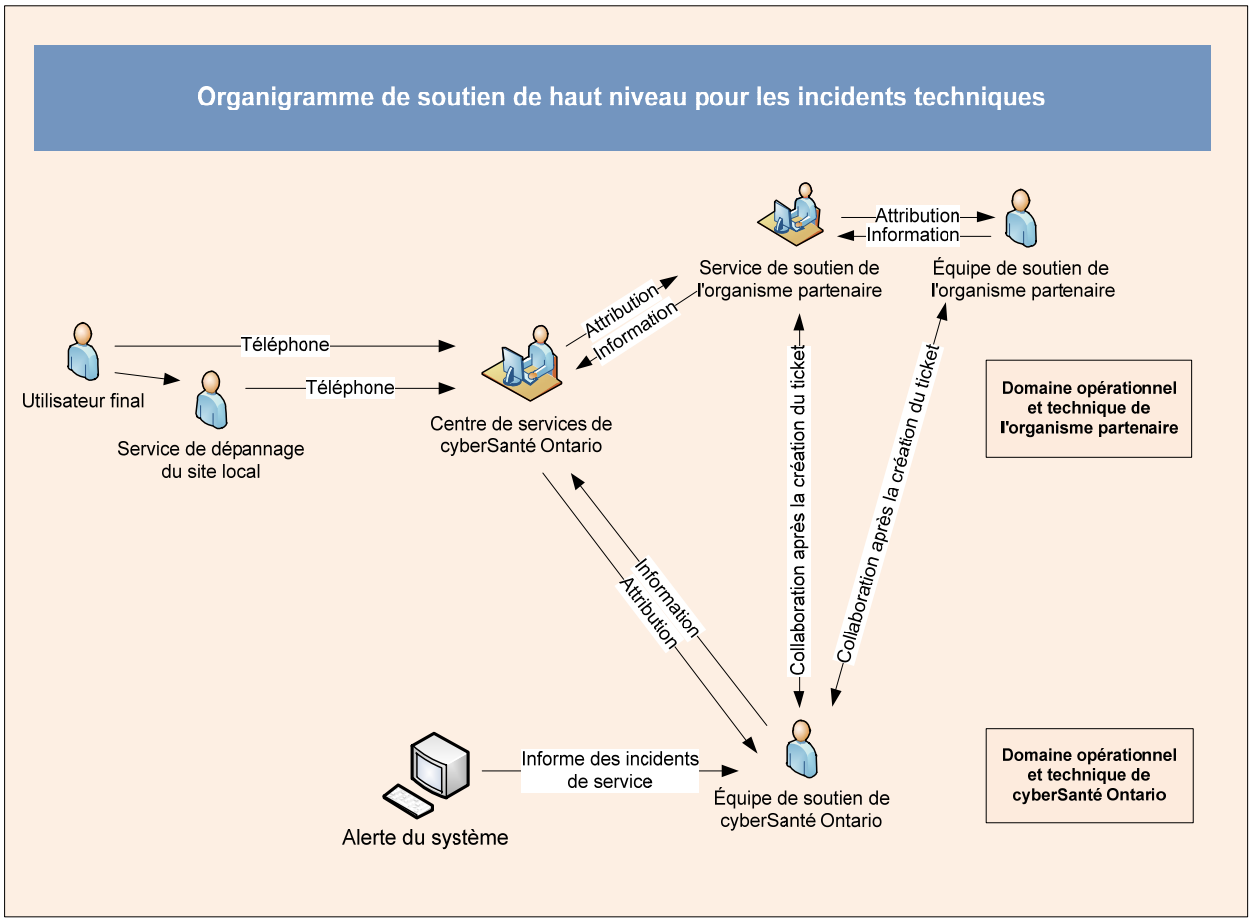


Figure 1 - Organigramme de soutien de haut niveau pour les incidents techniques

Le schéma suivant montre les interactions de haut niveau entre cyberSanté Ontario et l'organisme partenaire en ce qui a trait aux demandes d'opérations liées à la protection de la vie privée et aux incidents et aux violations touchant la protection de la vie privée dans les cas où le grand public est le déclencheur.

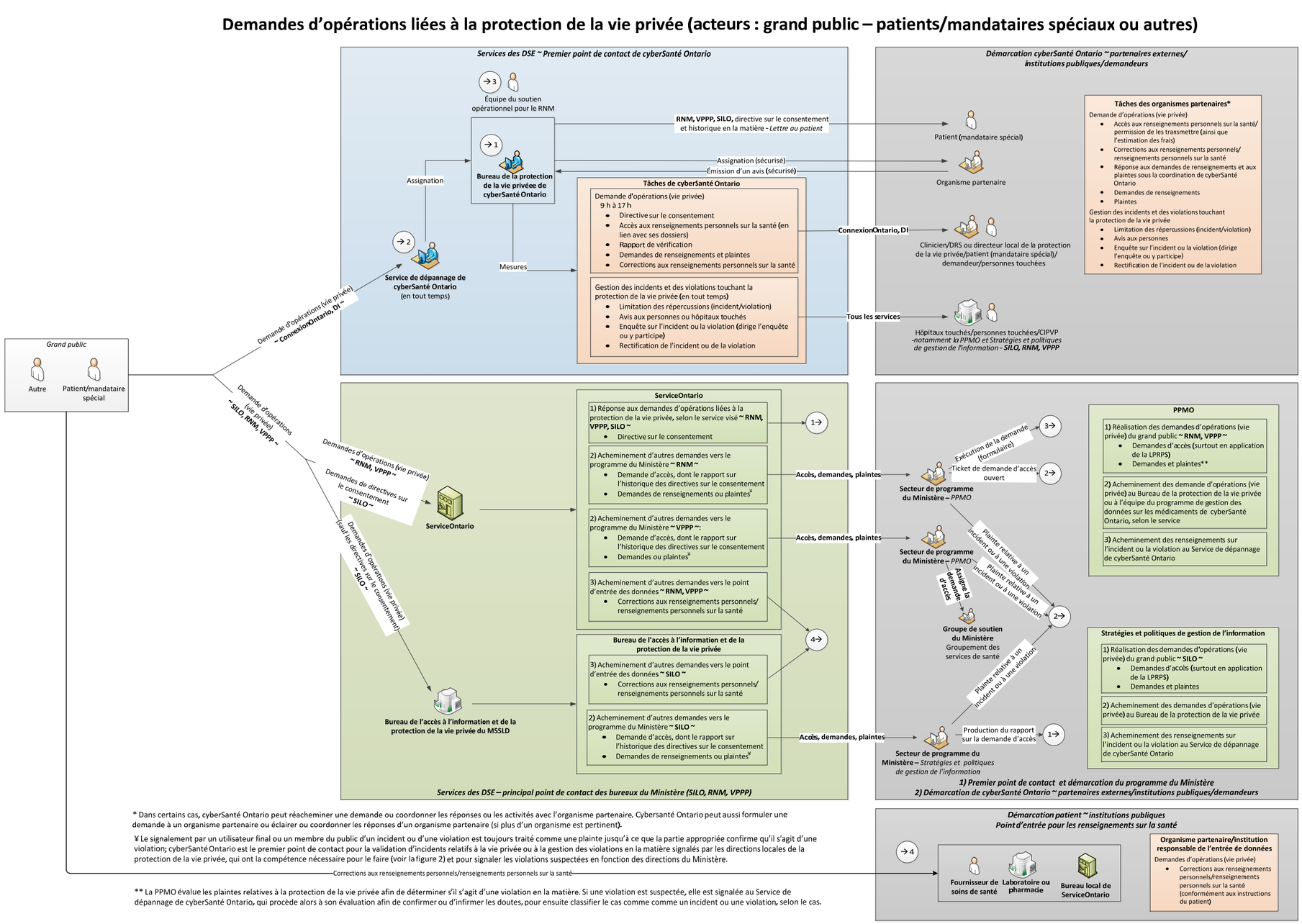


Figure 2 - Organigramme de soutien pour la gestion des demandes d'opérations liées à la protection de la vie privée et des incidents et des violations touchant la protection de la vie privée – Partie en cause : grand public

Le schéma suivant montre les interactions de haut niveau pour les demandes d'opérations liées à la protection de la vie privée et les incidents et les violations touchant la protection de la vie privée entre cyberSanté Ontario et l'organisme partenaire dans les cas où l'agent de protection de la vie privée est le déclencheur.

Demandes d'opérations liées à la protection de la vie privée – plaintes, directives sur le consentement, demandes de renseignements – et gestion des violations touchant la protection de la vie privée (acteur : directeur local de la protection de la vie privée)

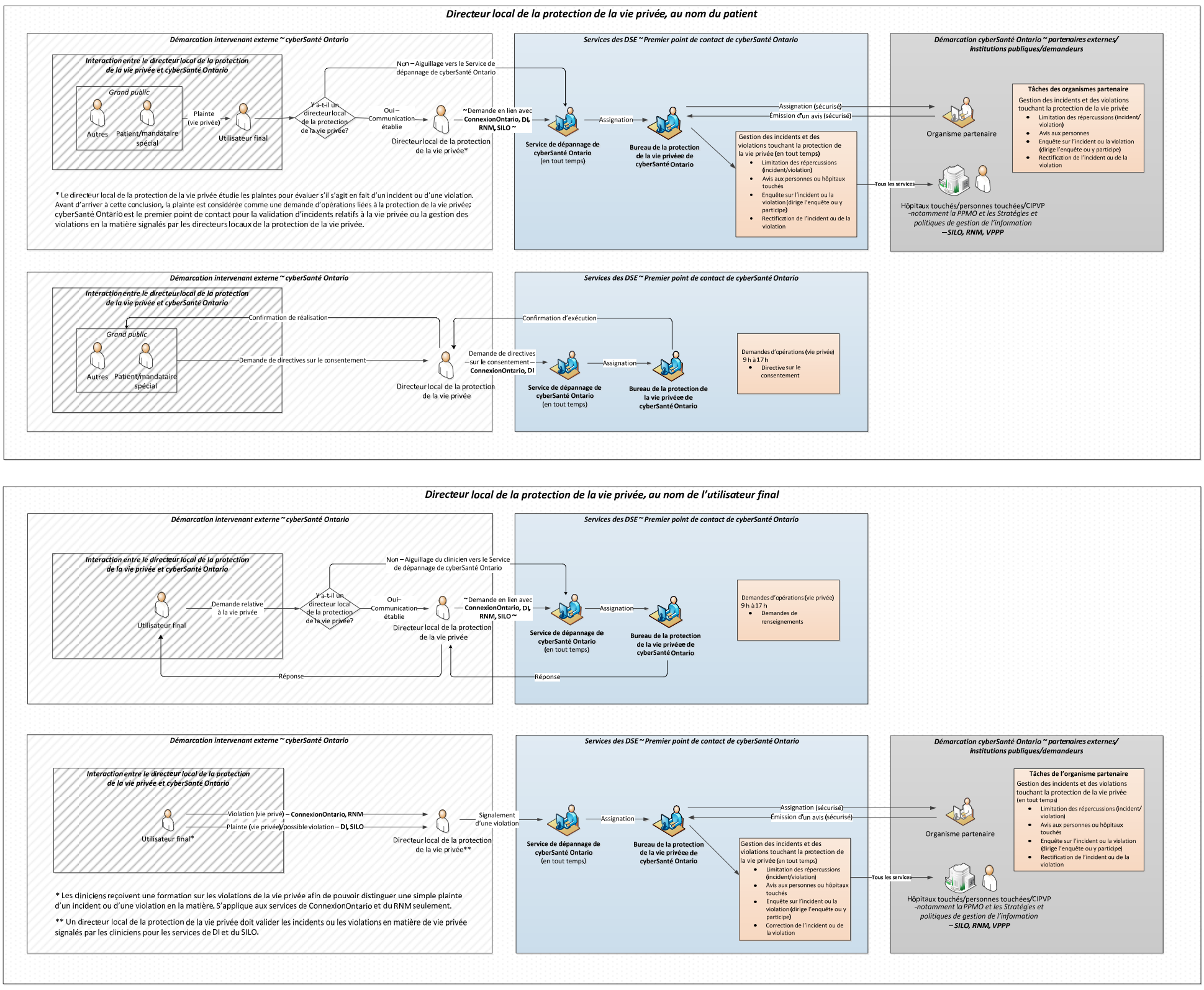
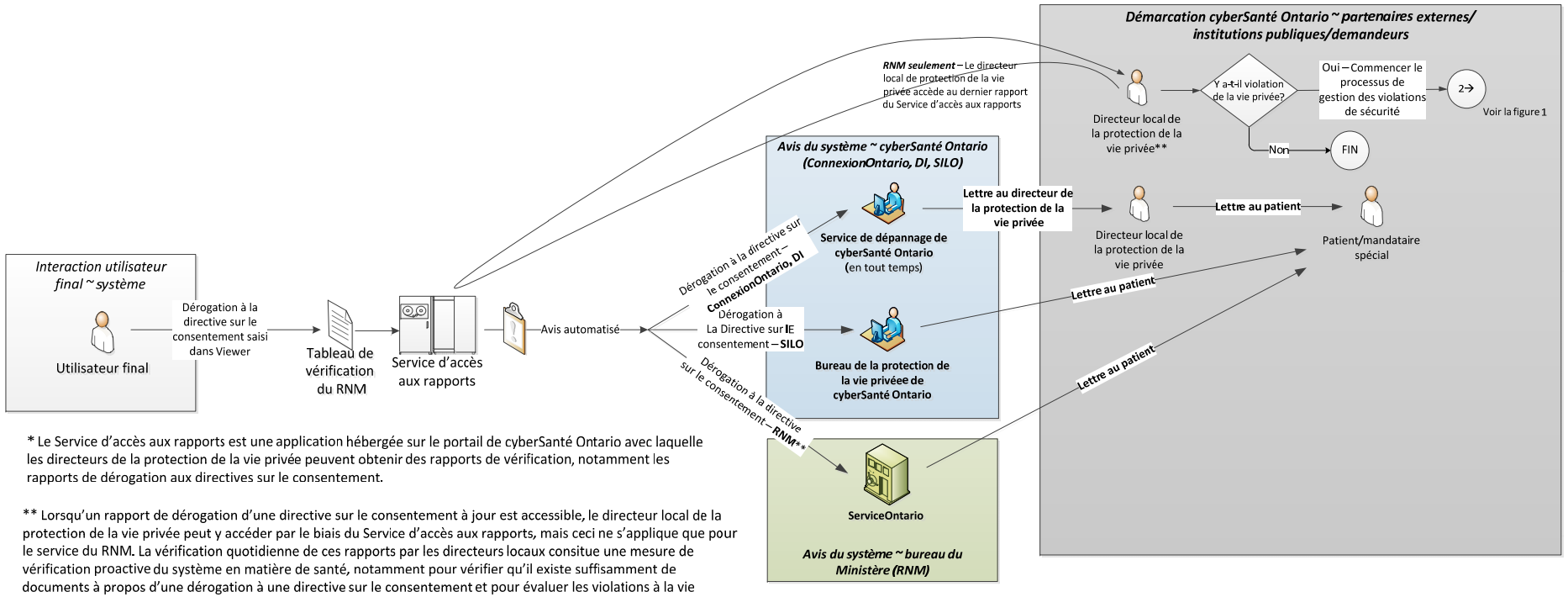


Figure 3 - Organigramme de soutien pour la gestion des demandes d'opérations liées à la protection de la vie privée et des incidents et des violations touchant la protection de la vie privée – Partie en cause : agent de protection de la vie privée

Le schéma suivant montre les interactions de haut niveau associées à la fonction de dérogation pour les directives en matière de consentement et à l'accès aux rapports de dérogation pour les directives en matière de consentement, lorsque l'utilisateur final et l'agent de protection de la vie privée local sont à l'origine des interactions. Le processus de GVS peut être mis en œuvre par un agent de protection de la vie privée local à la suite d'un examen des rapports sur les dérogations pour les directions en matière de consentement après y avoir accédé par l'intermédiaire de l'application du SIE.

Opérations liées à la protection de la vie privée – Rapport de dérogation à une directive sur le consentement (acteurs : utilisateurs finaux et directeurs locaux de la protection de la vie privée)



* Le Service d'accès aux rapports est une application hébergée sur le portail de cyberSanté Ontario avec laquelle les directeurs de la protection de la vie privée peuvent obtenir des rapports de vérification, notamment les rapports de dérogation aux directives sur le consentement.

** Lorsqu'un rapport de dérogation d'une directive sur le consentement à jour est accessible, le directeur local de la protection de la vie privée peut y accéder par le biais du Service d'accès aux rapports, mais ceci ne s'applique que pour le service du RNM. La vérification quotidienne de ces rapports par les directeurs locaux consitue une mesure de vérification proactive du système en matière de santé, notamment pour vérifier qu'il existe suffisamment de documents à propos d'une dérogation à une directive sur le consentement et pour évaluer les violations à la vie privée. L'examen d'un rapport de dérogation peut mener à la détermination d'une violation de la vie privée, auquel cas le directeur local de la protection de la vie privée suivra le scénario habituel en cas d'incident ou de violation de la vie privée, et communiquera avec le Service de dépannage de cyberSanté Ontario.

Figure 4 - Avis de dérogation et rapports sur les dérogations pour les directives en matière de consentement – Partie en cause : Utilisateur final et agent de protection de la vie privée local

2.7 Points de contact en cas de réacheminement

Points de contact en cas de réacheminement Les points de contact en cas de réacheminement au sein de cyberSanté Ontario et de l'organisme partenaire sont utilisés pour remédier rapidement aux défaillances de la chaîne de soutien et lorsque le respect de l'ENS de cyberSanté Ontario pour un ticket d'incident ou de demande de service semble menacé. La procédure de réacheminement peut être appliquée dans les cas suivants :

- Désaccord au sujet d'une décision liée au service prise conjointement par le client et cyberSanté Ontario;
- Inquiétude au sujet du déploiement d'un service;
- Inquiétude au sujet du rendement d'un service;
- Inquiétude au sujet de la gestion d'un incident ou d'une demande de service.

Dans le cas d'une procédure de réacheminement, l'organisme partenaire doit appeler le Service de dépannage de cyberSanté Ontario qui communiquera à son tour avec le chef de service ou le responsable du déploiement affecté au service de cyberSanté Ontario. Le chef de service ou le responsable du déploiement, ainsi que le gestionnaire des programmes clients (s'il est affecté au service de cyberSanté Ontario), prendront ensuite des mesures au nom de l'organisme partenaire pour accélérer la résolution du problème.

2.7.1 Point de contact de cyberSanté Ontario en cas de réacheminement

Service de dépannage de cyberSanté Ontario

Téléphone : 1 866 250-1554.

Adresse électronique : servicedesk@ehealthontario.on.ca

2.7.2 Point de contact de l'organisme partenaire en cas de réacheminement

Le point de contact de l'organisme partenaire en cas de réacheminement dans le cadre du processus de gestion des incidents de cyberSanté Ontario doit être établi durant la phase de projet du service et comprendre les éléments suivants : rôle/titre, nom, adresse de courriel, numéro de téléphone mobile ou cellulaire ou téléavertisseur. Toutes modifications des coordonnées durant la durée de vie du service doivent être signalées au Service de dépannage de cyberSanté Ontario, pour être ensuite transmises sous forme de demande de changement au chef de service de cyberSanté Ontario désigné.

3.0 Gestion des problèmes

3.1 Aperçu et introduction

Le processus de gestion des problèmes de cyberSanté Ontario suit la pratique exemplaire ITIL (Information Technology Infrastructure Library) V3. La gestion des problèmes au sein de cyberSanté Ontario est axée sur l'environnement de production. Un problème est un incident pour lequel on n'a pas déterminé de cause fondamentale au terme du règlement du ticket, ou une tendance indésirable observée au sein d'un élément de configuration, d'un site ou d'un service de cyberSanté Ontario. Un problème peut être détecté dans le cadre du processus de gestion des incidents ou de gestion des changements de cyberSanté Ontario, et peut faire intervenir n'importe quel niveau de priorité d'incident.

Le processus de gestion des problèmes permet de gérer le cycle de vie des problèmes. Ce processus vise à éviter les problèmes et les incidents qui en découlent, à éliminer les incidents récurrents et à réduire au minimum l'impact des incidents qui ne peuvent être évités.

Dans le cadre du processus de gestion des problèmes, on doit déterminer la cause fondamentale d'un problème et le moyen d'y remédier en appliquant des procédures de contrôle appropriées, comme la gestion des changements et la gestion des versions. Le processus vise à déterminer et recueillir des renseignements sur les erreurs connues et les solutions de rechange pouvant être utilisées par les équipes de soutien durant la gestion de l'incident en vue de rétablir rapidement le service. Il vise également à remédier aux erreurs connues.

La gestion proactive des problèmes consiste à repérer les tendances pouvant entraîner des problèmes afin de prévenir les incidents. Pour y parvenir, il faut mener une analyse des tendances à partir des données, notamment des dossiers d'incidents.

3.2 Processus d'intégration

3.2.1 Processus de gestion des problèmes

L'organigramme suivant présente le processus de gestion des problèmes de haut niveau au sein de cyberSanté Ontario.

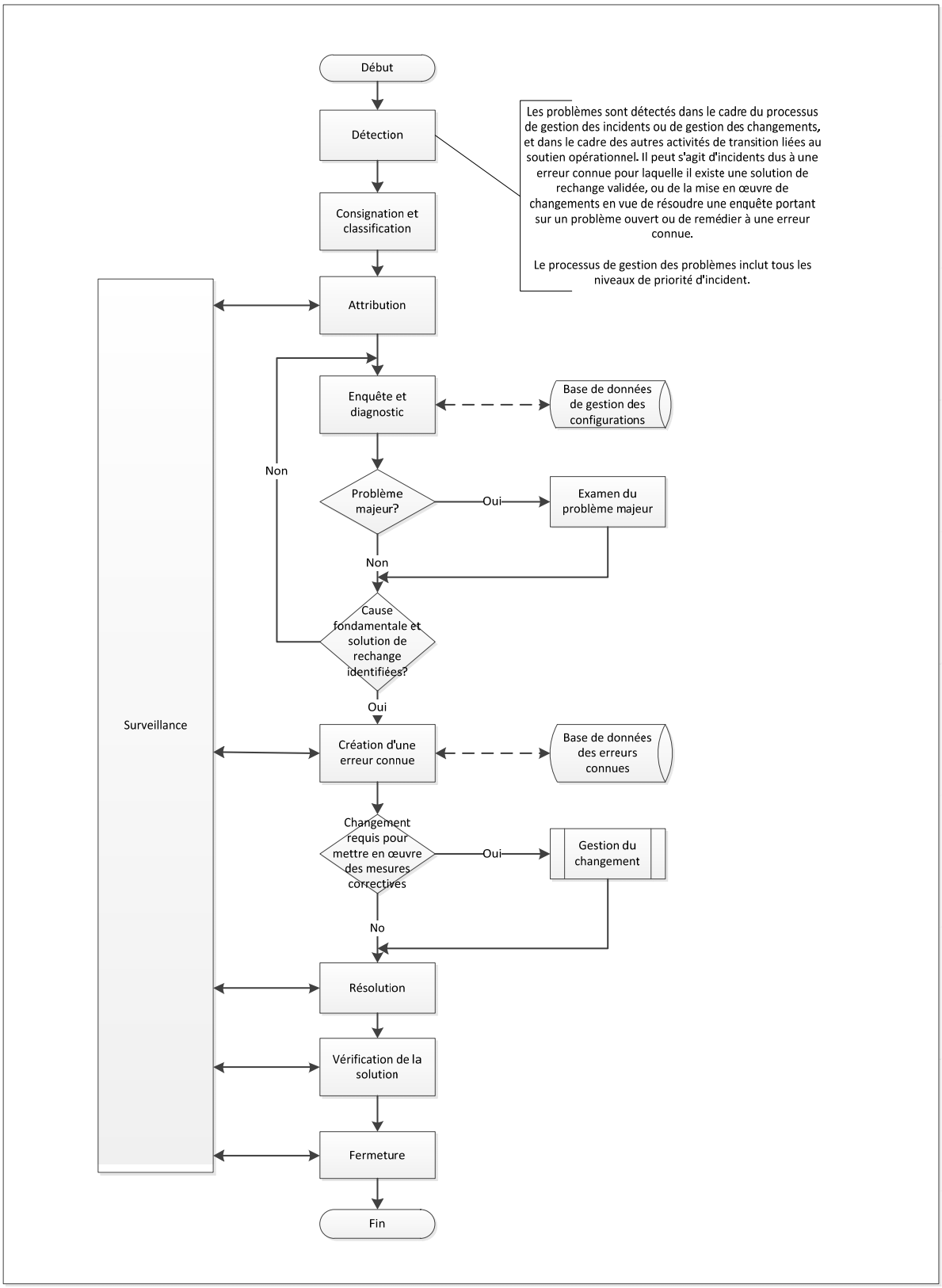


Figure 5 - Processus de gestion des problèmes

3.2.2 Coordination entre les rôles de PCU au sein de deux organismes

Les enquêtes et les demandes liées à des problèmes doivent être placées sous la coordination d'un point de contact unique (PCU) au sein de cyberSanté Ontario et de l'organisme partenaire, respectivement le chef de service de cyberSanté Ontario et le chef de service (ou le rôle équivalent) de l'organisme partenaire. À partir de ce PCU, les mesures et les activités entreprises passent ensuite par les processus internes de chaque organisme. De la même façon, les communications dans le cadre de la création d'un nouveau dossier de problème ou d'un autre point de l'enquête doivent continuer de passer par les PCU.

Une fois établies, les coordonnées des PCU doivent être communiquées au chef de service de cyberSanté Ontario affecté au service en question.

3.2.3 Activités et points de contact

Le tableau suivant présente les principales activités et tâches de haut niveau que doivent réaliser le point de contact de l'organisme partenaire et celui de cyberSanté Ontario dans le cadre du processus de gestion des problèmes.

Activité	cyberSanté Ontario	Partnering Organization
Détection	➢ Examiner les incidents ➢ Analyser les tendances des incidents (gestion proactive des problèmes)	➢ Examiner les incidents ➢ Analyser les tendances des incidents (gestion proactive des problèmes)
Consignation et classification	➢ Créer un nouveau dossier de problème ➢ Associer les incidents au dossier du problème ➢ Informer l'organisme partenaire d'un problème potentiel ➢ Recevoir un avis signalant un problème potentiel de la part de l'organisme partenaire ➢ Consigner le dossier du problème dans le système de gestion des problèmes de cyberSanté Ontario ➢ Classer le problème dans une catégorie et établir son impact, son degré d'urgence et son niveau de priorité	➢ Créer un nouveau dossier de problème ➢ Associer les incidents au dossier du problème ➢ Informer cyberSanté Ontario d'un problème potentiel ➢ Recevoir un avis signalant un problème potentiel de la part de cyberSanté Ontario ➢ Consigner le dossier du problème dans le système interne de gestion des problèmes ➢ Classer le problème dans une catégorie et établir son impact, son degré d'urgence et son niveau de priorité
Attribution	➢ Attribuer le problème à l'analyste approprié ➢ Assurer le suivi du problème	➢ Attribuer le problème à l'analyste approprié ➢ Assurer le suivi du problème

Activité	cyberSanté Ontario	Partnering Organization
Enquête et diagnostic	➢ Mener une enquête sur le problème ➢ Diagnostiquer le problème ➢ Consigner les résultats de l'enquête ➢ Participer à l'enquête et au diagnostic du problème, le cas échéant ➢ Informer l'organisme partenaire du diagnostic du problème provenant de cyberSanté Ontario ➢ Préciser l'impact opérationnel du problème pour établir son niveau de priorité ➢ Suivre l'enquête et le diagnostic du problème	➢ Mener une enquête sur le problème ➢ Diagnostiquer le problème ➢ Consigner les résultats de l'enquête ➢ Participer à l'enquête et au diagnostic du problème, le cas échéant ➢ Informer cyberSanté Ontario du diagnostic du problème provenant de l'organisme partenaire ➢ Préciser l'impact opérationnel du problème pour établir son niveau de priorité ➢ Suivre l'enquête et le diagnostic du problème
Résolution	➢ Résoudre le problème	➢ Résoudre le problème
Vérification de la solution	➢ Vérifier que le problème est résolu ➢ Informer l'organisme partenaire que le problème est résolu	➢ Vérifier que le problème est résolu ➢ Informer cyberSanté Ontario que le problème est résolu
Fermeture du problème	➢ Examiner le problème et déterminer s'il faut poursuivre l'enquête ➢ Informer l'organisme partenaire de la fermeture du problème ➢ Recevoir un avis lorsque l'organisme partenaire ferme le problème ➢ Accuser réception de l'avis de fermeture du problème ➢ Fermer le dossier du problème dans le système de suivi de cyberSanté Ontario en mettant l'information à jour	➢ Examiner le problème et déterminer s'il faut poursuivre l'enquête ➢ Informer cyberSanté Ontario de la fermeture du problème ➢ Recevoir un avis lorsque cyberSanté Ontario ferme le problème ➢ Accuser réception de l'avis de fermeture du problème ➢ Fermer le dossier du problème dans le système de suivi de l'organisme partenaire en mettant l'information à jour

Table 1 - Principales activités et tâches de gestion des problèmes de haut niveau

3.3 Définition d'un problème – Renseignements à inclure

Tous les tickets de problème ouverts par cyberSanté Ontario ou par l'organisme partenaire doivent contenir les renseignements suivants :

a. Nom et rôle de la personne qui soumet le problème;
b. Date de soumission;
c. Description du problème et de son impact;
d. Incidents et éléments connexes;
e. Solutions de rechange et plans d'action (le cas échéant);
f. Recommandations au sujet du groupe à affecter à l'enquête.

3.4 Éléments déclencheurs d'un problème

Le dossier d'un problème peut être ouvert par l'organisme partenaire ou par cyberSanté Ontario. Le processus de gestion des problèmes est déclenché dans les cas suivants :

- Apparition d'un incident majeur dont la cause est inconnue au terme de la résolution;

- Apparition d'une tendance (répétition d'incidents présentant des symptômes communs) au sein d'un élément de configuration, d'un environnement inférieur, d'un site ou d'un service de cyberSanté Ontario (gestion proactive des problèmes).

3.5 Examen d'un problème

Un examen des dossiers des problèmes ouverts est réalisé lors de la réunion qui a lieu tous les mois entre cyberSanté Ontario et l'organisme partenaire. Une réunion entre les gestionnaires des problèmes peut être organisée par l'intermédiaire du chef de service (ou le rôle équivalent) de l'organisme partenaire et du chef de service de cyberSanté Ontario affecté au service en question.

L'organisme partenaire transmet une liste des dossiers des problèmes à cyberSanté Ontario avant la réunion mensuelle conjointe. De la même façon, cyberSanté Ontario remet à l'organisme partenaire une liste des problèmes nuisant à son service. Chaque organisme doit présenter les éléments qui relèvent de sa responsabilité en matière d'opérations techniques et de maintenance (voir la section d'introduction) lors des réunions d'examen et d'enquête sur les problèmes. L'organisme partenaire et cyberSanté Ontario doivent se communiquer des rapports, et cyberSanté Ontario dirige l'examen et l'enquête sur les problèmes qui nuisent à son service.

En dehors des réunions d'examen des problèmes, il est possible d'obtenir des mises à jour ad hoc sur l'avancée de l'enquête en en faisant la demande auprès du chef de service de cyberSanté Ontario désigné.

3.5.1 Réunion d'examen : points à l'ordre du jour

Les points suivants constituent l'ordre du jour de la réunion d'examen des problèmes :

a. Examiner les dossiers des problèmes ouverts ou des erreurs connues, confirmer la validité, la catégorie, le niveau de priorité et l'affectation;
b. Discuter de chaque dossier de problème ouvert ou d'erreur connue, examiner les dernières mises à jour de la liste des problèmes, les progrès effectués et la marche à suivre pour accélérer la résolution;
c. Examiner les problèmes résolus pour confirmer que la cause fondamentale a bien été déterminée et que la solution de rechange a permis de résoudre le problème;
d. Examiner les erreurs connues résolues pour confirmer que la solution permanente qui a été mise en œuvre a permis de résoudre le problème;
e. Valider la fermeture de tous les dossiers de problèmes achevés.

4.0 Gestion des changements

Cette section présente les interactions entre un organisme partenaire et cyberSanté Ontario dans le cadre de la gestion des changements concernant tout élément qui permet la prestation d'un service de cyberSanté Ontario. Elle décrit la marche à suivre pour mettre en œuvre un changement lié à un élément technique qui intervient dans la prestation des services de cyberSanté Ontario, selon le domaine de responsabilité technique respectif de chaque organisme.

Le processus de gestion des changements vise à réduire au minimum le risque encouru par l'environnement de TI en veillant à ce que des procédures claires et normalisées soient mises en place pour permettre de gérer tous les changements de manière efficace. Pour modifier un élément intervenant dans la prestation d'un service de cyberSanté Ontario actif, il faut présenter une demande de changement (DC). Il s'agit d'un dossier contenant tous les renseignements au sujet du changement demandé : dates et heures de début et de fin, tâches à effectuer, procédures de sortie et ressources affectées, conformément au processus de gestion des changements de cyberSanté Ontario.

Cette section s'adresse à la fois à l'équipe responsable de la gestion des changements de cyberSanté Ontario et à celle de l'organisme partenaire. Elle s'adresse également aux employés du service à la clientèle et de la prestation de services de cyberSanté Ontario qui sont chargés de répondre aux demandes d'information des partenaires au sujet des changements. L'organisme partenaire est chargé de faciliter l'utilisation des points de contact de gestion des changements (indiqués dans le présent document) auprès de son équipe de gestion des changements et des fournisseurs ou prestataires de services tiers avec qui il entretient un rapport direct.

4.1 Critères de gestion des changements

Les changements introduits par cyberSanté Ontario ou par l'organisme partenaire qui ont des conséquences sur le service de cyberSanté Ontario doivent être soumis au comité d'approbation des changements (CAC). Tous les ajouts, les modifications et les suppressions de tout élément qui fait partie du service de cyberSanté Ontario constituent un changement. Il peut s'agir de services de TI, d'éléments de configuration, de processus, de documents, etc.

cyberSanté Ontario requiert un préavis de sept jours ouvrables pour les changements apportés à des éléments détenus ou gérés par l'organisme partenaire.

cyberSanté Ontario remet un préavis de cinq jours ouvrables aux organismes partenaires pour les changements apportés à un service de cyberSanté Ontario qui pourraient avoir un impact sur les utilisateurs finaux ou sur les éléments détenus ou gérés par l'organisme partenaire.

Pour présenter une demande de changement (DC) d'un service actif de cyberSanté Ontario, l'organisme partenaire doit communiquer avec le Service de dépannage de cyberSanté Ontario. Le Service de dépannage de cyberSanté Ontario attribue ensuite la demande de changement au responsable du déploiement ou au chef de service affecté au service de cyberSanté Ontario. Ce dernier, avec l'aide de l'organisme partenaire, consigne la DC soumise par l'organisme partenaire et est responsable du changement lors des réunions du CAC de cyberSanté Ontario.

L'organisme partenaire désigne ensuite un représentant qui jouera le rôle du point de contact unique (PCU) avec lequel le responsable du déploiement ou le chef de service de cyberSanté Ontario collaborera après la

création d'un ticket par l'intermédiaire du Service de dépannage de cyberSanté Ontario. Le représentant de l'organisme partenaire doit obtenir les approbations et les autorisations de changements nécessaires au sein de l'organisme partenaire avant de présenter la demande de changement.

Les changements peuvent notamment porter sur :

- l'infrastructure (portail et services Web);
- les applications;
- les bases de données;
- les procédures et processus de fonctionnement normalisés.

4.2 Matrice de changement

Le tableau ci-dessous présente les différents types de changements et leur définition. Les organismes partenaires doivent respecter ces définitions pour pouvoir utiliser et déclencher le processus de gestion des changements de cyberSanté Ontario.

Cette terminologie est utilisée dans le reste de la section.

Type de changement au sein de cyberSanté Ontario	Définition
Changement standard	Il s'agit d'un changement récurrent, peu risqué et à faible impact qui suit un chemin prédéfini et dont les approbations ont été obtenues avant la mise en œuvre. Ce type de changement n'a pas besoin d'être examiné par le CAC.
Changement normal	Il s'agit d'un changement qui doit suivre l'ensemble du processus de gestion des changements et dont l'approbation finale doit être accordée par le CAC. Le processus de gestion des changements est composé des étapes suivantes : évaluation, autorisation, approbation du CAC et planification du changement avant la mise en œuvre.
Changement de réparation d'urgence	Il s'agit d'un changement répondant rapidement à une interruption critique ou supprimant un risque élevé d'interruption. Il doit être mis en œuvre le plus rapidement possible. Ce type de changement intervient à la suite d'un incident et doit, en principe, faire l'objet d'une procédure d'évaluation ou d'autorisation accélérée pour réduire au minimum les risques qui peuvent nuire à sa mise en œuvre.
Changement opérationnel urgent	Il s'agit d'un changement qui répond rapidement à un besoin urgent du client et qui, s'il n'est pas mis en œuvre, portera atteinte à sa réputation. Ce type de changement doit, en principe, faire l'objet d'une procédure d'évaluation ou d'autorisation accélérée pour réduire au minimum les risques qui peuvent nuire à sa mise en œuvre.

Table 2 - Définition des types de changements

4.3 Calendrier du CAC et date limite de soumission des changements normaux

Le tableau ci-dessous indique le calendrier du comité d'approbation des changements (CAC) de cyberSanté Ontario pour l'examen et l'approbation des changements normaux. L'organisme partenaire doit soumettre une DC au chef de service désigné au plus tard le jeudi à 12 h. La DC est ensuite examinée par cyberSanté Ontario et soumis pour une inscription à l'ordre du jour de la réunion du CAC qui a lieu le mercredi suivant.

Organisme	Date et heure	Date limite de soumission
CAC* de cyberSanté Ontario	Le mercredi de 10 h à 12 h	Le jeudi à 12 h

Toutes les demandes de changement (DC) soumises par un organisme partenaire pour être approuvées par le CAC de cyberSanté Ontario doivent avoir été autorisées par les responsables désignés de l'organisme partenaire. Il incombe à la partie ayant soumis la DC d'obtenir toutes les autorisations nécessaires, et cyberSanté Ontario part du principe que ces mesures ont été prises lorsqu'il reçoit la DC.

4.4 Participation au CAC

Le chef de service ou le responsable du déploiement de cyberSanté Ontario est chargé de présenter les changements de l'organisme partenaire au CAC de cyberSanté Ontario. Les représentants de l'organisme partenaire ne participent pas au CAC de cyberSanté Ontario.

cyberSanté Ontario ne participe pas aux processus d'approbation des changements des organismes partenaires.

4.5 Fenêtre d'entretien

Une fenêtre d'entretien est une période prédéfinie au cours de laquelle les changements à apporter aux éléments qui soutiennent un service de cyberSanté Ontario doivent être mis en œuvre en réduisant au minimum les répercussions sur les éléments interdépendants et les utilisateurs finaux.

Cette fenêtre d'entretien permet de planifier correctement les activités de changement, de déterminer les répercussions, d'évaluer les conflits et d'obtenir les ressources adaptées. Puisqu'il s'agit d'un moment de faible activité pour la plupart des systèmes et des services, c'est la période acceptable pour effectuer de l'entretien et planifier des changements en réduisant au minimum les répercussions sur les éléments interdépendants et les utilisateurs finaux.

La fenêtre d'entretien régulière de cyberSanté Ontario est la suivante :

Organisme	Fenêtre d'entretien régulière
cyberSanté Ontario	Le dimanche de minuit à 6 h

Un changement peut être planifié en dehors de la fenêtre d'entretien régulière afin de répondre aux besoins opérationnels de l'organisme partenaire. Il doit avoir été reçu avant l'approbation du propriétaire du service de cyberSanté Ontario.

cyberSanté Ontario informe les organismes partenaires et les utilisateurs finaux concernés par l'entremise du Service de dépannage de cyberSanté Ontario si un changement nuit à l'accessibilité et à la disponibilité des services de cyberSanté Ontario en leur transmettant un avis de changement. Un avis de changement est également appelé « arrêt prévu » au sein de cyberSanté Ontario.

4.6 Renseignements à fournir sur le changement

Dans toutes ses demandes de changement (DC), l'organisme partenaire doit indiquer :

- la raison du changement;
- une description du changement;
- si un avis est requis;
- s'il existe un processus de reprise après catastrophe;
- s'il existe des documents tels que des manuels de formation ou des livres de version;
- si le changement a été éprouvé dans le laboratoire d'infrastructure;
- le niveau de risque;
- l'impact;
- le degré d'urgence;
- un résumé;
- si le changement aura un impact sur les utilisateurs (le cas échéant, indiquer l'impact dans le champ prévu à cet effet);
- si un arrêt est requis (le cas échéant, donner les dates de début et de fin);
- la liste des zones touchées;
- les dates de début et de fin demandées;
- la catégorie du produit (champ « niveau 1 »);
- l'élément de configuration du service opérationnel ou du service des TI (et ses composants, le cas échéant) dans le champ prévu à cet effet;
- qui est responsable de mettre en œuvre le changement d'infrastructure.

Toutes les DC soumises par l'organisme partenaire doivent être accompagnées d'un plan de mise en œuvre reposant sur le modèle de cyberSanté Ontario. L'organisme partenaire doit fournir les renseignements nécessaires au chef de service ou au responsable du déploiement de cyberSanté Ontario qui remplit le modèle au nom de l'organisme.

4.7 Gel des changements

Le gel des changements s'applique aux changements normaux au sein des environnements de TI actifs de cyberSanté Ontario. On établit un gel des changements pour réduire au minimum le risque encouru par les environnements. Ce gel peut être mis en œuvre par cyberSanté Ontario pour soutenir le déploiement de grands projets, les exercices de reprise après catastrophe ou les événements majeurs qui peuvent aggraver les retombées du changement sur la santé publique (p. ex., pandémie déclarée).

Si cyberSanté Ontario prévoit d'instaurer une période de gel des changements, il en informe l'organisme partenaire au moins 30 jours civils avant le début du gel. Pour tout gel des changements opéré par cyberSanté Ontario, une procédure de dérogation sera remise à l'organisme partenaire, ainsi qu'une déclaration de gel des changements.

Si un organisme partenaire qui détient ou qui gère des éléments participant au bon fonctionnement d'un service de cyberSanté Ontario prévoit d'instaurer une période de gel des changements, il doit en informer cyberSanté Ontario, par l'intermédiaire de son Service de dépannage de cyberSanté Ontario, au moins 30 jours civils avant le début du gel.

4.8 Réacheminement des demandes de changement

Tous les problèmes rencontrés durant la mise en œuvre d'une demande de changement sont traités comme un incident de service. Ils sont donc pris en charge par le processus de gestion des incidents de cyberSanté Ontario. Pour en savoir plus, consultez la section ci-dessus qui porte sur la gestion des incidents.

4.9 Délais d'exécution des changements

cyberSanté Ontario analyse l'impact opérationnel du changement dans le cadre d'un premier examen et des évaluations menées par le CAC.

Le tableau ci-dessous indique les délais requis par cyberSanté Ontario pour introduire un changement, une fois la DC soumise auprès du Service de dépannage de cyberSanté Ontario et examinée par le responsable du déploiement ou le chef de service désigné, et selon l'incidence perçue du changement.

Impact du changement	Description	Mise en œuvre du changement Délai d'exécution requis
1-Considérable/généralisé	Changement à impact élevé entraînant des répercussions opérationnelles majeures ou un grand retentissement pour les utilisateurs. • Résultats d'un changement effectué sur le plan des opérations ou de l'infrastructure (p. ex., consolidation de deux serveurs d'applications entraînant l'absence totale de disponibilité pour les utilisateurs). • Changements de longue haleine ou pour lesquels les procédures de sortie sont longues ou inexistantes (p. ex., la mise à jour des versions de la base de données sur le serveur d'applications, le lancement d'une application majeure).	10 jours ouvrables
2-Important/grand	Changement à impact moyen à élevé pouvant entraîner des répercussions opérationnelles majeures ou un grand retentissement pour les utilisateurs. La principale différence entre le changement à impact élevé et le changement à impact moyen à élevé est la suivante : les changements à impact moyen à élevé peuvent être assortis de procédures de sortie, mais ces changements peuvent être supprimés avec ou sans procédure.	10 jours ouvrables
3-Modéré/limité	Changements à impact moyen pouvant entraîner des répercussions minimes sur l'organisme. Les procédures de sortie sont relativement simples et efficaces.	5 jours ouvrables
4-Mineur/localisé	Changements à faible impact : il s'agit des changements quotidiens courants qui touchent des clients individuellement ou de petits groupes. Ils sont classés et rationalisés, mais ils font tout de même l'objet d'un suivi dans le cadre de l'évaluation des résultats des changements. Même si les demandes de service peuvent être considérées comme des changements à faible impact, les groupes des opérations de TI doivent les maintenir séparément afin de mieux gérer l'utilisation des ressources.	5 jours ouvrables

Table 3 - Répercussion sur les services et délais d'exécution des changements correspondants

4.10 Calendrier des demandes de changement

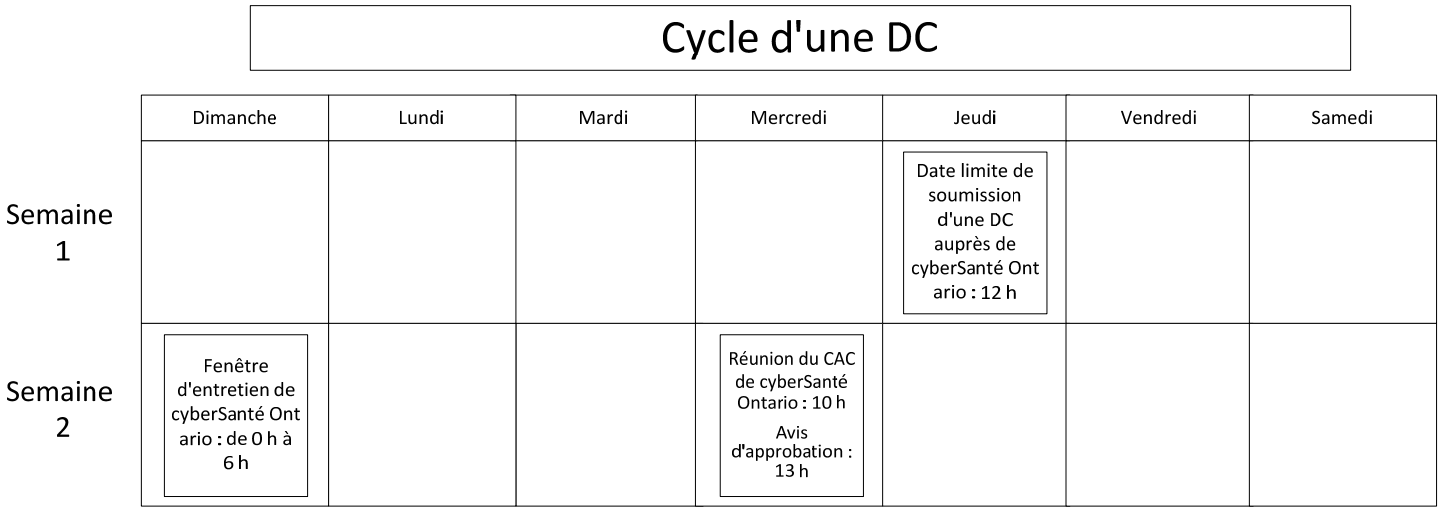


Figure 6 - Soumission des demandes de changement et cycle d'approbation

4.11 Traitement des demandes de changements normaux et urgents

Le schéma ci-dessous montre le processus de traitement des demandes de changements normaux et urgents entre cyberSanté Ontario et l'organisme partenaire pour le service de cyberSanté Ontario.

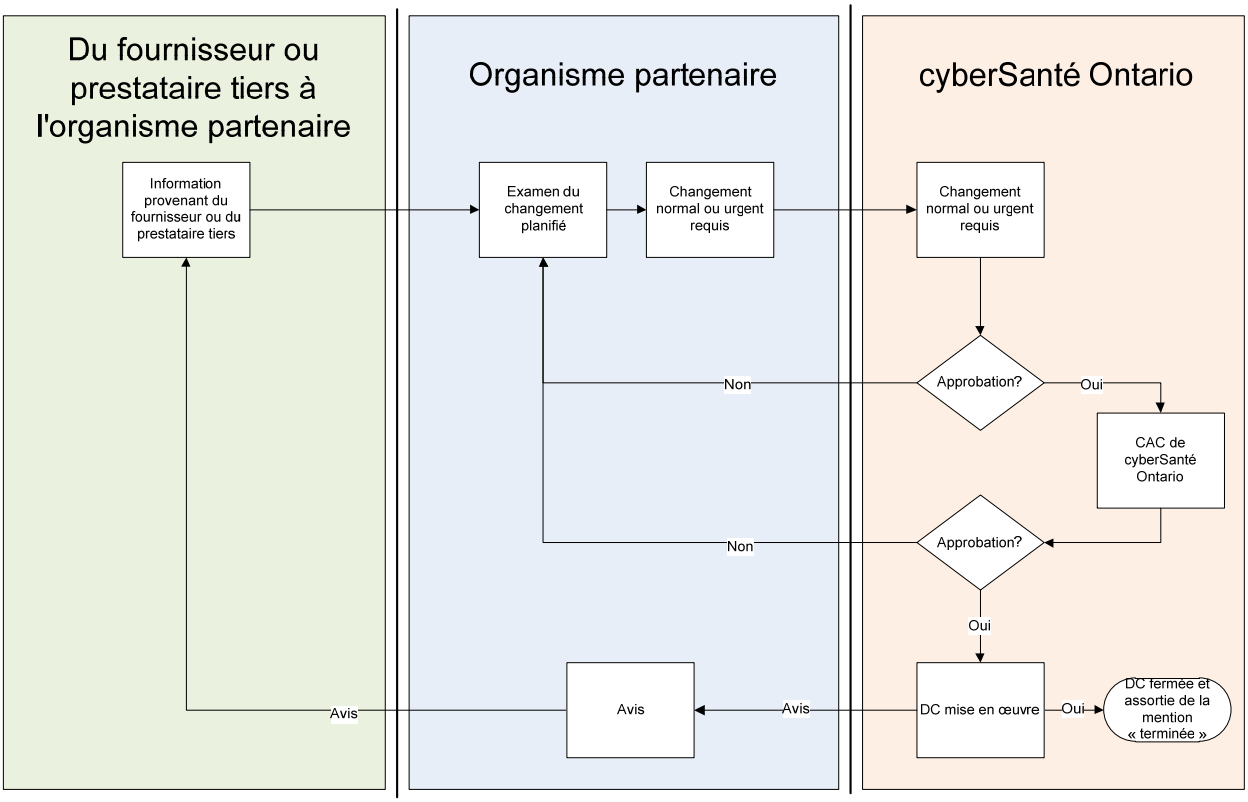


Figure 7 - Organigramme de soutien lié aux demandes de changements normaux et urgents

4.12 Types de changements

La section suivante présente le processus détaillé suivi par chaque type de changement lié à un service de cyberSanté Ontario, selon l'organisme à l'origine de la demande de changement et l'organisme responsable de sa mise en œuvre.

4.12.1 Changement normal

4.12.1.1 Déclenché par l'organisme partenaire et mis en œuvre par cyberSanté Ontario

Déclencheur	Organisme partenaire	**Exécutant**	cyberSanté Ontario
Situation	Changement normal ou planifié avec impact opérationnel On part du principe que le changement a déjà été approuvé par le responsable des changements internes de l'organisme partenaire.		
Date limite de soumission	Le jeudi à 12 h pour que le changement soit mis en œuvre après la réunion du CAC de cyberSanté Ontario qui a lieu le mercredi suivant.		
Étapes	1. L'organisme partenaire ouvre une demande de service auprès du Service de dépannage de cyberSanté Ontario. 2. L'équipe de cyberSanté Ontario désignée, en collaboration avec le représentant de l'organisme partenaire, crée la DC dans l'outil de GSTI de cyberSanté Ontario avant la date et l'heure limites de soumission. 3. Le représentant de l'organisme partenaire reçoit un avis par courriel de la part du chef de service ou du responsable du déploiement de cyberSanté Ontario désigné, demandant l'approbation de l'organisme partenaire. 4. Le chef de service ou le responsable du déploiement de cyberSanté Ontario et le représentant de l'organisme partenaire examinent la liste des impacts du changement, qui sera ensuite soumise à l'approbation du CAC de cyberSanté Ontario. 5. Le chef de service ou le responsable du déploiement de cyberSanté Ontario obtient l'approbation de la DC et en informe l'organisme partenaire. ➢ *Remarque : Pour tout rejet d'une DC de la part du CAC de cyberSanté Ontario, le chef de service ou le responsable du déploiement de cyberSanté Ontario doit en indiquer les raisons au représentant de l'organisme partenaire.* 6. cyberSanté Ontario met le changement en œuvre. 7. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe le représentant de l'organisme partenaire de l'état de la mise en œuvre (p. ex., réussie, annulée, ratée). 8. cyberSanté Ontario indique que la DC est « résolue ».		

4.12.1.2 Déclenché par cyberSanté Ontario et mis en œuvre par cyberSanté Ontario

Déclencheur	cyberSanté Ontario	**Exécutant**	cyberSanté Ontario
Situation	Changement normal ou planifié avec impact ou risque d'impact sur le service, l'infrastructure ou les processus de cyberSanté Ontario		
Date limite de soumission	Le jeudi à 12 h pour que le changement soit mis en œuvre après la réunion du CAC de cyberSanté Ontario qui a lieu le mercredi suivant.		
Étapes	1. L'équipe de cyberSanté Ontario crée une DC. 2. Le chef de service ou le responsable du déploiement de cyberSanté Ontario fournit des renseignements détaillés sur le changement au représentant de l'organisme partenaire avant la date et l'heure limites de soumission. 3. L'équipe de cyberSanté Ontario responsable du changement obtient l'approbation interne du CAC. 4. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe le représentant de l'organisme partenaire que la DC a été approuvée par le CAC de cyberSanté Ontario. 5. cyberSanté Ontario met le changement en œuvre. 6. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe le représentant de l'organisme partenaire de l'état de la mise en œuvre (p. ex., réussie, annulée, ratée). 7. cyberSanté Ontario indique que la DC est « résolue ».		

4.12.1.3 Déclenché par l'organisme partenaire et mis en œuvre par l'organisme partenaire

Déclencheur	Organisme partenaire	**Exécutant**	Organisme partenaire
Situation	Changement normal ou planifié avec impact opérationnel		
Date limite de soumission	Sans objet		
Étapes	1. Le chef de service (ou le rôle équivalent) de l'organisme partenaire informe le Service de dépannage de cyberSanté Ontario que le changement normal a été mis en œuvre.		

4.12.2 Changement opérationnel urgent

4.12.2.1 Déclenché par l'organisme partenaire et mis en œuvre par cyberSanté Ontario

Déclencheur	Organisme partenaire	**Exécutant**	cyberSanté Ontario
Situation	Le système est accessible, mais la DC doit être mise en œuvre sans passer par le processus de changement normal; il s'agit d'une priorité opérationnelle. On part du principe que le changement a déjà été approuvé par le responsable des changements internes de l'organisme partenaire.		
Date limite de soumission	Le délai d'exécution des changements normaux ou planifiés n'est pas respecté.		
Étapes	1. L'équipe de cyberSanté Ontario, en collaboration avec le représentant de l'organisme partenaire, crée la demande de changement opérationnel urgent. 2. Le chef de service ou le responsable du déploiement de cyberSanté Ontario suit le processus de changement interne de cyberSanté Ontario et obtient l'autorisation de la part du comité d'approbation des changements urgents (CACU). ➢ *Remarque : Pour tout rejet d'une DC de la part du CACU de cyberSanté Ontario, le chef de service* ou le responsable du déploiement de cyberSanté Ontario *doit en indiquer les raisons au représentant de l'organisme partenaire.* 3. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe le représentant de l'organisme partenaire de l'approbation du CACU. 4. cyberSanté Ontario met le changement en œuvre. 5. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe l'organisme partenaire de l'état de la mise en œuvre (p. ex., réussie, annulée, ratée). 6. L'équipe de cyberSanté Ontario indique que la DC est « résolue ».		

4.12.2.2 Déclenché par cyberSanté Ontario et mis en œuvre par cyberSanté Ontario

Déclencheur	cyberSanté Ontario	**Exécutant**	cyberSanté Ontario
Situation	Le système est accessible, mais la DC doit être mise en œuvre sans passer par le processus de changement normal; il s'agit d'une priorité opérationnelle.		
Date limite de soumission	Le délai d'exécution des changements normaux ou planifiés n'est pas respecté et le changement peut être soumis uniquement pendant les heures d'ouverture de cyberSanté Ontario.		
Étapes	1. L'équipe de cyberSanté Ontario crée une demande de changement opérationnel urgent. 2. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe le représentant de l'organisme partenaire du changement opérationnel urgent et fournit des renseignements détaillés à son sujet. 3. L'équipe de cyberSanté Ontario applique le processus relatif aux changements opérationnels urgents pour obtenir l'approbation du changement. 4. cyberSanté Ontario met le changement en œuvre.		

	5. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe le représentant de l'organisme partenaire de l'état de la mise en œuvre (p. ex., réussie, annulée, ratée). 6. cyberSanté Ontario indique que la DC est « résolue ».

4.12.2.3 Déclenché par l'organisme partenaire et mis en œuvre par l'organisme partenaire

Déclencheur	Organisme partenaire	**Exécutant**	Organisme partenaire
Situation	Le système est accessible, mais la DC doit être mise en œuvre sans passer par le processus de changement normal; il s'agit d'une priorité opérationnelle.		
Date limite de soumission	Sans objet		
Étapes	1. Le chef de service (ou le rôle équivalent) de l'organisme partenaire informe le Service de dépannage de cyberSanté Ontario que le changement opérationnel urgent a été mis en œuvre.		

4.12.3 Changement de réparation d'urgence

4.12.3.1 Déclenché par l'organisme partenaire et mis en œuvre par cyberSanté Ontario

Les processus internes de cyberSanté Ontario relatifs aux DC de réparation s'appliquent à cette situation.

Déclencheur	Organisme partenaire	**Exécutant**	cyberSanté Ontario
Situation	Ouverture d'un incident. Un changement de réparation d'urgence est soumis au processus de gestion des changements. On part du principe que le changement a déjà été approuvé par le responsable des changements internes de l'organisme partenaire.		
Date limite de soumission	S.O.		
Étapes	1. Le représentant de l'organisme partenaire informe le Service de dépannage de cyberSanté Ontario du changement requis qui est lié à un ticket d'incident de priorité 1 ou 2. 2. cyberSanté Ontario applique le processus interne relatif aux changements urgents, en fonction du niveau de priorité : a. Pour un incident de priorité 1 ou 2, toutes les DC latentes doivent être déposées dans un délai de 24 heures; b. Pour un incident de priorité 3 ou 4, une demande de changement de réparation d'urgence doit être soumise. 3. cyberSanté Ontario met le changement en œuvre. 4. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe le représentant de l'organisme partenaire de l'état de la mise en œuvre (p. ex., réussie, annulée, ratée). 5. Le demandeur du changement de cyberSanté Ontario attribue l'état « fermé » à la demande de changement de réparation d'urgence ou à la DC latente.		

4.12.3.2 Déclenché par cyberSanté Ontario et mis en œuvre par cyberSanté Ontario

Les processus internes de cyberSanté Ontario relatifs aux DC de réparation ou aux DC latentes s'appliquent à cette situation.

Déclencheur	cyberSanté Ontario	**Exécutant**	cyberSanté Ontario
Situation	Ouverture d'un incident de priorité 1 ou 2. Arrêt du système (changement de réparation).		
Date limite de soumission	Sans objet		
Étapes	1. L'équipe de cyberSanté Ontario met en œuvre le changement urgent. 2. cyberSanté Ontario applique le processus interne relatif aux changements urgents pour un incident de priorité 1 ou 2, en veillant notamment à ce que toutes les DC latentes soient déposées dans un délai de 24 heures. 3. cyberSanté Ontario met en œuvre le changement urgent. 4. Le chef de service ou le responsable du déploiement de cyberSanté Ontario informe le représentant de l'organisme partenaire de la mise en œuvre du changement urgent. 5. Le demandeur du changement de cyberSanté Ontario indique que la DC associée ou latente est « résolue ».		

4.12.3.3 Déclenché par l'organisme partenaire et mis en œuvre par l'organisme partenaire

Déclencheur	Organisme partenaire	**Exécutant**	Organisme partenaire
Situation	Ouverture d'un incident de priorité 1 ou 2 (rétablissement). Arrêt du système (changement de réparation).		
Date limite de soumission	Sans objet		
Étapes	1. Le chef de service (ou le rôle équivalent) de l'organisme partenaire informe le représentant de cyberSanté Ontario que le changement urgent a été mis en œuvre.		

4.12.4 Changements standards

Les changements standards sont préalablement approuvés par le CAC. Ils n'ont pas besoin d'être approuvés par l'organisme partenaire ou par le CAC de cyberSanté Ontario pour être mis en œuvre.

Un changement est qualifié de « changement standard » par le CAC si sa mise en œuvre n'altère pas le service visé et n'entraîne pas son arrêt, et si ce changement n'a aucun impact sur les autres systèmes, composants ou éléments de configuration.

4.13 Environnements de services

Les changements demandés sont évalués et mis à l'essai dans des environnements inférieurs avant d'être mis en œuvre dans l'environnement de production réel du service de cyberSanté Ontario. Toutefois, les organismes partenaires ne participent pas aux cycles des environnements hors production ou inférieurs de cyberSanté Ontario, tels que les environnements de test et de pré-production.

Une fois la demande de changement lancée par l'organisme partenaire par l'intermédiaire du Service de dépannage de cyberSanté Ontario, le chef de service ou le responsable du déploiement représente ensuite la demande de changement au nom de l'organisme partenaire comme suit :

- Il fait entrer la DC dans le cheminement de promotion des environnements inférieurs;
- Il représente la DC au CAC de cyberSanté Ontario;
- Il suit l'approbation ou la promotion de la DC dans l'environnement de production de cyberSanté Ontario.

Remarque : L'environnement de production de cyberSanté Ontario est pris en charge 24 heures sur 24, 7 jours sur 7, 365 jours par an, et les environnements hors production ou inférieurs sont pris en charge durant les heures d'ouverture de cyberSanté Ontario, soit de 8 h à 17 h, heure de l'Est (HE).

5.0 Gestion du niveau de service

5.1 Disponibilité du service

La disponibilité du service constitue un élément essentiel de l'évaluation du rendement global d'un service de cyberSanté Ontario. Elle repose sur la somme des disponibilités de chaque composant qui assure le fonctionnement du service. Pendant la phase de projet du service, les organismes partenaires doivent indiquer à cyberSanté Ontario l'objectif de disponibilité opérationnelle pour les composants qu'ils possèdent ou qu'ils gèrent et qui permettent de mener à bien un service de cyberSanté Ontario. cyberSanté Ontario doit être informé de toutes les modifications de cet objectif pendant la durée de vie du service, par l'intermédiaire de son Service de dépannage de cyberSanté Ontario.

Les normes de cyberSanté Ontario qui régissent les niveaux de disponibilité et de service dans le cadre de l'objectif de disponibilité d'un service de cyberSanté Ontario sont les suivantes :

Résumé des niveaux de service			
Paramètre du niveau de service	**Paramètre d'évaluation de l'objectif**	**Critères de mesure**	**Fréquence des rapports**
Disponibilité du service			
Temps de disponibilité du service de cyberSanté Ontario	Établi individuellement pour chaque service de cyberSanté Ontario et représenté sous la forme d'un pourcentage (%) de temps maximal disponible par mois	Le ***temps maximal disponible*** est le temps de service convenu au cours de la période de référence. Il est exprimé en nombre total de minutes par mois et se calcule comme suit : *Disponibilité* = temps maximal disponible – temps d'arrêt non prévu / temps maximal disponible *100 Le ***temps d'arrêt non prévu*** (mesuré en minutes) correspond aux interruptions de services de niveau P1-Critique selon cyberSanté Ontario, mais exclut : • Les temps d'arrêt prévus dans le cadre d'un entretien approuvé préalablement; • Les interruptions survenant en dehors des heures de soutien convenues; • Les interruptions de services de niveau P2-Élevé ou moins selon	Tous les mois

Résumé des niveaux de service			
Paramètre du niveau de service	**Paramètre d'évaluation de l'objectif**	**Critères de mesure**	**Fréquence des rapports**
		cyberSanté Ontario.	
Reprise après catastrophe (RC)			
Objectif de délai de rétablissement (ODR)	Établi individuellement pour chaque service et fonction de cyberSanté Ontario.	Il s'agit de la période de temps à l'intérieur de laquelle les services de TI et les services connexes sont rétablis dans leur ensemble.	Au besoin
Objectif de point de rétablissement (OPR)	Établi individuellement pour chaque service et fonction de cyberSanté Ontario.	Il s'agit de la période de temps à l'intérieur de laquelle des données pourraient être perdues à la suite d'un incident majeur touchant un service de TI. L'OPR est indépendant de l'objectif de délai de rétablissement (ODR).	Au besoin
ENS			
Service de cyberSanté Ontario – Temps moyen de réparation (TMR)	Norme de cyberSanté Ontario relative aux incidents	On attribue un niveau de priorité (1, 2, 3 ou 4) aux incidents en fonction de leur impact et de leur portée, ainsi qu'une ENS pour leur résolution. L'IRC (indicateur de rendement clé) de cyberSanté Ontario pour le TMR est de résoudre 90 % de tous les tickets d'incidents (quel que soit le niveau de priorité) au sein de l'ENS.	Tous les mois
Service de cyberSanté Ontario – Demande de service réglée dans les délais impartis	Norme de cyberSanté Ontario relative aux demandes de service	Il s'agit de la période moyenne entre l'enregistrement d'une demande de service et le moment où cette demande est satisfaite. La durée de résolution ciblée varie selon le niveau de priorité. L'objectif global est de parvenir à atteindre cette durée 90 % du temps.	Tous les mois

Résumé des niveaux de service			
Paramètre du niveau de service	**Paramètre d'évaluation de l'objectif**	**Critères de mesure**	**Fréquence des rapports**
Opérations liées à la protection de la vie privée	Norme de cyberSanté Ontario relative aux demandes de service	Il s'agit de la période moyenne entre l'enregistrement d'une demande de service et le moment où cette demande est satisfaite. La durée de résolution ciblée varie selon le niveau de priorité. L'objectif global est de parvenir à atteindre cette durée 90 % du temps.	S.O.
Gestion des incidents et des violations touchant la protection de la vie privée	Norme de cyberSanté Ontario relative aux incidents	Il s'agit de la période moyenne entre l'enregistrement d'un incident et sa résolution. La durée de résolution ciblée varie selon le niveau de priorité. L'objectif global est de parvenir à atteindre cette durée 90 % du temps. Pour tous les types d'incident, l'« incident résolu dans les délais impartis » est mesuré en fonction du niveau de priorité et représente le pourcentage d'incidents résolus dans les délais ciblés.	S.O.
Gestion des incidents de sécurité	Norme de cyberSanté Ontario relative aux incidents	Il s'agit de la période moyenne entre l'enregistrement d'un incident et sa résolution. La durée de résolution ciblée varie selon le niveau de priorité. L'objectif global est de parvenir à atteindre cette durée 90 % du temps. Pour tous les types d'incident, l'« incident résolu dans les délais impartis » est mesuré en fonction du niveau de priorité et représente le pourcentage d'incidents résolus dans les délais ciblés.	Tous les mois
Service de dépannage de cyberSanté Ontario			
Vitesse de réponse aux appels	En moins de 60 secondes 90 % du temps	Moyenne mensuelle du temps mis pour répondre à l'appel d'un client. L'objectif est de parvenir à répondre aux appels en moins de	Tous les mois

Résumé des niveaux de service			
Paramètre du niveau de service	**Paramètre d'évaluation de l'objectif**	**Critères de mesure**	**Fréquence des rapports**
		60 secondes 90 % du temps.	
Taux d'abandon	Inférieur ou égal à 5 % du nombre total d'appels reçus	Nombre de correspondants qui raccrochent avant d'obtenir une réponse, exprimé sous forme de pourcentage du nombre total d'appels auxquels on a répondu. Mesuré pour tous les clients bénéficiant de services de soutien mensuels de la part de cyberSanté Ontario. Le Service de dépannage de cyberSanté Ontario peut être joint par téléphone durant ses heures d'ouverture.	Tous les mois
Incidents signalés par courriel	D'après l'objectif de niveau de service (ONS) de cyberSanté Ontario	Dans un délai de 2 heures • 70 % avant le 31 avril 2016; • 75 % du 1er mai au 30 septembre 2016; • 80 % après le 1er octobre 2016. Dans un délai de 8 heures • 85 % avant le 31 avril 2016; • 90 % du 1er mai au 30 septembre 2016; • 98 % après le 1er octobre 2016.	Tous les mois

Table 4 - Résumé des niveaux de service

5.2 Réunions d'examen du service

Il est possible d'organiser des réunions à une fréquence convenue (tous les mois, généralement) pour procéder à l'examen du service. Ces réunions peuvent être l'occasion de discuter des objectifs de niveau de service, d'étudier la disponibilité du service, d'exprimer ses préoccupations, d'aborder le prochain entretien programmé et les changements opérés par cyberSanté Ontario et par l'organisme partenaire. Elles seront animées par le gestionnaire des programmes clients ou par le chef de service de cyberSanté Ontario.

Appendix A - Jours fériés et congés de cyberSanté Ontario

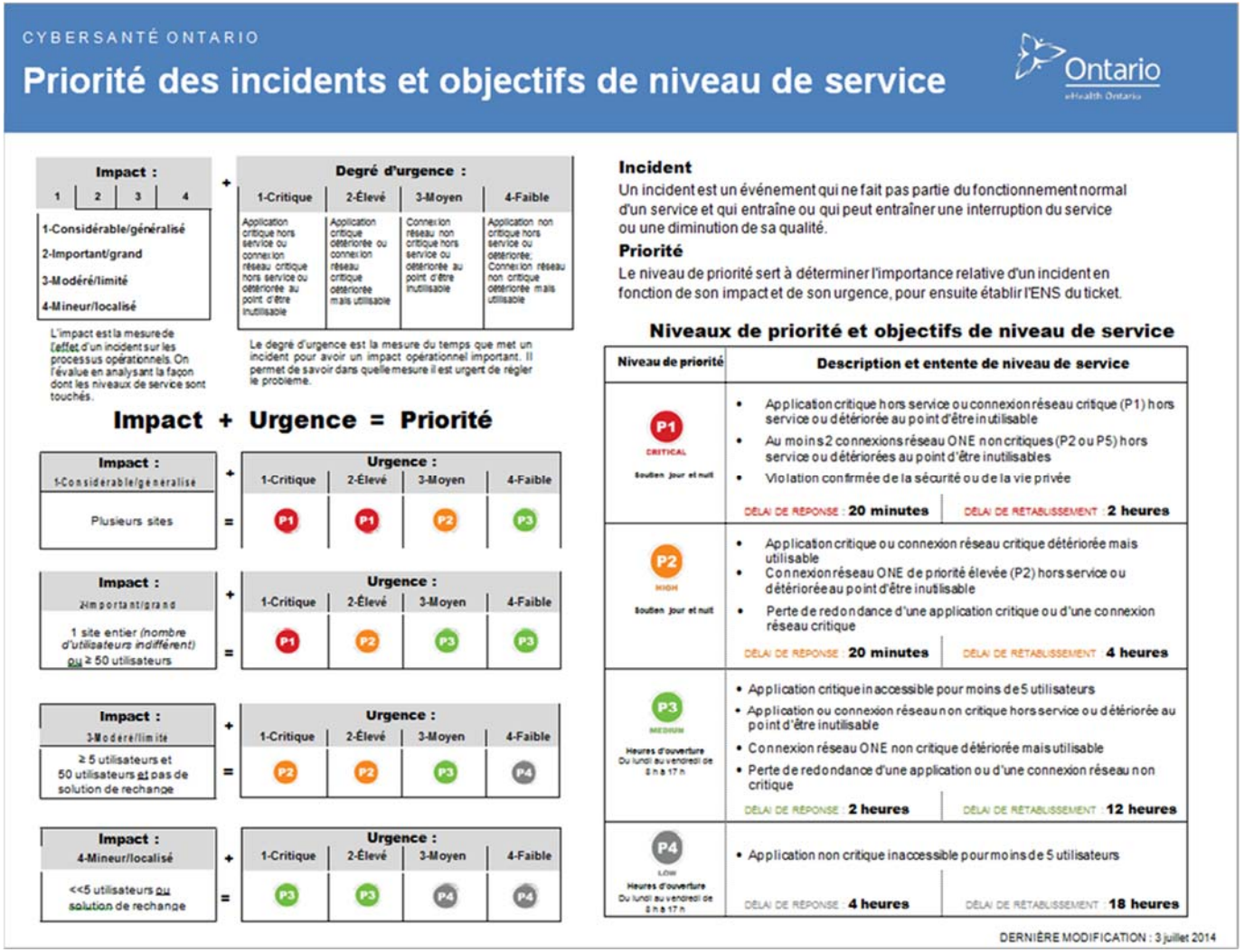
La liste ci-après indique les jours fériés officiels observés en Ontario et les autres jours chômés par cyberSanté Ontario. L'ENS sera interrompue lors des jours chômés par cyberSanté Ontario si les équipes de soutien de cyberSanté Ontario qui doivent prendre des mesures dans le cadre du processus de résolution de l'incident travaillent uniquement pendant les heures d'ouverture.

Jour férié	Province de l'Ontario
Jour de l'An	Congé
Jour de la Famille	Congé
Vendredi saint	Congé
Fête de Victoria	Congé
Fête du Canada	Congé
Fête du Travail	Congé
Action de grâces	Congé
Jour de Noël	Congé
Lendemain de Noël	Congé

Jour non férié	cyberSanté Ontario
Lundi de Pâques	Congé
Congé civique d'août (fête de Simcoe)	Congé
Jour du Souvenir	Congé

Note: La date de ces congés (excepté le jour du Souvenir) varie d'une année à l'autre.

Appendix B - Normes de cyberSanté Ontario en matière de priorité des incidents et d'objectifs de niveau de service



CYBERSANTÉ ONTARIO

Priorité des incidents et objectifs de niveau de service

Ontario eHealth Ontario

Impact :	1	2	3	4
1-Considérable/généralisé				
2-Important/grand				
3-Modéré/limité				
4-Mineur/localisé				

L'impact est la mesure de l'effet d'un incident sur les processus opérationnels. On l'évalue en analysant la façon dont les niveaux de service sont touchés.

Degré d'urgence :	1-Critique	2-Élevé	3-Moyen	4-Faible
	Application critique hors service ou connexion réseau critique hors service ou détériorée au point d'être inutilisable	Application critique détériorée ou connexion réseau critique détériorée mais utilisable	Connexion réseau non critique hors service ou détériorée au point d'être inutilisable	Application non critique hors service ou détériorée; Connexion réseau non critique détériorée mais utilisable

Le degré d'urgence est la mesure du temps que met un incident pour avoir un impact opérationnel important. Il permet de savoir dans quelle mesure il est urgent de régler le problème.

Impact + Urgence = Priorité

Impact :	Urgence : 1-Critique	2-Élevé	3-Moyen	4-Faible
1-Considérable/généralisé : Plusieurs sites	P1	P1	P2	P3
2-Important/grand : 1 site entier *(nombre d'utilisateurs indifférent)* ou ≥ 50 utilisateurs	P1	P2	P3	P3
3-Modéré/limité : ≥ 5 utilisateurs et 50 utilisateurs et pas de solution de rechange	P2	P2	P3	P4
4-Mineur/localisé : <<5 utilisateurs ou solution de rechange	P3	P3	P4	P4

Incident

Un incident est un événement qui ne fait pas partie du fonctionnement normal d'un service et qui entraîne ou qui peut entraîner une interruption du service ou une diminution de sa qualité.

Priorité

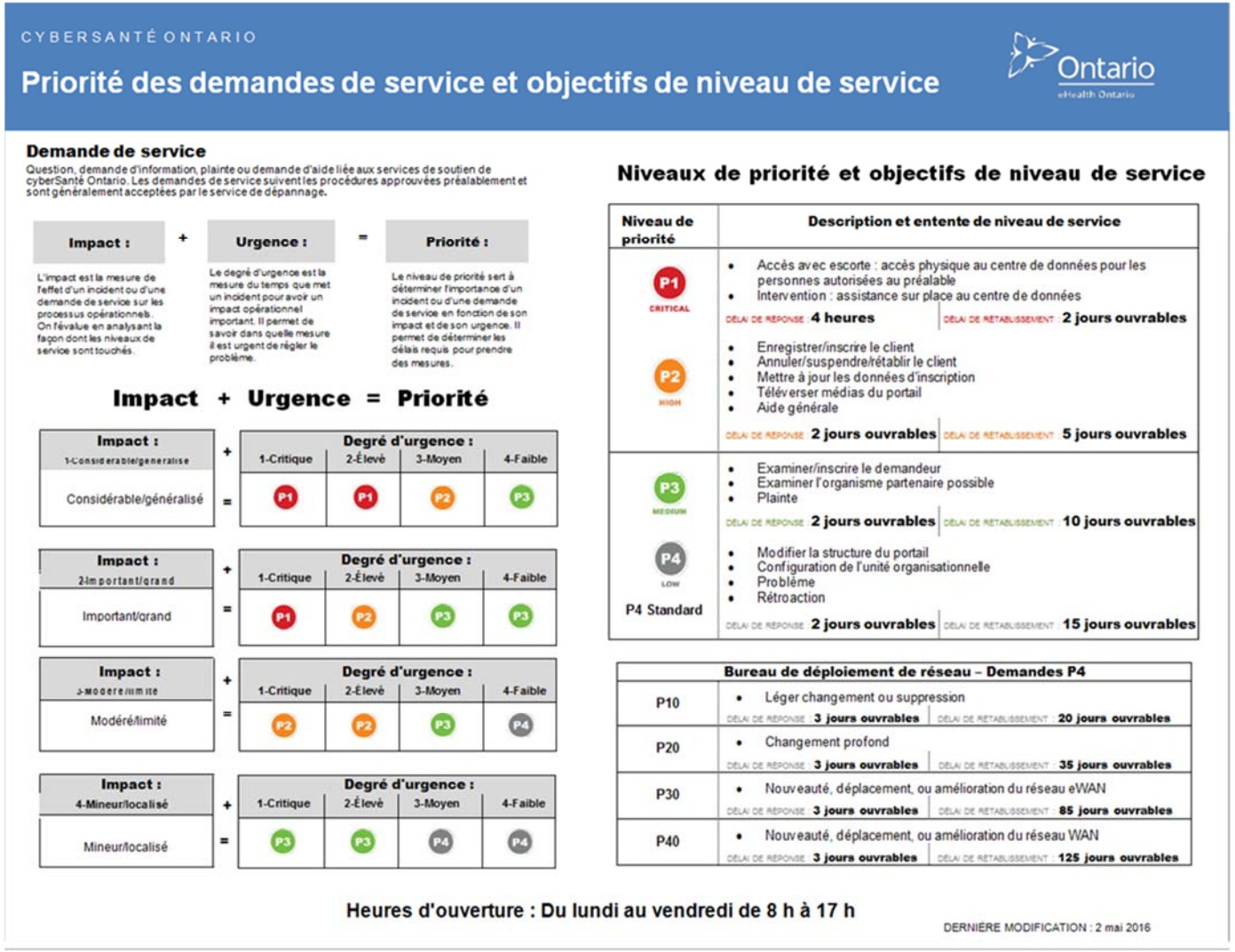
Le niveau de priorité sert à déterminer l'importance relative d'un incident en fonction de son impact et de son urgence, pour ensuite établir l'ENS du ticket.

Niveaux de priorité et objectifs de niveau de service

Niveau de priorité	Description et entente de niveau de service	
P1 CRITICAL — Soutien jour et nuit	• Application critique hors service ou connexion réseau critique (P1) hors service ou détériorée au point d'être inutilisable • Au moins 2 connexions réseau ONE non critiques (P2 ou P5) hors service ou détériorées au point d'être inutilisables • Violation confirmée de la sécurité ou de la vie privée	DÉLAI DE RÉPONSE : **20 minutes** — DÉLAI DE RÉTABLISSEMENT : **2 heures**
P2 HIGH — Soutien jour et nuit	• Application critique ou connexion réseau critique détériorée mais utilisable • Connexion réseau ONE de priorité élevée (P2) hors service ou détériorée au point d'être inutilisable • Perte de redondance d'une application critique ou d'une connexion réseau critique	DÉLAI DE RÉPONSE : **20 minutes** — DÉLAI DE RÉTABLISSEMENT : **4 heures**
P3 MEDIUM — Heures d'ouverture Du lundi au vendredi de 9 h à 17 h	• Application critique inaccessible pour moins de 5 utilisateurs • Application ou connexion réseau non critique hors service ou détériorée au point d'être inutilisable • Connexion réseau ONE non critique détériorée mais utilisable • Perte de redondance d'une application ou d'une connexion réseau non critique	DÉLAI DE RÉPONSE : **2 heures** — DÉLAI DE RÉTABLISSEMENT : **12 heures**
P4 LOW — Heures d'ouverture Du lundi au vendredi de 9 h à 17 h	• Application non critique inaccessible pour moins de 5 utilisateurs	DÉLAI DE RÉPONSE : **4 heures** — DÉLAI DE RÉTABLISSEMENT : **18 heures**

DERNIÈRE MODIFICATION : 3 juillet 2014

Appendix C - Normes de cyberSanté Ontario en matière de priorité des demandes de service et d'objectifs de niveau de service



CYBERSANTÉ ONTARIO

Priorité des demandes de service et objectifs de niveau de service

Ontario
eHealth Ontario

Demande de service

Question, demande d'information, plainte ou demande d'aide liée aux services de soutien de cyberSanté Ontario. Les demandes de service suivent les procédures approuvées préalablement et sont généralement acceptées par le service de dépannage.

Impact :	+	Urgence :	=	Priorité :
L'impact est la mesure de l'effet d'un incident ou d'une demande de service sur les processus opérationnels. On l'évalue en analysant la façon dont les niveaux de service sont touchés.		Le degré d'urgence est la mesure du temps que met un incident pour avoir un impact opérationnel important. Il permet de savoir dans quelle mesure il est urgent de régler le problème.		Le niveau de priorité sert à déterminer l'importance d'un incident ou d'une demande de service en fonction de son impact et de son urgence. Il permet de déterminer les délais requis pour prendre des mesures.

Impact + Urgence = Priorité

Impact :	Degré d'urgence : 1-Critique	2-Élevé	3-Moyen	4-Faible
1-Considérable/généralisé : Considérable/généralisé	P1	P1	P2	P3
2-Important/grand : Important/grand	P1	P2	P3	P3
3-Modéré/limité : Modéré/limité	P2	P2	P3	P4
4-Mineur/localisé : Mineur/localisé	P3	P3	P4	P4

Niveaux de priorité et objectifs de niveau de service

Niveau de priorité	Description et entente de niveau de service
P1 CRITICAL	• Accès avec escorte : accès physique au centre de données pour les personnes autorisées au préalable • Intervention : assistance sur place au centre de données DÉLAI DE RÉPONSE : **4 heures** | DÉLAI DE RÉTABLISSEMENT : **2 jours ouvrables**
P2 HIGH	• Enregistrer/inscrire le client • Annuler/suspendre/rétablir le client • Mettre à jour les données d'inscription • Téléverser médias du portail • Aide générale DÉLAI DE RÉPONSE : **2 jours ouvrables** | DÉLAI DE RÉTABLISSEMENT : **5 jours ouvrables**
P3 MEDIUM	• Examiner/inscrire le demandeur • Examiner l'organisme partenaire possible • Plainte DÉLAI DE RÉPONSE : **2 jours ouvrables** | DÉLAI DE RÉTABLISSEMENT : **10 jours ouvrables**
P4 LOW P4 Standard	• Modifier la structure du portail • Configuration de l'unité organisationnelle • Problème • Rétroaction DÉLAI DE RÉPONSE : **2 jours ouvrables** | DÉLAI DE RÉTABLISSEMENT : **15 jours ouvrables**

Bureau de déploiement de réseau – Demandes P4	
P10	• Léger changement ou suppression DÉLAI DE RÉPONSE : **3 jours ouvrables** | DÉLAI DE RÉTABLISSEMENT : **20 jours ouvrables**
P20	• Changement profond DÉLAI DE RÉPONSE : **3 jours ouvrables** | DÉLAI DE RÉTABLISSEMENT : **35 jours ouvrables**
P30	• Nouveauté, déplacement, ou amélioration du réseau eWAN DÉLAI DE RÉPONSE : **3 jours ouvrables** | DÉLAI DE RÉTABLISSEMENT : **85 jours ouvrables**
P40	• Nouveauté, déplacement, ou amélioration du réseau WAN DÉLAI DE RÉPONSE : **3 jours ouvrables** | DÉLAI DE RÉTABLISSEMENT : **125 jours ouvrables**

Heures d'ouverture : Du lundi au vendredi de 8 h à 17 h

DERNIÈRE MODIFICATION : 2 mai 2016

Appendix D - Acronymes

Terme	Définition/Description
BAIPVP du MSSLD	Ministère de la Santé et des Soins de longue durée et Bureau de l'accès à l'information et de la protection de la vie privée
CAC	Comité d'approbation des changements
CACU	Comité d'approbation des changements urgents
DC	Demande de changement
DCU	Demande de changement urgent
DMC	Directive en matière de consentement
DSPGI	Direction des stratégies et des politiques de gestion de l'information
Environnement de production	Il s'agit de l'environnement dans lequel le service de cyberSanté Ontario est actif et à la disposition des utilisateurs externes. Il constitue la base de la durée de vie du service.
Environnements inférieurs	Également appelés « environnements hors production », il s'agit des environnements de développement (développement et test d'intégration (DTI)), des environnements de test (ETI1 et ETI2) et des environnements de pré-production (EPP, ATP [auto-test partenaire], test des renseignements personnels sur la santé).
GIS	Gestion des incidents de sécurité de cyberSanté Ontario
GSC	Gestionnaire des services à la clientèle
GSS du MSSLD	Groupement des services de santé du ministère de la Santé et des Soins de longue durée
GSTI	Gestion des services de technologie de l'information
GVS	Gestion des violations de sécurité cyberSanté Ontario
ID	Image diagnostique
ITIL	Information Technology Infrastructure Library L'ITIL V3 est la version publiée en 2007.
P1	Niveau de priorité le plus élevé (incident ou ticket) – Critique
P2	Deuxième niveau de priorité le plus élevé (incident ou ticket) – Élevé
PCU	Point de contact unique
PPMO	Programmes publics de médicaments de l'Ontario (PPMO)
RNM	Répertoire numérique des médicaments
RP	Renseignements personnels
RPS	Renseignements personnels sur la santé
SIE	Système d'information aux entreprises
SILO	Système d'information de laboratoire de l'Ontario

Terme	Définition/Description
VPPP	Visualiseur des profils pharmaceutiques des patients