Ministère de la Santé
et des Services sociaux

Technologies de l'information

DIRECTIVE

MSSS-DIR06

Recours aux services infonuagiques

Version : 1.4

Approuvée par:	**Reno Bernier**, sous-ministre associé Dirigeant réseau de l'information
Publiée le :	2022-12-22

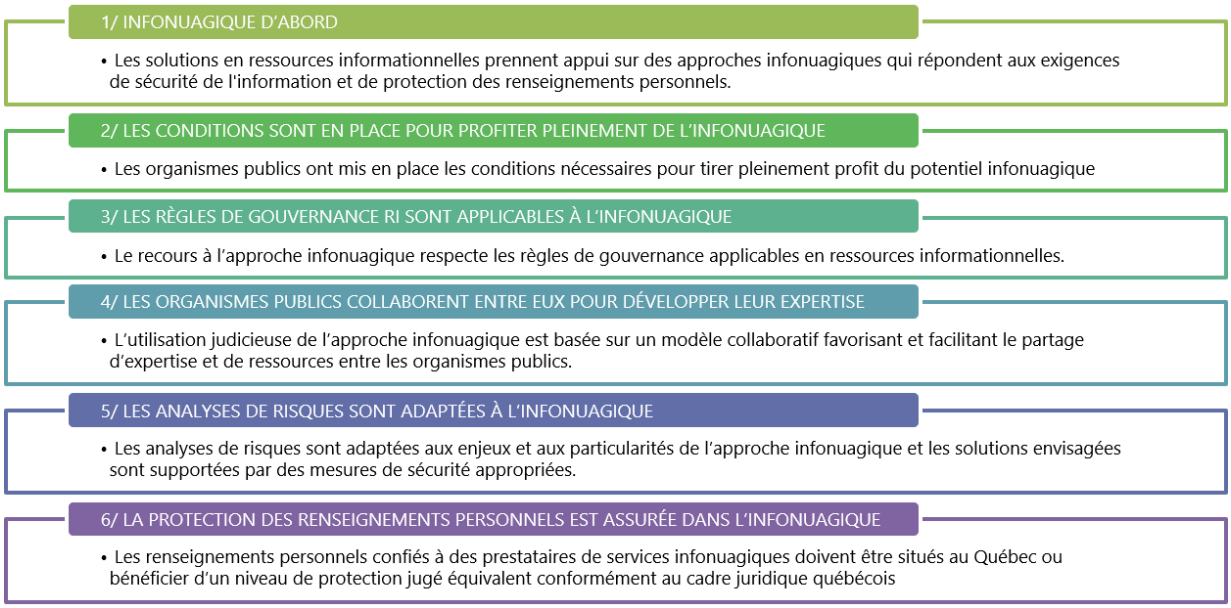
Québec

Table des matières

Objectifs

Le présent document vise à formuler les directives adaptées au contexte de l'informatisation du secteur de la santé et des services sociaux dans le but d'encadrer les pratiques en matière d'approvisionnement et de consommation des services infonuagiques.

Le Secrétariat du Conseil du trésor (SCT) a adopté et publié, le 8 juillet 2019, des orientations gouvernementales en matière de services infonuagiques s'adressant à tous les ministères et organismes publics (OP) québécois. Les orientations, initialement définies par le SCT et reprises par le Ministère de la Cybersécurité et du Numérique (MCN) en janvier 2022, visent à établir les grandes lignes directrices auxquelles tout OP doit se conformer en vue d'acquérir des services infonuagiques. En fait, elles constituent le périmètre à respecter en vue de favoriser des actions concertées en conformité avec le cadre de référence gouvernemental.



Dans le cadre des décrets 38-2019 et 596-2020 et de son Programme de consolidation des centres de traitement informatique (PCCTI), de la stratégie gouvernementale en technologie de l'information (TI) et de la stratégie de transformation numérique gouvernementale (STNG), auxquels le MSSS et RSSS sont assujettis, le gouvernement du Québec prend de grands moyens pour renouveler l'état par les technologies de l'information.

Conforme avec la vision stratégique gouvernementale, le MCN planifie et organise la mise en place de services infonuagiques communs pour tous les OP en fonction de leurs besoins d'affaires.

L'infonuagique est un modèle qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de services ou ressources informatiques configurables et externalisés. L'infonuagique offre des solutions d'affaires standardisées (*infrastructures, plateformes et logiciels*).

Vision MSSS

La vision du MSSS en regard de l'utilisation de services infonuagiques est en lien avec celle du MCN : *« Tirer profit de l'infonuagique pour accroître l'agilité gouvernementale et pour réaliser des économies en ressources informationnelles tout en assurant la pérennité des actifs informationnels et le respect de la vie privée ».*

Dans un souci de respecter cette vision, le MSSS juge opportun de diffuser un ensemble de directives claires et précises que tout organisme du RSSS doit respecter.

L'investissement dans les services et solutions communes et partageables par l'ensemble des organismes du RSSS est priorisé.

Les solutions infonuagiques sont privilégiées lorsqu'arrive l'opportunité de remplacer, de développer ou d'acquérir une solution d'affaires.

Le MSSS vise à :

- Respecter la mise en application de la vision gouvernementale de façon à tirer profit de l'infonuagique.
- Informer les organismes du RSSS quant au processus d'approvisionnement de solutions en mode infonuagique.
- Encadrer les pratiques du RSSS quant à l'utilisation de solutions en mode infonuagique externe.
- Sensibiliser les organismes du RSSS quant au respect des exigences en matière de sécurité de l'information et de protection des renseignements personnels par les fournisseurs de services infonuagiques.

Toute initiative en infonuagique qui nécessite des investissements est considérée à titre de projet en ressources informationnelles (RI) et par conséquent, est soumis aux mêmes mécanismes de gouvernance du plan de gestion en ressources informationnelles. Toute initiative en vue d'acquérir un service infonuagique doit être autorisée préalablement par le MSSS selon les règles de gouvernance établie.

Champ d'application

Cette directive s'applique à tous les organismes relevant du Dirigeant de l'information (DI), plus précisément :

1° au MSSS;

2° aux établissements visés par la Loi sur les services de santé et les services sociaux (LSSSS - L.R.Q., c. S-4.2);

3° au Conseil cri de la santé et des services sociaux de la Baie James institué en vertu de la Loi sur les services de santé et les services sociaux pour les autochtones cris (L.R.Q., c. S-5);

4° aux centres de communication santé visés par la Loi sur les services préhospitaliers d'urgence (chapitre S-6.2);

5° au Commissaire à la santé et au bien-être;

6° à la Corporation d'Urgences-Santé;

7° à Héma-Québec;

8° à l'Institut national d'excellence en santé et en services sociaux;

9° à l'Institut national de santé publique du Québec;

10° à l'Office des personnes handicapées du Québec;

11° à la Régie de l’assurance maladie du Québec (RAMQ).

Cadre de référence

- Décret 38-2019
- Décret 596-2020
- Énoncé d’orientation infonuagique du gouvernement du Québec
- Guides de référence de l'infonuagique (les 3 volets)
- Guide utilisateur IaaS, PaaS du courtier infonuagique
- Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels
- Loi sur les services de santé et les services sociaux RLRQ - chapitre S.4.2 (LSSSS)
- Guide d’analyse des préjudices du MCN une fois rendu public.

Définitions

Terme	Définition
Fournisseur	Une personne morale de droit privé, une société en nom collectif, en commandite ou en participation ou une personne physique qui exploite une entreprise individuelle.
Renseignement personnel	Un renseignement est personnel lorsqu'il concerne une personne physique et permet de l'identifier. Un tel renseignement est confidentiel et ne peut être communiqué à une autre personne sauf si la personne concernée par ce renseignement y consent ou que la loi permet sa divulgation.
Renseignement confidentiel	Tout renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) ci-après, Loi sur l'accès, notamment un renseignement personnel, un renseignement ayant des incidences sur les relations intergouvernementales, sur les négociations entre organismes publics, sur l'économie, sur l'administration de la justice et la sécurité publique, sur les décisions administratives ou politiques ou sur la vérification.
Nuage externe	Infrastructure accessible par Internet et utilisée par un large public. L'infrastructure est la propriété d'une entreprise qui joue le rôle de fournisseurs de service.
Nuage gouvernemental	Service infonuagique gouvernemental basé sur le modèle IaaS (*Infrastructure as a Service*) rendu disponible par le MCN. Hébergé dans un environnement physique sécurisé, il offre un service hautement automatisé, en mode libre-service et payable à la consommation.
Multi-nuages	Le multi-nuages est un modèle de déploiement de l'infonuagique qui permet aux entreprises de fournir des services d'application sur plusieurs nuages privés et externes contenant une ou plusieurs combinaisons de ce qui suit : plusieurs fournisseurs infonuagiques, plusieurs comptes et contrats infonuagiques, plusieurs zones d'accueil et disponibilité infonuagiques ou plusieurs régions infonuagiques.
Approche infonuagique native *(cloud native)*	Les technologies infonuagiques natives permettent aux organisations de créer et d'exécuter des applications évolutives dans des environnements dynamiques et modernes, tels que des nuages externes, privés et hybrides. Les conteneurs, les maillages de service, les micro-services, l'infrastructure immuable et les API déclaratives illustrent cette approche. Cette approche présente certains avantages par rapport au développement et à la programmation traditionnels : • Développement et déploiement de code plus rapide

	• Rotation plus rapide des services • Adoption d'une programmation sans serveur • Plus grande incitation à l'utilisation de processus DevOps • Évolutivité • Résilience • Services réutilisables
Solution logicielle en tant que service (SaaS)	La capacité offerte au consommateur consiste à utiliser les applications du fournisseur s'exécutant sur une infrastructure infonuagique. Les applications sont accessibles à partir de divers périphériques clients via une interface client légère telle qu'un navigateur Web (par exemple, un e-mail basé sur le Web). Le consommateur ne gère ni ne contrôle l'infrastructure infonuagique sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même les capacités des applications individuelles, à l'exception possible des paramètres de configuration des applications spécifiques à l'utilisateur ou à l'organisation.
Plate-forme en tant que service (PaaS)	La capacité fournie au consommateur consiste à déployer sur l'infrastructure infonuagique des applications créées ou acquises par le consommateur à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure infonuagique sous-jacente, notamment le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais contrôle les applications déployées et éventuellement les paramètres de configuration de l'environnement d'hébergement d'applications.
Infrastructure en tant que service (IaaS)	La capacité fournie au consommateur est de fournir le traitement, le stockage, les réseaux et d'autres ressources informatiques fondamentales où le consommateur est capable de déployer et d'exécuter des logiciels arbitraires, qui peuvent inclure l'exploitation systèmes et applications. Le consommateur ne gère ni ne contrôle l'infrastructure infonuagique sous-jacente, mais contrôle les systèmes d'exploitation, le stockage et les applications déployées ; et éventuellement un contrôle limité de certains composants réseau (par exemple, les pare-feu hôtes). IaaS "Natif" (Fournisseur) : Pas de couche d'intégration / intermédiaire. Pour les solutions existantes ne pouvant être déployées en SaaS ou PaaS public ou qu'il faut reconduire en IaaS publique pour d'autres raisons : techniques, capacité, temps, etc. IaaS " Non-natif " : Pour les solutions devant utiliser une couche d'intégration/intermédiaire (ex : VMware), pour des impératifs de temps de livraison, de capacité, de compatibilité ou pour toute autre considération technique dans l'éventualité où le mode IaaS public

	"natif" n'est pas applicable ou pertinent. Ce mode de prestation devrait être considéré comme temporaire ou transitoire.
Salle de proximité	Local informatique propre à des équipements informatiques jugés essentiels qui ne peuvent aller dans des centres de traitement informatiques conventionnels, ni dans l'infonuagique et qui doivent demeurer sur place. Par exemple : • Équipements de réseautique en soutien aux réseaux de bureautique, en soutien aux réseaux étendus et pour accéder aux services infonuagiques; • Systèmes de sécurité, de gestion de la climatisation et de surveillance audiovisuelle d'édifices hébergeant des œuvres d'art, certains systèmes de sécurité d'un centre de détention, laboratoires éducatifs, systèmes biomédicaux, etc.; • Postes de travail bureautique et équipements physiques d'impression ou de numérisation.
Profil A, B et C	Un profil est un ensemble de contrôles de sécurité visant à protéger adéquatement un actif informationnel dans le nuage selon son niveau de sensibilité. Le PCCTI propose trois profils (A, B, et C), au choix, selon la sensibilité de l'actif. La différence entre les trois profils réside essentiellement dans le nombre de contrôles de sécurité à mettre en place. Plus l'actif est sensible, plus les exigences et les contrôles de sécurité sont élevés. • **Profil A -** Ce profil est jugé approprié pour la protection d'informations non sensibles, c'est-à-dire des informations dont la divulgation non autorisée, l'atteinte à l'intégrité ou l'indisponibilité causeraient des préjudices de gravité très faible ou faible. • **Profil B** - Ce profil est jugé approprié pour la protection d'informations sensibles, c'est-à-dire des informations dont la divulgation non autorisée, l'atteinte à l'intégrité ou l'indisponibilité causeraient des préjudices de gravité modérée. • **Profil C** - Ce profil est jugé approprié pour la protection d'informations hautement sensibles, c'est-à-dire des informations dont la divulgation non autorisée, l'atteinte à l'intégrité ou l'indisponibilité causeraient des préjudices de gravité élevée et très élevée.

Directive 1. L'infonuagique d'abord

1 Le MSSS et les organismes du RSSS ont recours aux solutions infonuagiques lorsque celles-ci sont disponibles.

Précisions à considérer :

1.1 Dans l'évaluation des solutions pour répondre à leurs besoins d'affaires, l'organisme considère d'abord l'utilisation des services communs rendus disponibles provincialement et les solutions infonuagiques incluses dans les catalogues de service (MSSS ou MCN).

1.2 Une analyse d'impact d'affaire sur l'actif doit être réalisée afin d'inscrire l'actif informationnel dans le plan de continuité des affaires de l'organisme. De cette analyse doivent ressortir les points suivants: la priorité de l'actif vis-à-vis des services essentiels, la durée maximale d'interruption acceptable (RTO) et la perte de donnée maximale acceptable (RPO).

1.3 Un exercice déterminant la catégorisation de l'information doit préalablement être effectué. La catégorisation permet d'attribuer des niveaux d'impact sur la disponibilité, l'intégrité et la confidentialité de l'actif (DIC) vis-à-vis de l'information contenue ou en traitement.

1.4 Une analyse des préjudices, prescrite par le MCN, doit obligatoirement être produite pour permettre la classification de la sensibilité des données et par la suite, l'identification du modèle d'hébergement et du profil de sécurité associé (A, B ou C). Le niveau de préjudices résultant détermine les exigences et les contrôles de sécurité de base qui sont requis et qui doivent obligatoirement être mis en place par le fournisseur de service infonuagique.

1.5 L'analyse de risques demeure une exigence quant à la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels. Elle détermine les mesures de sécurité complémentaires qui seront spécifiques à la solution.

1.6 En ce qui concerne le lieu d'hébergement des données :

1.6.1 Si l'actif est considéré comme sensible (profil B ou C) (héberge des données jugées sensibles ou très sensibles) : les renseignements confidentiels (notamment des renseignements cliniques, médicaux ou sociaux des usagers du RSSS) doivent demeurer au Canada. À titre exceptionnel, le MSSS ou un organisme du RSSS peut héberger des renseignements à l'extérieur du Canada (ex. : un produit dont les fournisseurs existants n'ont pas d'infrastructure au Canada). Le cas échéant, le MSSS ou l'organisme doit s'assurer que les renseignements bénéficieront d'une protection équivalente à celle prévue à la Loi sur l'accès ou, selon le cas, à la LSSSS. Cette équivalence de protection peut être démontrée par un avis juridique d'un cabinet d'avocats canadien, lequel devrait comporter une analyse comparative des dispositions de la Loi sur l'accès ainsi que, selon le cas, de la LSSSS et des lois, règlements, procédures, standards, directives, politiques ou documents de même nature du pays où les renseignements seront utilisés ou communiqués. L'équivalence de protection des renseignements personnels doit demeurer valide tant et aussi longtemps que des

données sont hébergées dans les lieux identifiés. À noter qu'à compter du 22 septembre 2023, cette équivalence devrait être directement produite lors l'évaluation des facteurs relatifs à la vie privées, qui devient obligatoire pour toute évolution ou pour toute nouvelle solution en RI.

1.6.2 Si l'actif est considéré comme moins sensible (profil A) (héberge des données jugées non sensibles) : concernant les renseignements personnels détenus, utilisés ou communiqués à l'extérieur du Québec, le MSSS ou l'organisme doit s'assurer qu'ils bénéficieraient d'une protection équivalente à celle prévue à la Loi sur l'accès. Ceci inclut tout lieu d'hébergement des données dont notamment les centres de données primaires et les centres de données de relève. Les lieux d'hébergement suivants sont d'emblée considérés offrir une protection équivalente, et en conséquence, autorisés[1] :

1. N'importe où au Canada ;
2. Tous pays membres de l'Union européenne ;
3. Tous pays ayant adopté ou inclus à sa législation, le Règlement général sur la protection des données (RGPD) ;
4. Tous pays ayant fait l'objet d'une décision d'adéquation par la Commission européenne

Au regard d'une entreprise visée par le Privacy Shield Framework et qui souhaitait héberger des données aux États-Unis, le fournisseur sera invité à démontrer au dirigeant de l'information du MSSS (DI) ou de l'organisme du RSSS (CSIO), l'équivalence de protection des renseignements personnels par un cabinet d'avocat canadien.

Cette démonstration de l'équivalence de protection des renseignements personnels s'effectue à la lumière de règles issues en grande partie des Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'Organisation de coopération et de développement économique (OCDE).

1.6.3 Lorsqu'un fournisseur souhaite offrir un actif au MSSS ou à un organisme du RSSS, celui-ci devrait fournir toutes les informations ou tous documents nécessaires, incluant un avis juridique d'un cabinet d'avocats canadien tel que mentionné à l'article 1.6.1, pour que le MSSS ou l'organisme puisse s'assurer de l'équivalence de protection des renseignements personnels des lieux identifiés.

1.7 Le choix d'une solution infonuagique doit se faire en privilégiant le type de solution selon l'ordre suivant :

1. Solution logicielle en tant que service (SaaS)
2. Plateforme en tant que service (PaaS)
3. Infrastructure en tant que service (IaaS) - natif
4. Infrastructure en tant que service (IaaS) - non-natif

1.8 L'utilisation des solutions répondant aux besoins d'affaires, présentes au catalogue infonuagique du MCN, est obligatoire.

- [1] Référence : guide_utilisateur_IaaS_PaaS_courtier_infonuagique.pdf (gouv.qc.ca)

1.9 Pour tout type de services (IaaS, PaaS et SaaS), l'organisme exprime ses besoins auprès du courtier en infonuagique du MCN.

Directive 2. Recours à des services infonuagiques externes – Solution logicielle en tant que service (SaaS) en priorité

2 L'organisme priorise les solutions toute faites et hébergées par le fournisseur, de type « solution logicielle en tant que services » ou « software as a service », aux autres modèles infonuagiques afin de répondre à son besoin d'affaires.

Précision à considérer :

2.1 Les profils A, B et C de l'analyse de préjudice sont acceptés dans ce type d'hébergement.

2.2 Une solution logicielle hébergée par le fournisseur, peu importe le modèle utilisé par le fournisseur, est considérée comme répondants aux critères SaaS.

2.3 Précision : Les solutions hébergés par un fournisseur privé ne doivent pas consommer les offres PaaS/IaaS au catalogue du MCN.

Directive 3. Recours à des services infonuagiques externes PaaS / IaaS

3 Les organismes doivent recourir et utiliser des services infonuagiques externes PaaS / IaaS qualifiés au catalogue du courtier en infonuagique du MCN pour répondre à leurs besoins.

Précision à considérer :

3.1 Les profils A et B.

3.2 Le MSSS et les organismes ont recours à l'approche infonuagique native en mode IaaS et PaaS.

Directive 4. Recours à des services infonuagiques gouvernementaux (PaaS / IaaS)

4 Les organismes doivent avoir recours aux services du nuage gouvernemental lorsque l'infonuagique externe ne répond pas aux contrôles de sécurité des données en lien avec la confidentialité de l'information.

Précision à considérer :

4.1 Le profil C seulement.

Directive 5. Recours à l'hébergement du MCN (Colocation)

5 Le gouvernement offre un service d'hébergement physique d'infrastructures technologiques à Québec et à Montréal, dans le respect des lois, des règlements et des politiques en vigueur au regard de ce type d'infrastructure. Le service assure l'attribution d'espace plancher pour accueillir les infrastructures technologiques dans les centres de traitement du MCN. Chaque entente fait l'objet d'une revue diligente pour tenir compte des besoins du client et pour établir la tarification appropriée.

Précision à considérer :

5.1 Seulement pour les solutions technologiques non supportées par les solutions infonuagiques (SaaS / PaaS / IaaS).

Directive 6. Utilisation des salles de proximité

6 L'utilisation des salles de proximité est possible pour les solutions technologiques non supportées par les solutions infonuagiques (directive 1, 2, 3 et 4) et qui ne peuvent être hébergées au MCN (directive 5), si et seulement si toutes les options d'hébergement précédentes ont démontré l'impossibilité pour les solutions de fonctionner à distance.

Précision à considérer :

6.1 Un formulaire de justification doit être rempli auprès du MCN.

Abréviations et acronymes

Le texte du document réfère à des abréviations et acronymes dont voici la description :

Abréviation ou acronyme	Description
CSIO	Chef de la sécurité de l'information organisationnelle
DI	Dirigeant de l'Information
IaaS	Infrastructure en tant que service
Loi sur l'accès	Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1)
LSSSS	Loi sur les services de santé et les services sociaux (RLRQ, chapitre S-4.2)
MCN	Ministère de la Cybersécurité et du Numérique
MSSS	Ministère de la Santé et des Services sociaux
OP	Organisme public
PaaS	Plateforme en tant que service
PCCTI	Programme de consolidation des centres de traitement informatique
RAMQ	Régie d'assurance maladie du Québec
RI	Ressources informationnelles
RGPD	Règlement général sur la protection des données
RPO	Perte de donnée maximale acceptable
RSSS	Réseau de la santé et des services sociaux
RTO	Durée maximale d'interruption acceptable
SaaS	Solution logicielle en tant que service
SCT	Secrétariat du Conseil du trésor
STNG	Stratégie de Transformation Numérique Gouvernementale

TI	Technologie de l'information

Le présent document est disponible en version électronique à l'adresse suivante : **http://www.ti.msss.gouv.qc.ca/Familles-de-services/Orientations-et-gouvernance.aspx**