



Résumé du dossier du patient pancanadien

Guide d'accompagnement : cas d'utilisation et définitions

Version : 1.0.0

Type : version de mise à l'essai

Date de la version : 17 octobre 2022



Table des matières

1 Introduction	3
2 Public cible	4
3 But	5
4 Le résumé du dossier du patient	6
4.1 Que sont l'IPS et le RDP-CA?.....	6
4.1.1 Quels problèmes règlent-ils?	6
4.2 Le résumé du dossier du patient, une priorité	6
4.2.1 Le rôle d'Inforoute	7
4.3 Quels sont les avantages concrets escomptés?	7
4.3.1 Retombées annuelles prévues	9
5 Cas d'utilisation	14
5.1 Index des cas d'utilisation.....	14
5.2 UC-01 : Le PS crée un RDP-CA.....	15
5.3 UC-02 : Le PS visualise/consomme un RDP-CA.....	19
5.4 UC-03 : Le patient visualise/consomme un RDP-CA	21
6 Définition des exigences	25
6.1 Structure des exigences.....	25
6.2 Identification des exigences	26
6.3 Exigences pour les tests d'interopérabilité.....	27
6.4 Exigences d'orientation et de soutien	30
6.5 Exigences : série complète.....	34
6.5.1 Exigences opérationnelles et juridiques.....	34
6.5.2 Exigences syntaxiques et sémantiques	41
6.5.3 Exigences techniques	42

1 Introduction

Le Guide d'accompagnement : cas d'utilisation et définitions du résumé du dossier du patient pancanadien, qui accompagne la spécification d'interopérabilité du RDP-CA, présente le contexte global des considérations d'ordre clinique et administratif, de l'interopérabilité et du développement de solutions qui se sont présentées durant l'élaboration du RDP-CA. Il définit le problème lié aux soins de santé que le RDP-CA vient pallier et inclut des cas d'utilisation et des exigences d'interopérabilité qui peuvent être reliés au contenu du Guide d'accompagnement de l'architecture de référence du RDP-CA, qui définit les acteurs et leurs interactions avec d'autres acteurs, et du Guide d'implantation FHIR du RDP-CA, qui définit le contenu et l'interopérabilité sémantique du RDP-CA.

Le présent document appuiera aussi les versions suivantes et les prochains éléments de la feuille de route de la spécification RDP-CA.

2 Public cible

Le présent document s'adresse, sans s'y limiter, aux destinataires suivants :

- les décideurs qui ne s'occupent pas des aspects techniques;
- les services des TI des établissements de santé (gestionnaires de produit technique, gestionnaires en informatique, personnel opérationnel);
- le personnel technique des fournisseurs qui participent à l'initiative IHE;
- les experts qui participent à l'élaboration des normes;
- les professionnels de la santé qui participent à la création et à l'utilisation de résumés du dossier du patient;
- les personnes et les équipes responsables de l'implantation de solutions logicielles, comme les gestionnaires de projet, les chefs de la technologie, les chefs de la sécurité de l'information, les ingénieurs en logiciels, les gestionnaires de produit technique, les gestionnaires en informatique, le personnel opérationnel et d'autres professionnels du même type.

3 But

Le but du présent document est de présenter les cas d'utilisation et les définitions du projet de résumé du dossier du patient pancanadien (RDP-CA), dont les suivants :

- la définition du RDP-CA;
- les avantages et la valeur cliniques du RDP-CA, tels que décrits par les professionnels de la santé canadiens;
- les cas d'utilisation et les scénarios;
- les exigences d'interopérabilité et les exigences relatives à la solution, regroupées dans les catégories suivantes :
 - opérationnelles et juridiques;
 - syntaxiques et sémantiques;
 - techniques.

4 Le résumé du dossier du patient

4.1 Que sont l'IPS et le RDP-CA?

L'**IPS (International Patient Summary, ou résumé international du dossier médical du patient)** est un extrait du dossier de santé électronique qui contient des renseignements médicaux essentiels sur un patient (sujet de soins). Il représente un ensemble minimal et non exhaustif de données pertinentes et normalisées sur un patient, toutes maladies et toutes spécialités confondues, que tous les cliniciens peuvent utiliser pour la prestation de soins (transfrontaliers) non planifiés. Bien qu'il soit axé sur les soins transfrontaliers non planifiés, il fournit aussi des solutions génériques et potentiellement réutilisables qui peuvent être appliquées n'importe où dans le monde.

Les profils normalisés (ou la spécification) du **résumé du dossier du patient pancanadien (RDP-CA)** s'appuient sur les principes de l'IPS et (actuellement) ses ensembles de données pour créer un résumé du dossier du patient de base qui appuie la prestation de soins efficaces et de qualité dans le contexte canadien. Mise au point en collaboration avec les provinces et les territoires et leurs cliniciens, la spécification RDP-CA décrit les données indispensables pour les cliniciens, les normes de données (langage de données) dont tous les systèmes ont besoin pour communiquer et s'échanger des données et les méthodes normalisées d'échange de données, comme [CA:FeX](#) (échange FHIR canadien).

4.1.1 Quels problèmes règlent-ils?

Même à l'ère de la santé numérique, en raison des incompatibilités entre les systèmes et du manque d'intégration et de transférabilité des données aux points d'intervention, les données se retrouvent souvent « enfermées » dans un système. Cela entraîne plusieurs problèmes :

1. Mis à part la consultation du médecin de famille (qui conserve la majeure partie des données primaires de ses patients), la plupart des autres épisodes de soins sont pris en charge sans accès aux données, ce qui augmente le risque d'effets secondaires ou indésirables des traitements et réduit inévitablement la qualité des soins.
2. Les longs délais d'attente pour obtenir un diagnostic quand l'information est manquante, inaccessible ou, parfois, inexacte, créent de la déception et de l'insatisfaction chez les patients.
3. Le temps que doivent passer des cliniciens déjà à bout de souffle pour trouver l'information nuit à la prestation des soins.
4. Les bailleurs de fonds sont incapables d'obtenir des renseignements opérationnels fiables pour prendre les meilleures décisions possibles en matière de financement.

Lorsque le langage de données, les éléments de données communs et les méthodes d'échange sont harmonisés et que les composantes techniques sont accessibles, l'information peut être échangée rapidement, efficacement et facilement, que ce soit à l'échelle régionale, provinciale ou territoriale, nationale ou internationale.

4.2 Le résumé du dossier du patient, une priorité

Le résumé du dossier du patient (RDP) est un contenant qui contient les domaines de données sur la santé les plus pertinents qui regroupent l'information sur le patient dans divers milieux de soins. Plus de 200 millions de transactions utilisant ces domaines passent par les systèmes de DME aux points d'intervention, dans les milieux de soins primaires et de soins actifs seulement; elles représentent la plus grande source de données des résumés médicaux des patients. Pour régler les problèmes mentionnés ci-dessus, il faut établir une solution permettant d'échanger les RDP.

Inforoute collabore depuis longtemps avec les provinces et les territoires pour transformer le réseau de la santé. Qu'il s'agisse de la transition du dossier papier au dossier électronique, des consultations en personne aux consultations virtuelles ou de la normalisation des données selon les normes internationales

(langage de données commun pour les systèmes), la prochaine étape critique consiste à libérer les données du patient. La pandémie a souligné à grands traits la nécessité de donner aux informations médicales une perspective non seulement locale ou nationale, mais aussi mondiale.

De nombreux gouvernements provinciaux et territoriaux l'ont également compris et ont mis le RDP sur leur liste de priorités. Comme nous l'avons toujours fait, nous continuerons de les soutenir et de nous aligner sur eux pour réaliser leurs objectifs et améliorer les soins de santé au Canada.

4.2.1 Le rôle d'Inforoute

Consciente du fait que les diverses spécialisations médicales au Canada ont le même contenu, mais des langages de données différents, Inforoute :

- collabore avec les provinces et les territoires et des intervenants clés pour regrouper les exigences;
- évalue le contenu existant pour définir et normaliser les éléments communs à l'échelle du pays et ainsi établir un profil de base pour tous;
- examine les profils de chaque administration pour s'assurer qu'ils sont alignés sur le profil commun;
- aligne les profils de base sur les normes internationales, y compris l'IPS;
- fournit une expertise et un leadership sur les exigences techniques et les normes de données (langage de données);
- représente le Canada dans la communauté internationale des normes de données et de l'interopérabilité, comme le GDHP et ses membres, IHE International et ses membres affiliés, pour promouvoir les spécifications internationales et des changements à la lumière des commentaires des intervenants;
- informe les fournisseurs des nouveaux profils et de la façon de les implanter;
- teste et note les implantations des fournisseurs en fonction de leur alignement sur les spécifications pancanadiennes publiées.

4.3 Quels sont les avantages concrets escomptés?

Le RDP-CA est un tremplin vers l'avenir. Il permet d'accéder aux données médicales les plus importantes aujourd'hui tout en laissant la porte ouverte à l'établissement d'écosystèmes modernes, « juste à temps » et sécurisés qui respectent la confidentialité des patients et permettent en même temps aux citoyens de participer à la prestation de leurs propres soins. Les normes communes qui s'appliquent au RDP, notamment la façon dont il est échangé, peuvent apporter de multiples avantages à différents intervenants, comme la capacité de créer un dossier patient unique longitudinal.

Intervenant	Avantages
Patients	<p>Amélioration de l'expérience des patients découlant de l'échange de données efficace et exhaustif entre professionnels de la santé (PS), ce qui donne lieu à de meilleurs résultats pour la santé.</p> <p>Capacité d'accéder à leurs propres renseignements médicaux et de les partager.</p>
Bailleurs de fonds en santé	<p>Réduction des coûts et du temps nécessaires pour implanter le RDP et les solutions d'interopérabilité en raison de l'accessibilité de contenu de données et de profils techniques réutilisables qui reflètent plus de 80 % des exigences communes.</p> <p>Disponibilité de rapports automatisés plus fiables pour mieux cibler les dépenses en santé selon les besoins.</p>

Provinces et territoires	<p>Réduction du fardeau de l'implantation grâce à une expertise centralisée dans des domaines spécialisés de l'interopérabilité et à des composantes de profil réutilisables, ce qui réduit par le fait même la demande de ressources.</p> <p>Capacité de réutiliser du contenu de données et des profils techniques qui reflètent plus de 80 % des exigences communes, et, par conséquent, diminution du temps nécessaire pour l'implantation.</p> <p>Meilleur potentiel d'évolutivité et d'amélioration des solutions de RDP moyennant un effort minimal, de façon que les fournisseurs puissent intégrer de nouveaux éléments sans être soumis à la surveillance des provinces et des territoires.</p>
Fournisseurs	<p>Capacité de réutiliser un grand nombre de composantes normalisées pour les implanter dans toutes les administrations sans devoir y apporter beaucoup de modifications.</p> <p>Réduction du temps nécessaire pour l'implantation.</p> <p>Réduction de la complexité et des ressources nécessaires grâce à une approche coordonnée pour toutes les administrations.</p> <p>L'alignement sur les normes mondiales est également bénéfique pour les fournisseurs étrangers, qui n'auront plus à adapter leurs solutions spécialement pour le Canada.</p>
Cliniciens/professionnels de la santé	<p>Meilleure communication entre les professionnels de la santé : Décloisonnement du réseau de la santé (p. ex. entre les milieux de soins actifs, primaires et spécialisés, soins de longue durée) pour permettre une coordination et des transitions des soins plus efficaces, ainsi qu'un meilleur soutien à la prise de décisions cliniques. De plus, la capacité de communiquer entre différentes solutions et entre différentes administrations facilite le cheminement des patients d'une province et d'un territoire à l'autre.</p> <p>Amélioration de l'expérience et de la satisfaction des professionnels de la santé : Des renseignements médicaux plus accessibles et mieux organisés leur font gagner beaucoup de temps, ce qui leur en laisse plus pour s'occuper de leurs patients. Quand ils ont moins de tâches administratives, que les flux de tâches sont plus efficaces et qu'ils utilisent plus efficacement leurs heures de consultation, les cliniciens sont moins à risque d'épuisement professionnel et ont plus de facilité à préserver un bon équilibre entre leur travail et leur vie personnelle.</p> <p>Amélioration de la qualité et de l'actualité des données : Des dossiers d'examen et de résultats de test clairs et uniformes permettent d'effectuer des investigations et des examens plus ciblés, et diminuent la probabilité qu'on demande au patient de subir des tests inutilement. Le fait d'avoir accès plus rapidement à de l'information plus exacte sur les antécédents médicaux du patient améliore sa sécurité et peut empêcher des préjudices, des retards dans la prestation des soins ou des traitements inappropriés.</p> <p>Soutien de la prestation des soins virtuels : Les professionnels de la santé qui utilisent différents modes/solutions de soins peuvent accéder aux mêmes informations sur un patient. L'accès uniforme à l'information</p>

	<p>et une meilleure communication facilitent également les consultations avec des professionnels de la santé inconnus du patient au point d'intervention (c'est-à-dire un professionnel qui traite, par l'intermédiaire d'une plateforme de télésanté, un patient qui n'a pas de médecin traitant).</p> <p>Meilleurs résultats pour la santé : L'accès uniforme à l'information médicale aide les cliniciens et les patients à prendre des décisions et favorise la prise en charge proactive de la santé. Une meilleure coordination et des transitions de soins plus efficaces contribuent à la sécurité des patients en leur permettant d'obtenir des soins plus rapidement, en réduisant le nombre d'analyses inutiles et en prévenant la prescription de médicaments ou de traitements contraindiqués. Les soins sont plus efficaces et sont donnés plus rapidement dans tous les milieux de soins.</p>
--	--

4.3.1 Retombées annuelles prévues

Une adoption de l'ordre de **50 %** devrait avoir les retombées annuelles suivantes :

- Transitions de soins **sûres et efficaces**
- **Réseau de la santé = 490 M\$** attribuables à l'amélioration des interactions en milieu de soins ambulatoires, au recours efficace à l'urgence, aux services aux patients hospitalisés et à la réduction du nombre d'analyses de laboratoire/d'imagerie diagnostique reprises inutilement
- **Canadiens = 448 M\$** grâce au temps gagné par les patients
- **Cliniciens = 328 M\$** grâce au temps gagné par les cliniciens

5 Cas d'utilisation

Le présent document décrit les cas d'utilisation et les scénarios de flux de tâches qui s'appliquent à l'échange d'un RDP entre différentes solutions. Comme l'implantation des éléments des cas d'utilisation pourrait varier d'une province et d'un territoire à l'autre, ceux-ci ne sont montrés qu'à titre d'exemples. Ils ne représentent pas toutes les options d'implantation possibles ni des choix d'implantation obligatoires. Ils décrivent les interactions générales entre un PS, son système de dossiers de santé et d'autres systèmes de dossiers de santé, ainsi que les échanges ou la « conversation » entre un système et ses utilisateurs (participants). À noter qu'un « participant » peut être une personne (p. ex. PS, patient) ou un système (p. ex. DME, dépôt de DSE). Les interactions sont définies en détail dans le Guide d'accompagnement de l'architecture de référence du RDP-CA.

Chaque cas d'utilisation comprend :

- un scénario;
- des exemples de déclencheurs, de préconditions et de postconditions;
- une description des participants (personnes et systèmes);
- un diagramme des interactions entre les participants;
- les étapes qui correspondent au diagramme et les autres flux possibles; et
- un renvoi aux exigences opérationnelles correspondantes.

5.1 Index des cas d'utilisation

La présente section propose une liste de cas d'utilisation qui ont été jugés prioritaires au terme de l'analyse de l'environnement pancanadien. Par la suite, en collaboration avec les provinces et les territoires participants, on en a précisé la portée et les priorités pour les versions initiales et les versions subséquentes.

La présente version de la spécification RDP-CA couvre les cas d'utilisation UC-01, UC-02 et UC-03.

La liste ci-dessous contient l'identifiant, le nom et la description des cas d'utilisation. Pour chaque cas d'utilisation, vous trouverez une liste des provinces et des territoires qui ont indiqué que celui-ci fera partie de la version 1 ou de versions subséquentes de leur RDP.

ID du cas d'utilisation	Nom	Description	Indiqué par
UC-01	Le PS crée un RDP-CA	Un PS, dans n'importe quel milieu de soins, crée un RDP afin qu'il soit utilisé au point d'intervention, et les consommateurs de RDP y ont accès.	AB, CB, TNL, ON, SK
UC-02	Le PS visualise/consomme un RDP-CA	Un PS, dans n'importe quel milieu de soins, visualise et utilise un RDP-CA au point d'intervention.	AB, CB, TNL, ON, SK
UC-03	Le patient visualise/consomme un RDP-CA	Un patient ou un sujet de soins accède à son RDP-CA pour le visualiser ou en obtenir une copie.	AB, CB, TNL, ON

① VERSIONS FUTURES

En plus des cas d'utilisation retenus pour la présente version de la spécification RDP-CA, on en a relevé d'autres pour un examen ultérieur. Les cas d'utilisation UC-04, UC-05 et UC-06 seront pris en considération pour des versions subséquentes prévues dans la feuille de route de la spécification RDP-CA.

ID du cas d'utilisation	Nom	Description	Indiqué par
UC-04	Le PS envoie le RDP-CA à un autre PS dans le cadre d'un flux de tâches cliniques (p. ex. demande de consultation électronique)	Un PS crée/produit un RDP-CA et l'envoie avec d'autres documents cliniques dans le cadre d'un flux de tâches cliniques (p. ex. demande de consultation, consultation entre PS, etc.).	AB, CB, TNL, ON, SK
UC-05	Le patient transmet son RDP-CA à un PS	Un patient ou un sujet de soins transmet son RDP-CA à un PS, qui peut le visualiser/consommer pour soutenir le traitement.	AB, CB, TNL, ON, SK
UC-06	Le PS demande l'assemblage d'un RDP-CA sur demande	Un PS, dans n'importe quel milieu de soins, demande l'accès à un RDP-CA assemblé sur demande en temps réel pour l'utiliser au point d'intervention ou dans le cadre d'un flux de tâches cliniques (p. ex. demande de consultation).	ON

5.2 UC-01 : Le PS crée un RDP-CA

Description

Un PS, dans n'importe quel milieu de soins, crée un RDP afin qu'il soit utilisé au point d'intervention, et les consommateurs de RDP y ont accès.

Scénario

Un patient prend rendez-vous pour une consultation avec son médecin traitant, dans son centre de médecine familiale, parce qu'il est étourdi et a mal aux oreilles. Il mentionne que, depuis sa dernière consultation, le personnel d'une autre clinique lui a dit qu'il faisait de la haute pression (hypertension), et qu'il prend sa tension artérielle à la maison pour le moment. Il indique aussi qu'on soupçonne une allergie à la pénicilline. Le médecin détermine que le patient a une infection de l'oreille externe (otite externe) et lui prescrit des antibiotiques. Il crée une note clinique dans son DME, laquelle pourrait déclencher des mises à jour automatiques, par exemple aux données d'ordonnance. Il décide de créer un nouveau résumé du dossier pour ce patient (ou de remplacer le résumé existant, s'il y en a un) et de le transmettre au dépôt de DSE provincial ou territorial afin de le rendre accessible aux autres PS susceptibles de prodiguer des soins au patient.

Veillez noter que l'élément déclencheur de la création d'un nouveau RDP ou du remplacement d'un résumé existant pourrait être automatisé ou varier d'une solution à l'autre. Par exemple, la mise à jour de certains renseignements cliniques pourrait déclencher la mise à jour d'un RDP existant.

Déclencheurs, préconditions et postconditions

Les points suivants donnent des exemples de déclencheurs, de préconditions et de postconditions liés à la création d'un RDP. Ils ne couvrent pas tous les scénarios de flux de tâches qui pourraient être implantés dans les provinces et territoires.

Déclencheurs

- Le PS traite un patient et met à jour son dossier.
- Le PS reçoit d'autres renseignements concernant un patient. Par exemple, il reçoit les résultats d'analyses d'un patient, met à jour la liste des problèmes de santé d'un patient ou ajoute une note clinique, ce qui déclenche la création d'un nouveau RDP.

Préconditions

- Le RDP porte un ID unique associé au patient (p. ex. ID du registre des clients) pour être partagé entre les différents systèmes provinciaux/territoriaux.
- Dans les provinces et territoires où il faut obtenir le consentement explicite du patient pour partager son résumé du dossier :
 - Le patient donne ou a déjà donné son consentement au versement de son information clinique dans le DSE.

Postconditions

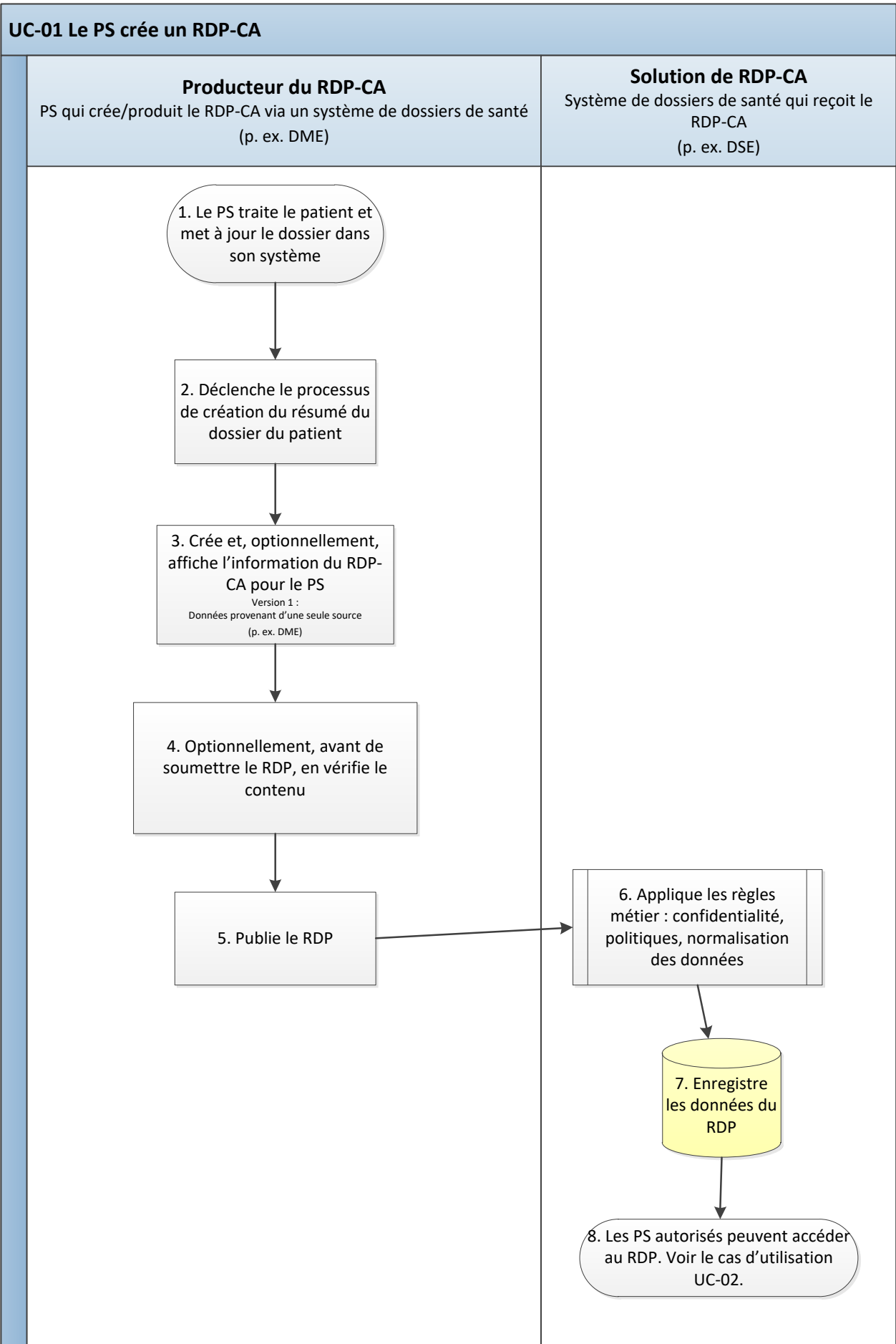
- Le nouveau RDP est enregistré dans la solution qui reçoit le RDP-CA et pourrait, s'il y a lieu, remplacer un RDP existant (p. ex. selon les règles provinciales/territoriales comme lorsque, par exemple, il s'agit du même patient, du même PS et du même endroit).
- Les PS autorisés peuvent visualiser le nouveau RDP ou recevoir une notification selon laquelle un nouveau RDP est disponible pour le patient.

Cas d'utilisation – participants et diagramme

Les participants du cas d'utilisation UC-01 sont les suivants :

- producteur de RDP-CA (PS qui crée/produit un RDP-CA via un système de dossiers de santé)
- solution de RDP-CA (système de dossiers de santé qui reçoit le RDP-CA)

Le diagramme du cas d'utilisation suivant représente les participants et leur rôle dans le cas d'utilisation et donne une vue générale du flux d'information.



Cas d'utilisation – flux primaire

Voici la description textuelle des étapes du diagramme du cas d'utilisation :

1. Le PS traite le patient et met à jour son dossier dans son système de dossiers de santé (p. ex. dossier médical électronique (DME), système d'information sur la santé (SIS)).
2. Le PS détermine qu'un nouveau RDP devrait être créé et demande au système de dossiers de santé (p. ex. DME) de créer l'information du RDP.
3. Le système de dossiers de santé (p. ex. DME, SIS) extrait de son système l'information à inclure dans le RDP (le DME crée un RDP uniquement à partir des données du dossier du patient qu'il contient).
4. Le PS, optionnellement, examine et valide le RDP avant de le transmettre/publier.
5. Le PS envoie/publie le RDP au système de dossiers de santé (p. ex. DSE).
6. Le système de dossiers de santé qui reçoit le RDP (ou la couche de traitement des données, comme le centre informatique provincial ou territorial) applique les règles métier (p. ex. normalisation des données, confidentialité, politiques, etc.).

Par exemple :

- a. Il valide les données du RDP (p. ex. le PS est identifié et peut soumettre un RDP, le patient est identifié, etc.)
- b. Il vérifie s'il existe déjà un RDP pour le même patient/PS – application des règles de remplacement/d'archivage
7. Le système de dossiers de santé qui reçoit le RDP l'enregistre.
8. Le RDP est accessible aux PS autorisés (voir le cas d'utilisation UC-02 : Le PS visualise/consomme un RDP-CA).

Cas d'utilisation – autres flux

Voici les autres flux qui pourraient se produire dans le cas d'utilisation UC-01.

- Étape 4 : Le PS peut sauter l'étape de la vérification du RDP, ce qui permet au système de dossiers de santé de transmettre/publier automatiquement le RDP au système de dossiers de santé destinataire.
- Étape 4 : Après avoir vérifié le RDP, le PS décide de modifier des renseignements médicaux contenus dans son dossier de santé avant de publier le RDP. Si les modifications ont une incidence sur le contenu du RDP, un nouveau RDP sera créé.
- Étape 4 : Après avoir examiné le RDP, le PS décide de retenir une partie ou la totalité de l'information contenue dans le RDP pour ne pas qu'elle soit transmise/publiée dans un autre système de dossiers de santé.
- Étape 5 : Après avoir soumis le RDP, le PS se rend compte qu'il y a des renseignements erronés ou manquants. Le PS pourra créer et publier un nouveau RDP pour remplacer le précédent.
- Étape 5 : Après avoir soumis le RDP, le PS se rend compte qu'il contient des renseignements erronés ou qu'il concerne un autre patient. Le PS pourra retirer/supprimer le plus récent RDP qu'il a soumis pour les mêmes patient, professionnel et lieu.
 - **Note** : Les règles métier relatives à la façon dont un système de gestion de documents gère les documents qu'il reçoit (p. ex. situations dans lesquelles un document peut être supprimé, durée de l'archivage, moment où le système devrait alerter les utilisateurs de l'ajout de nouvelles informations, etc.) ne font pas partie de la présente spécification RDP-CA. D'autres cas d'utilisation et règles métier seront abordés dans des versions ultérieures de la spécification RDP-CA. La présente version constitue le fondement technique sur lequel pourront s'appuyer les nouveaux cas d'utilisation.

5.3 UC-02 : Le PS visualise/consomme un RDP-CA

Description

Un PS, dans n'importe quel milieu de soins, visualise et utilise un RDP-CA au point d'intervention.

Scénario

Un patient prend rendez-vous pour une consultation avec un PS, à l'extérieur de son centre de médecine familiale, parce qu'il est étourdi et a mal aux oreilles. Il mentionne qu'il a un médecin traitant dans son centre de médecine familiale, qu'il fait de la haute pression (hypertension), et qu'il prend sa tension artérielle à la maison pour le moment. Le PS recueille les renseignements du patient et lance une recherche dans sa solution de RDP-CA pour voir s'il n'existerait pas déjà un RDP (il lance une recherche dans son réseau pour déterminer si un RDP a été créé et partagé par un autre PS). Après avoir trouvé un RDP associé à son patient, le PS visualise et utilise l'information qu'il renferme pour traiter le patient.

Déclencheurs, préconditions et postconditions

Les points suivants donnent des exemples de déclencheurs, de préconditions et de postconditions liés à la création du RDP. Ils ne couvrent pas tous les scénarios de flux de tâches qui pourraient être implantés dans les provinces et territoires.

Déclencheurs

- Le PS recueille toute l'information possible sur son patient pour le traiter.
- Le PS reçoit une notification l'avisant que de nouveaux renseignements médicaux sont accessibles au sujet du patient (si le PS a demandé à recevoir de telles notifications pour ce patient).

Préconditions

- Dans les provinces et territoires où le patient a appliqué une directive de consentement à son RDP, le PS se conforme aux politiques de confidentialité en vigueur.

Postconditions

- Le PS visualise et utilise le RDP pour traiter le patient.

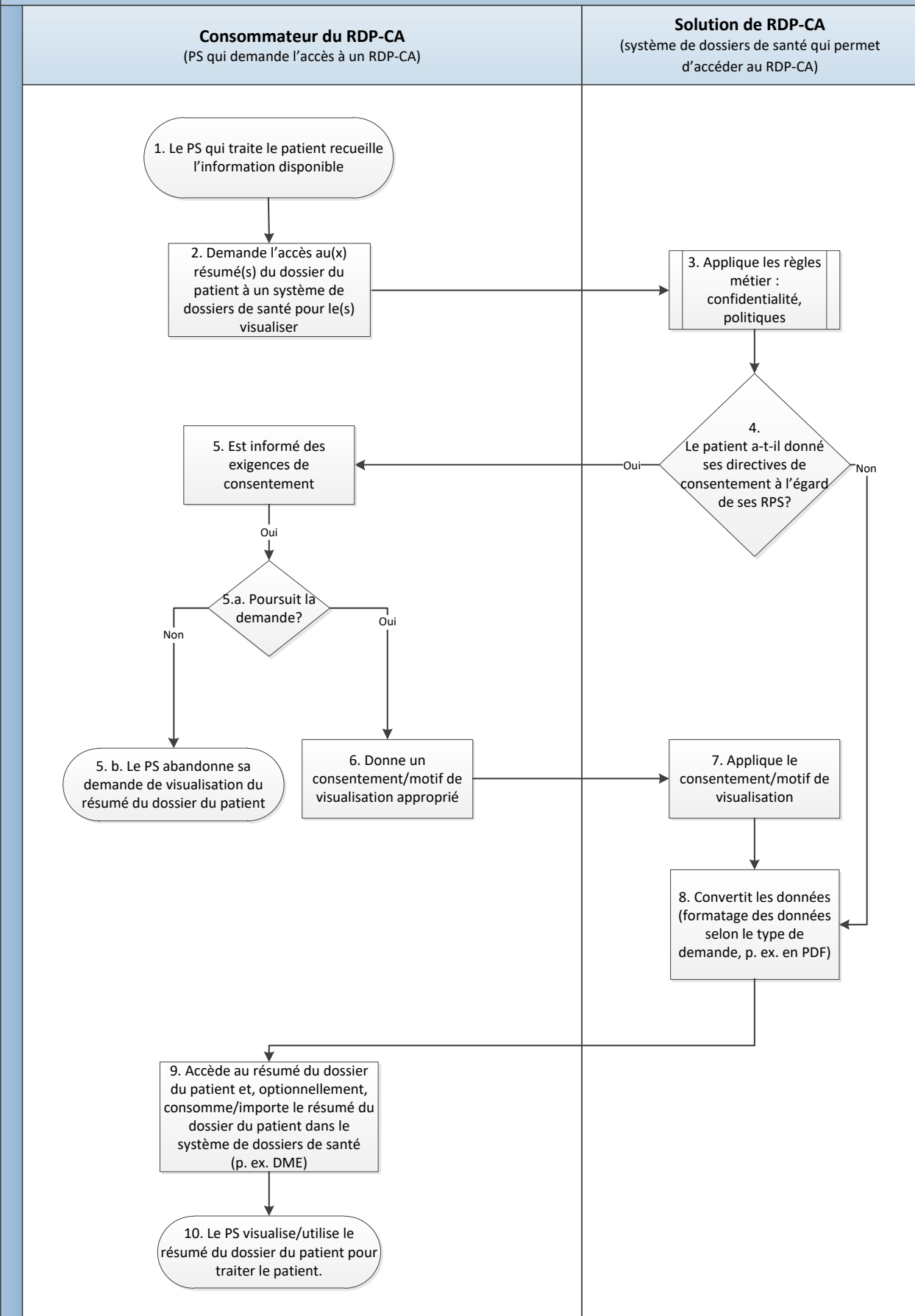
Cas d'utilisation – participants et diagramme

Les participants du cas d'utilisation UC-02 sont les suivants :

- consommateur de RDP-CA (PS qui demande l'accès à un RDP-CA)
- solution de RDP-CA (système de dossiers de santé qui donne accès au RDP-CA)

Le diagramme du cas d'utilisation suivant représente les participants et leur rôle dans le cas d'utilisation et donne une vue générale du flux d'information.

UC-02 Le PS visualise/consomme un RDP-CA



Cas d'utilisation – flux primaire

Voici la description textuelle des étapes du diagramme du cas d'utilisation :

1. Le PS qui traite le patient recueille des renseignements sur le patient et d'autres informations qui pourraient se trouver dans la solution de RDP-CA (p. ex. système de dossiers de santé comme un DSE).
2. Le PS demande à la solution de RDP-CA de lui accorder l'accès pour visualiser un RDP existant pour son patient.
3. La solution de RDP-CA applique les règles métier/de confidentialité/les politiques applicables (p. ex. règles de confidentialité relatives au consentement).
4. La solution de RDP-CA détermine si des directives de consentement du patient s'appliquent au RDP. S'il y en a, on passe à l'étape 5. S'il n'y en a pas, on passe à l'étape 8.
5. Le PS se voit présenter les directives de consentement du patient dans son système de dossiers de santé (p. ex. DME).
 - a. Le PS poursuit-il sa demande de visualisation du RDP? Si oui, on passe à l'étape 6. Si non, on passe à l'étape 5.b.
 - b. Le PS abandonne sa demande de visualisation du RDP. Le processus est terminé. (Voir l'autre flux pour l'étape 5.b.)
6. Le PS respecte les politiques de confidentialité locales/provinciales/territoriales (p. ex. donne un code de motif de visualisation du RDP).
7. La solution de RDP-CA applique l'information relative aux politiques de confidentialité locales/provinciales/territoriales fournie par le PS (p. ex. enregistre le code de motif de visualisation du RDP).
8. La solution de RDP-CA convertit les données et accorde l'accès pour la visualisation/consommation du RDP (p. ex. accorde l'accès pour la visualisation des RPS en format PDF).
9. Le PS obtient l'accès au RDP et, optionnellement, consomme l'information dans son système de dossiers de santé.
10. Le PS visualise/utilise le plus récent RDP disponible pour traiter le patient.

Cas d'utilisation – autre flux

Voici l'autre flux qui pourrait se produire dans le présent cas d'utilisation.

- Étape 5.b. Le PS n'est pas autorisé à visualiser le RDP. Le processus prend fin, et le PS n'a pas accès au RDP. Le PS pourrait aussi recueillir d'autres renseignements auprès du patient.

5.4 UC-03 : Le patient visualise/consomme un RDP-CA

Description

Un patient ou un sujet de soins accède à son RDP-CA pour le visualiser ou en obtenir une copie.

Scénario

Un patient, ou son proche aidant désigné, aimerait accéder aux renseignements médicaux qui figurent dans son RDP pour jouer un rôle actif dans ses soins de santé.

Veuillez noter qu'une instance provinciale ou territoriale pourrait choisir de présenter aux patients une version du RDP différente de celle que voient les PS. Par exemple, la version patient du RDP pourrait utiliser un vocabulaire plus adapté aux patients, et certaines informations pouvant nuire au patient pourraient être caviardées (par exemple, dans le cas de patients qui suivent une thérapie comportementale).

Déclencheurs, préconditions, postconditions

La présente section donne des exemples de déclencheurs, de préconditions et de postconditions liés à la création du RDP. Elle ne couvre pas tous les scénarios de flux de tâches qui pourraient être implantés dans les provinces et les territoires.

Déclencheurs

- Le patient, ou son proche aidant désigné, visualise le RDP pour se tenir au courant.
- Le patient aimerait obtenir une copie de son RDP pour l'apporter en voyage.
- Le patient aimerait obtenir une copie de son RDP pour le transmettre à un autre PS.

Préconditions

- Un système clinique auquel le patient a accès est en place dans la province ou le territoire.
- Un RDP a été créé pour le patient (voir les cas d'utilisation UC-01 et UC-06). Veuillez noter que le RDP qui est assemblé pour un patient pourrait contenir un ensemble de données différent/modifié par rapport à celui qui est assemblé pour un PS.
- Le patient a créé un compte personnel avec un nom d'utilisateur/mot de passe dans le système clinique provincial/territorial (p. ex. portail-patient).
- S'il y a lieu, le patient a autorisé un proche aidant à accéder à son dossier médical.
- Le patient, ou son proche aidant désigné, a ouvert une session dans le système clinique provincial/territorial (p. ex. portail-patient).

Postconditions

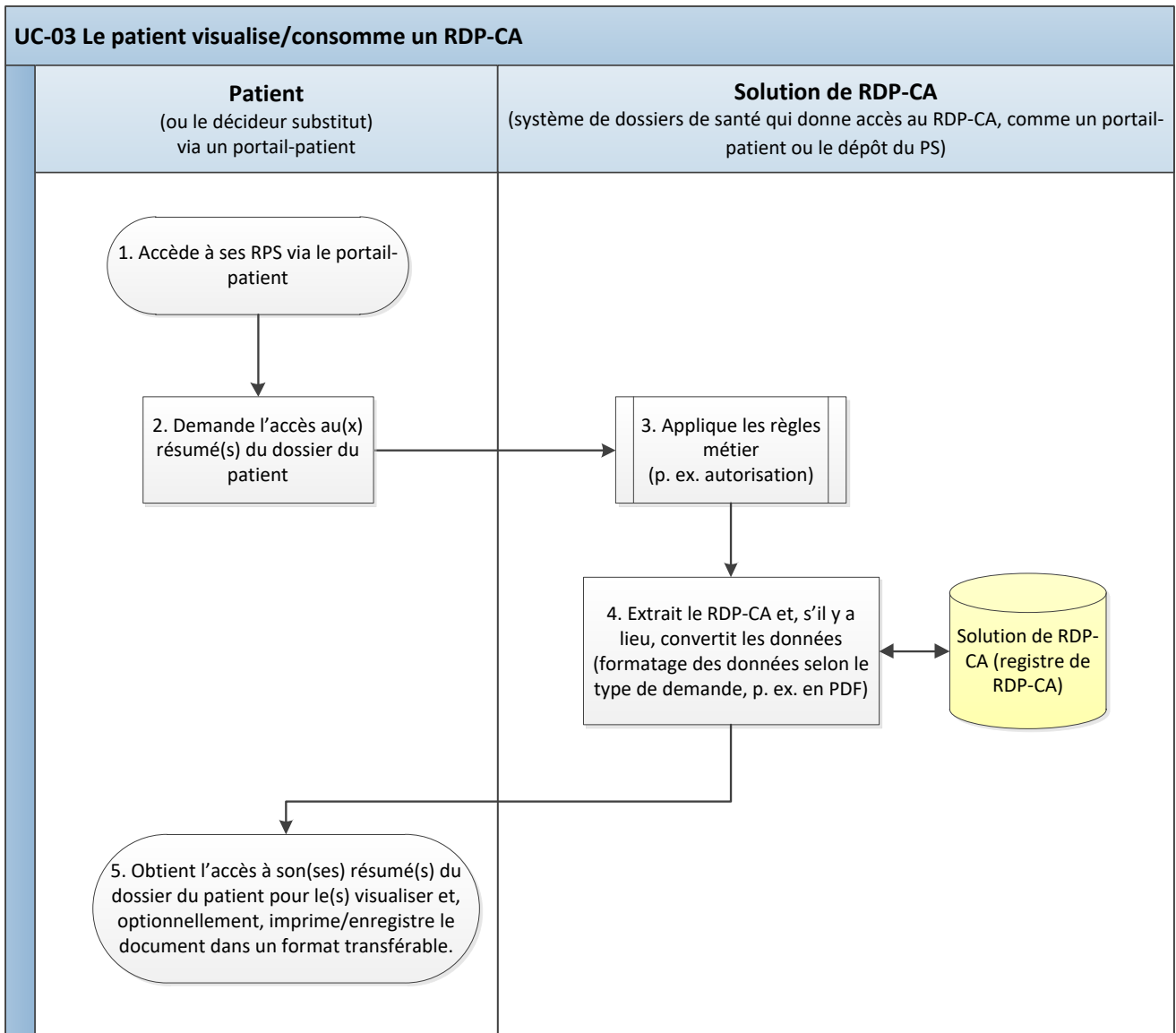
- Le patient, ou son proche aidant désigné, a accédé à son RDP et l'a visualisé.
- Optionnellement, le patient, ou son proche aidant désigné, a obtenu une copie (téléchargement ou impression du rapport) de son RDP.
- Le patient, ou son proche aidant désigné, transmet son RDP à un autre PS pour assurer la continuité des soins (voir le cas d'utilisation UC-05, où le patient transmet son RDP à un PS dans une autre province ou un autre territoire).

Cas d'utilisation – participants et diagramme

Les participants du présent cas d'utilisation sont les suivants :

- le patient/sujet de soins, via le portail-patient
- la solution de RDP-CA (p. ex. DSP)

Le diagramme du cas d'utilisation suivant représente les participants et leur rôle dans le cas d'utilisation ainsi qu'une vue générale du flux d'information.



Cas d'utilisation – flux primaire

Voici la description textuelle des étapes du diagramme du cas d'utilisation :

1. Le patient/sujet de soins accède à ses renseignements personnels sur la santé via un portail-patient.
2. Le patient/sujet de soins ou le décideur substitut demande l'accès pour visualiser son(ses) RDP.
3. La solution de RDP-CA (p. ex. DSP) applique les règles métier/politiques en vigueur (validation des données de connexion du patient).
4. La solution de RDP-CA (p. ex. DSP) extrait le RDP-CA (dans une mémoire locale ou dans un registre externe de RDP-CA). S'il y a lieu, la solution de RDP-CA pourrait convertir les données, notamment en formatant l'information en PDF.
5. Le patient/sujet de soins obtient l'accès à son(ses) RDP et, optionnellement, imprime/enregistre le document dans un format transférable.

Cas d'utilisation – autre flux

Voici un autre flux qui pourrait se produire dans le cas d'utilisation UC-02.

- Un décideur substitut qui possède les autorisations nécessaires accède au RDP ou l'obtient.

6 Définition des exigences

La présente section regroupe les exigences d'interopérabilité et les exigences liées aux solutions qui appuient la spécification d'interopérabilité du RDP-CA. Ces exigences sont les suivantes :

- les exigences d'interopérabilité, qui peuvent être testées/validées par des activités de prototypage; et
- un vaste ensemble d'exigences à prendre en considération ou destinées à guider les responsables de l'implantation du RDP-CA. Par exemple, des exigences complémentaires pourraient renvoyer à des politiques et/ou des normes locales/provinciales/territoriales, et le responsable de l'implantation devrait donc vérifier si certaines exigences sont nécessaires dans une province ou un territoire.

Les exigences représentent une expression normalisée des interactions entre les acteurs, les entités et l'utilisateur et le système, qui seront mieux définies dans le Guide d'accompagnement de l'architecture de référence du RDP-CA. Les définitions des termes utilisés dans les exigences se trouvent dans le [Glossaire des termes et abréviations](#) de la spécification RDP-CA.

D'autres exigences pourraient s'ajouter et être incluses dans des versions subséquentes de la spécification RDP-CA.

6.1 Structure des exigences

Les exigences ont été regroupées dans trois catégories (opérationnelles/juridiques, syntaxiques et sémantiques, techniques) et deux sous-catégories (interopérabilité et solutions), et selon trois types de priorité (doit, devrait et pourrait), qui sont décrits dans le tableau suivant :

Catégories d'exigences	
Exigences opérationnelles/juridiques	<ul style="list-style-type: none"> • Conditions permettant à des organisations indépendantes les unes des autres d'exécuter un processus ou de fournir un service en collaboration.
Exigences syntaxiques/sémantiques	<ul style="list-style-type: none"> • Conditions syntaxiques et sémantiques nécessaires pour que les données échangées entre les systèmes de dossiers médicaux puissent être interprétées correctement et que leur signification puisse être établie sans ambiguïté.
Exigences techniques	<ul style="list-style-type: none"> • Conditions requises pour qu'un système de dossiers médicaux transmette des données à un autre système de dossiers médicaux et pour que le système récepteur accuse réception des données utiles.
Sous-catégories d'exigences	
Exigences d'interopérabilité	<ul style="list-style-type: none"> • Conditions requises pour qu'un système informatique transmette des données à un autre système informatique et pour que le système récepteur accuse réception des données utiles. • Conditions syntaxiques et sémantiques nécessaires pour que les données échangées entre les systèmes informatiques puissent

	<p>être interprétées correctement et que leur signification puisse être établie sans ambiguïté.</p> <ul style="list-style-type: none"> • Conditions permettant à des organisations indépendantes les unes des autres d'exécuter un processus ou de fournir un service en collaboration.
Exigences liées aux solutions	<ul style="list-style-type: none"> • Longue liste d'exigences dont disposent les administrations pour conceptualiser la façon dont les systèmes et les solutions disponibles sur le marché peuvent être utilisés pour créer/produire, communiquer, échanger et consulter/consommer des RDP selon la norme du RDP-CA. • Les exigences peuvent soutenir le développement de solutions et dépasser le cadre des exigences d'interopérabilité. • Les politiques provinciales/territoriales peuvent donner d'autres définitions de ces exigences.
Priorité des exigences	
Doit	<ul style="list-style-type: none"> • Désigne un élément obligatoire ou requis, qui doit impérativement être respecté.
Devrait	<ul style="list-style-type: none"> • Désigne un élément recommandé, c'est-à-dire dont l'implantation est considérée comme une bonne pratique, mais sans être obligatoire (facultatif).
Pourrait	<ul style="list-style-type: none"> • Désigne un élément optionnel dont l'implantation est permise, mais pas obligatoire.
Ne doit pas	<ul style="list-style-type: none"> • Désigne une action ou un élément interdit/non autorisé.

6.2 Identification des exigences

Chaque exigence est identifiée par les éléments suivants :

- Identifiant : Les trois premiers caractères de l'identifiant de l'exigence (BRn^o) représentent la catégorie, et les trois chiffres suivants représentent le numéro de l'exigence dans la catégorie.
Exemple :
 - **BR1-001** = Première exigence de la catégorie des exigences opérationnelles/juridiques
 - **BR2-001** = Première exigence de la catégorie des exigences syntaxiques/sémantiques
 - **BR3-001** = Première exigence de la catégorie des exigences techniques
- Définition
- Sous-catégorie : Interopérabilité ou solutions
- Type (priorité) : Obligatoire, recommandée ou optionnelle

6.3 Exigences pour les tests d'interopérabilité

Les tableaux suivants contiennent une série d'exigences d'interopérabilité qui seront testées dans le cadre des tests de la spécification d'interopérabilité du RDP-CA.

Note : Certaines des exigences incluses dans la section Exigences d'orientation et de soutien pourraient être précisées dans de futures versions de la spécification RDP-CA et être reclassées dans la catégorie Exigences pour les tests d'interopérabilité.

Exigences opérationnelles/juridiques : Exigences pour les tests d'interopérabilité

Le tableau suivant contient un sous-ensemble des exigences d'interopérabilité opérationnelle/juridique qui seront testées pour la présente version.

ID	Description	Type	Sous-catégorie
BR1-05	Une solution de RDP-CA doit permettre à un consommateur de RDP autorisé (PS autorisé) de déterminer la provenance (auteur, producteur, date et sujet de soins du RDP-CA) d'un RDP courant et antérieur.	Obligatoire	Interopérabilité
BR1-11	Une solution de RDP-CA doit limiter l'échange de renseignements médicaux à ce qui est cliniquement nécessaire et suffisant, conformément à la législation applicable et à la spécification RDP-CA. Note : Par exemple, le clinicien pourra créer le RDP-CA avec un sous-ensemble des domaines de données défini dans la spécification d'interopérabilité du RDP-CA.	Obligatoire	Interopérabilité
BR1-13	Une solution de RDP-CA doit donner au patient/sujet de soins un droit d'accès à son RDP conformément aux politiques et aux dispositions législatives de la province ou du territoire.	Obligatoire	Interopérabilité
BR1-14	Une solution de RDP-CA doit limiter l'accès aux producteurs et aux consommateurs de RDP-CA autorisés.	Obligatoire	Interopérabilité

Exigences syntaxiques et sémantiques : Exigences pour les tests d'interopérabilité

Le tableau suivant contient un sous-ensemble des exigences d'interopérabilité syntaxique et sémantique qui seront testées pour la présente version.

ID	Description	Type	Sous-catégorie
----	-------------	------	----------------

BR2-01	Une solution de RDP-CA doit permettre à un PS autorisé de créer/produire un RDP fondé sur le Guide d'implantation FHIR du RDP-CA.	Obligatoire	Interopérabilité
BR2-02	Une solution de RDP-CA doit respecter les normes d'interopérabilité syntaxique, sémantique/terminologique et de contenu établies dans le Guide d'implantation FHIR du RDP-CA.	Obligatoire	Interopérabilité

Exigences techniques : Exigences pour les tests d'interopérabilité

Le tableau suivant contient un sous-ensemble des exigences d'interopérabilité technique qui seront testées pour la présente version.

ID	Description	Type	Sous-catégorie
BR3-01	Une solution de RDP-CA doit permettre de consigner et de communiquer l'identité du sujet de soins du RDP.	Obligatoire	Interopérabilité
BR3-02	Une solution de RDP-CA doit permettre de consigner et de communiquer l'identité de l'auteur autorisé du RDP-CA.	Obligatoire	Interopérabilité
BR3-04	Une solution de RDP-CA doit permettre de visualiser les différentes versions d'un RDP et de fournir une version antérieure sur demande, conformément aux politiques provinciales/territoriales.	Obligatoire	Interopérabilité
BR3-05	Une solution de RDP-CA pourrait permettre de produire un RDP-CA dans un format transférable (p. ex. PDF) accessible aux patients/sujets de soins.	Optionnelle	Interopérabilité
BR3-08	Une solution de RDP-CA doit protéger les renseignements médicaux en transit, conformément aux normes de cryptage provinciales/territoriales. Note : Par exemple, les normes de cryptage provinciales/territoriales devraient porter sur des concepts d'algorithmes et de protocoles cryptographiques, ainsi que sur la gestion des clés de cryptage durant la transmission des RPS pour maintenir la confidentialité et l'intégrité du RDP.	Obligatoire	Interopérabilité
BR3-13	Une solution de RDP-CA doit permettre d'identifier un RDP-CA par un identifiant unique.	Obligatoire	Interopérabilité
BR3-16	Une solution de RDP-CA doit créer le RDP-CA	Obligatoire	Interopérabilité

dans un format structuré conforme à la norme
FHIR R4 (v4.0.1) + JSON et XML.

6.4 Exigences d'orientation et de soutien

Les tableaux qui suivent présentent un vaste ensemble d'exigences d'interopérabilité et d'exigences liées aux solutions **à prendre en considération ou destinées à guider** les responsables de l'implantation du RDP-CA. Ces exigences ne feront pas partie des exigences testables pour la présente version.

Note : Certaines des exigences de soutien pourraient être précisées dans de futures versions de la spécification RDP-CA et recatégorisées comme des exigences testables.

Exigences opérationnelles/juridiques : Exigences d'orientation et de soutien

ID	Description	Type	Sous-catégorie
BR1-01	Une solution de RPD-CA devrait permettre le versionnage, le stockage, la conservation, la destruction et l'archivage des RDP produits et consommés par des utilisateurs autorisés du système conformément aux politiques provinciales/territoriales.	Recommandée	Solutions
BR1-02	Une solution de RDP-CA devrait donner à un PS la possibilité de vérifier et d'approuver le contenu du RDP avant qu'il soit accessible aux consommateurs de RDP-CA. Note : Si le PS détermine que des modifications doivent être apportées au RDP avant de l'approuver, il les apporte dans le dossier du patient. Si les changements ont une incidence sur le contenu du RDP, le PS créera un nouveau RDP qu'il vérifiera et approuvera ensuite.	Recommandée	Solutions
BR1-03	Une solution de RDP-CA doit permettre à un PS d'invalider un RDP s'il détermine qu'il a été entré par erreur ou qu'il est invalide, conformément aux politiques provinciales/territoriales.	Obligatoire	Interopérabilité
BR1-04	Une solution de RDP-CA devrait respecter les règles de conservation des données établies par les politiques locales/provinciales/territoriales et les exigences du système.	Recommandée	Solutions
BR1-06	Une solution de RDP-CA pourrait permettre d'extraire et d'enregistrer des données discrètes d'un RDP si un utilisateur autorisé du système le demande.	Optionnelle	Solutions
BR1-07	Un auteur de RDP-CA devrait raisonnablement s'assurer que les renseignements médicaux qu'il contient sont exacts, suffisamment complets et à jour pour répondre à l'objectif clinique spécifié.	Recommandée	Solutions
BR1-08	Une solution de RDP-CA devrait pouvoir se conformer à une ordonnance de préservation de la preuve rendue par une entité autorisée,	Recommandée	Solutions

conformément aux politiques provinciales/territoriales.

*Note : Les politiques sur la préservation de la preuve empêchent l'élimination de toute information stockée électroniquement dans le RDP-CA qui pourrait être requise dans un litige.

BR1-09	Une solution de RDP-CA devrait pouvoir omettre ou masquer des données dans un RDP-CA conformément aux politiques sur la confidentialité locales/provinciales/territoriales.	Recommandée	Solutions
BR1-10	<p>Une solution de RDP-CA doit pouvoir produire un RDP qui respecte les directives de consentement du sujet de soins, conformément aux normes et politiques locales/provinciales/territoriales.</p> <p>Note : Par exemple, les normes locales/provinciales/territoriales pourraient comprendre l'association des directives de consentement aux RPS contenus dans le RDP, notamment sur des concepts comme le maintien de l'association, le traitement des directives de consentement, le blocage de la transmission des RPS contenus dans un RDP lorsque les directives de consentement sont violées ou qu'aucune exception à une divulgation n'est établie dans une loi ou une politique provinciale/territoriale, et la notification des demandeurs lorsque des données sont bloquées en raison de directives de consentement.</p>	Obligatoire	Interopérabilité
BR1-12	Une solution de RDP-CA doit pouvoir indiquer au consommateur de RDP-CA (p. ex. un PS) que de l'information sur le sujet de soins a été omise ou masquée conformément à des directives de consentement et des politiques provinciales/territoriales.	Obligatoire	Interopérabilité

Exigences techniques : Exigences d'orientation et de soutien

ID	Description	Type	Sous-catégorie
BR3-09	<p>Une solution de RDP-CA devrait respecter les normes minimales de l'industrie sur les mécanismes de contrôle de l'accès et de sécurité en fonction du rôle, notamment définir le niveau de sécurité et le profil d'autorisation de tous les acteurs autorisés et faire le mappage de chaque utilisateur avec un ou plusieurs rôles et de chaque rôle avec une ou plusieurs fonctions du système, selon les normes provinciales/territoriales et les exigences du système.</p> <p>Note : Par exemple, les normes provinciales/territoriales sur le contrôle de l'accès fondé sur le rôle devraient tenir compte de normes telles que ISO 22600-1:2014, qui décrit</p>	Recommandée	Solutions

les scénarios et les paramètres cruciaux de l'échange d'informations d'un domaine de politique à un autre, et ISO 22600-2:2014, qui décrit et explique de manière plus détaillée les architectures et les modèles sous-jacents de la gestion des privilèges et du contrôle d'accès nécessaires à la sécurisation de l'échange de données incluant la représentation formelle des politiques.

BR3-06	Une solution de RDP-CA devrait respecter les normes minimales locales/provinciales/territoriales relativement à l'authentification (p. ex. authentification multifactorielle) des utilisateurs autorisés.	Recommandée	Solutions
--------	---	-------------	-----------

BR3-07	Une solution de RDP-CA devrait, lorsque c'est possible, séparer les fonctions et les domaines de responsabilité pour réduire les possibilités de modification non autorisée ou d'utilisation inappropriée de RPS, conformément aux normes provinciales/territoriales.	Recommandée	Solutions
--------	---	-------------	-----------

Note : Par exemple, des contrôles d'accès appropriés devraient être en place pour séparer les fonctions des acteurs autorisés qui ont accès aux composantes hébergées du RDP afin de réduire les possibilités de modification non autorisée ou d'utilisation inappropriée de RPS et de données de système critiques pour la sécurité, conformément aux normes provinciales/territoriales.

BR3-10	Une solution de RDP-CA devrait respecter les normes provinciales/territoriales en ce qui a trait à la création de journaux d'audit sécurisés qui enregistrent toutes les activités d'accès, de modification ou de divulgation liées à l'information du RDP-CA. Cela comprend les activités des producteurs, des consommateurs et des demandeurs de RDP-CA.	Recommandée	Solutions
--------	--	-------------	-----------

Note : Par exemple, les normes provinciales/territoriales sur la tenue d'enregistrements d'audit sécurisés appropriés devraient permettre de journaliser les événements liés aux RPS, comme l'accès au RDP (y compris l'accès à des données confidentielles), la création du RDP, les changements apportés au RDP, la traçabilité du consentement, les dérogations aux directives de consentement et d'autres activités liées au RDP.

BR3-11	Une solution de RDP-CA devrait pouvoir enregistrer le contenu des journaux d'audit sécurisés, conformément aux normes provinciales/territoriales ou aux exigences du système.	Recommandée	Solutions
--------	---	-------------	-----------

Note : Par exemple, les normes provinciales/territoriales ou les exigences du système relatives aux journaux d'audit sécurisés devraient tenir compte du schéma et du contenu des journaux du RDP tels que l'ID utilisateur des acteurs autorisés, le rôle de l'utilisateur,

l'organisation de l'utilisateur qui accède au RDP (à tout le moins dans les cas où une personne accède à l'information pour le compte de plusieurs organisations), l'ID de patient du sujet des données (patient/personne), la fonction de l'utilisateur qui accède au RDP, un timbre-horodateur, dans le cas d'une dérogation pour accéder à des dossiers ou des portions de dossier bloqués ou masqués, la raison de la dérogation, et dans le cas de la modification de directives de consentement effectuée par un décideur substitut, l'identité de cette personne.

BR3-12	Une solution de RDP-CA pourrait permettre d'anonymiser le RDP-CA conformément aux exigences locales/provinciales/territoriales.	Optionnelle	Solutions
BR3-14	Une solution de RDP-CA devrait pouvoir extraire des éléments de données du RDP-CA de la source de données locale de l'auteur du RDP-CA.	Recommandée	Solutions
BR3-15	Une solution de RDP-CA pourrait permettre de convertir des documents structurés (p. ex. selon la norme FHIR) en documents non structurés (p. ex. PDF), et de convertir des documents structurés en d'autres documents structurés (p. ex. CDA).	Optionnelle	Solutions
BR3-17	<p>Une solution de RDP-CA devrait protéger les renseignements sur la santé au repos conformément aux normes de cryptage provinciales/territoriales.</p> <p>Note : Par exemple, les normes de cryptage provinciales/territoriales devraient porter sur des concepts d'algorithmes et de protocoles cryptographiques, ainsi que sur la gestion des clés de cryptage pour maintenir la confidentialité et l'intégrité du RDP.</p>	Recommandée	Solutions

6.5 Exigences : série complète

La présente section contient toutes les exigences d'interopérabilité et exigences liées aux solutions :

- énumérées dans les Exigences pour les tests d'interopérabilité de la présente version de la spécification d'interopérabilité du RDP-CA,
- énumérées dans les Exigences d'orientation et de soutien de la présente version de la spécification d'interopérabilité du RDP-CA; et
- susceptibles d'être incluses dans une version ultérieure.

6.5.1 Exigences opérationnelles et juridiques

Les exigences opérationnelles/juridiques sont des exigences qui permettent à des organisations indépendantes les unes des autres d'exécuter un processus ou de fournir un service en collaboration.

Le tableau suivant présente une vue d'ensemble des exigences opérationnelles/juridiques d'interopérabilité et liées aux solutions. Pour en savoir plus sur chaque exigence, cliquez sur l'identifiant de la règle opérationnelle (BR).

ID	Description	Type	Sous-catégorie
BR1-01	Une solution de RPD-CA devrait permettre le versionnage, le stockage, la conservation, la destruction et l'archivage des RDP produits et consommés par des utilisateurs autorisés du système conformément aux politiques provinciales/territoriales.	Recommandée	Solutions
BR1-02	Une solution de RDP-CA devrait donner à un PS la possibilité de vérifier et d'approuver le contenu du RDP avant qu'il soit accessible aux consommateurs de RDP-CA. Note : Si le PS détermine que des modifications doivent être apportées au RDP avant de l'approuver, il les apporte dans le dossier du patient. Si les changements ont une incidence sur le contenu du RDP, le PS créera un nouveau RDP qu'il vérifiera et approuvera ensuite.	Recommandée	Solutions
BR1-03	Une solution de RDP-CA doit permettre à un PS d'invalider un RDP s'il détermine qu'il a été entré par erreur ou qu'il est invalide, conformément aux politiques provinciales/territoriales.	Obligatoire	Interopérabilité
BR1-04	Une solution de RDP-CA devrait respecter les règles de conservation des données établies par les politiques locales/provinciales/territoriales et les exigences du système.	Recommandée	Solutions
BR1-05	Une solution de RDP-CA doit permettre à un consommateur de RDP autorisé (PS autorisé) de déterminer la provenance (auteur, producteur, date et sujet de soins du RDP-CA) d'un RDP	Obligatoire	Interopérabilité

courant et antérieur.

BR1-06	Une solution de RDP-CA pourrait permettre d'extraire et d'enregistrer des données discrètes d'un RDP si un utilisateur autorisé du système le demande.	Optionnelle	Solutions
BR1-07	Un auteur de RDP-CA devrait raisonnablement s'assurer que les renseignements médicaux qu'il contient sont exacts, suffisamment complets et à jour pour répondre à l'objectif clinique spécifié.	Recommandée	Solutions
BR1-08	Une solution de RDP-CA devrait pouvoir se conformer à une ordonnance de préservation de la preuve rendue par une entité autorisée, conformément aux politiques provinciales/territoriales. *Note : Les politiques sur la préservation de la preuve empêchent l'élimination de toute information stockée électroniquement dans le RDP-CA qui pourrait être requise dans un litige.	Recommandée	Solutions
BR1-09	Une solution de RDP-CA devrait pouvoir omettre ou masquer des données dans un RDP-CA conformément aux politiques sur la confidentialité locales/provinciales/territoriales.	Recommandée	Solutions
BR1-10	Une solution de RDP-CA doit pouvoir produire un RDP qui respecte les directives de consentement du sujet de soins, conformément aux normes et politiques locales/provinciales/territoriales. Note : Par exemple, les normes locales/provinciales/territoriales pourraient comprendre l'association des directives de consentement aux RPS contenus dans le RDP, notamment sur des concepts comme le maintien de l'association, le traitement des directives de consentement, le blocage de la transmission des RPS contenus dans un RDP lorsque les directives de consentement sont violées ou qu'aucune exception à une divulgation n'est établie dans une loi ou une politique provinciale/territoriale, et la notification des demandeurs lorsque des données sont bloquées en raison de directives de consentement.	Obligatoire	Interopérabilité
BR1-11	Une solution de RDP-CA doit limiter l'échange de renseignements médicaux à ce qui est cliniquement nécessaire et suffisant, conformément à la législation applicable et à la spécification RDP-CA. Note : Par exemple, le clinicien pourra créer le RDP-CA avec un sous-ensemble des domaines de données défini dans la spécification d'interopérabilité du RDP-CA.	Obligatoire	Interopérabilité

BR1-12	Une solution de RDP-CA doit pouvoir indiquer au consommateur de RDP-CA (p. ex. un PS) que de l'information sur le sujet de soins a été omise ou masquée conformément à des directives de consentement et des politiques provinciales/territoriales.	Obligatoire	Interopérabilité
BR1-13	Une solution de RDP-CA doit donner au patient/sujet de soins un droit d'accès à son RDP conformément aux politiques et aux dispositions législatives de la province ou du territoire.	Obligatoire	Interopérabilité
BR1-14	Une solution de RDP-CA doit limiter l'accès aux producteurs et aux consommateurs de RDP-CA autorisés.	Obligatoire	Interopérabilité

BR1-01

ID	BR1-01
Description	Une solution de RDP-CA devrait permettre le versionnage, le stockage, la conservation, la destruction et l'archivage des RDP produits et consommés par des utilisateurs autorisés du système conformément aux politiques provinciales/territoriales.
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solutions

BR1-02

ID	BR1-02
Description	<p>Une solution de RDP-CA devrait donner à un PS la possibilité de vérifier et d'approuver le contenu du RDP avant qu'il soit accessible aux consommateurs de RDP-CA.</p> <p>Note : Si le PS détermine que des modifications doivent être apportées au RDP avant de l'approuver, il les apporte dans le dossier du patient. Si les changements ont une incidence sur le contenu du RDP, le PS créera un nouveau RDP qu'il vérifiera et approuvera ensuite.</p>
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solutions

BR1-03

ID	BR1-03
Description	Une solution de RDP-CA doit permettre à un PS d'invalider un RDP s'il détermine qu'il a été entré par erreur ou qu'il est invalide, conformément aux politiques provinciales/territoriales.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR1-04

ID	BR1-04
Description	Une solution de RDP-CA devrait respecter les règles de conservation des données établies par les politiques locales/provinciales/territoriales et les exigences du système.
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solutions

BR1-05

ID	BR1-05
Description	Une solution de RDP-CA doit permettre à un consommateur de RDP autorisé (PS autorisé) de déterminer la provenance (auteur, producteur, date et sujet de soins du RDP-CA) d'un RDP courant et antérieur.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR1-06

ID	BR1-06
Description	Une solution de RDP-CA pourrait permettre d'extraire et d'enregistrer des données discrètes d'un RDP si un utilisateur autorisé du système le demande.
Type	Optionnelle
Statut	APPROUVÉE
Sous-catégorie	Solutions

BR1-07

ID	BR1-07
Description	Un auteur de RDP-CA devrait raisonnablement s'assurer que les renseignements médicaux qu'il contient sont exacts, suffisamment complets et à jour pour répondre à l'objectif clinique spécifié.
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solutions

BR1-08

ID	BR1-08
Description	<p>Une solution de RDP-CA devrait pouvoir se conformer à une ordonnance de préservation de la preuve rendue par une entité autorisée, conformément aux politiques provinciales/territoriales.</p> <p>*Note : Les politiques sur la préservation de la preuve empêchent l'élimination de toute information stockée électroniquement dans le RDP-CA qui pourrait être requise dans un litige.</p>
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solutions

BR1-09

ID	BR1-09
Description	Une solution de RDP-CA devrait pouvoir omettre ou masquer des données dans un RDP-CA conformément aux politiques sur la confidentialité locales/provinciales/territoriales.
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solutions

BR1-10

ID	BR1-10
Description	<p>Une solution de RDP-CA doit pouvoir produire un RDP qui respecte les directives de consentement du sujet de soins, conformément aux normes et politiques locales/provinciales/territoriales.</p> <p>Note : Par exemple, les normes locales/provinciales/territoriales pourraient comprendre l'association des directives de consentement aux RPS contenus dans le RDP, notamment sur des concepts comme le maintien de l'association, le traitement des directives de consentement, le blocage de la transmission des RPS contenus dans un RDP lorsque les directives de consentement sont violées ou qu'aucune exception à une divulgation n'est établie dans une loi ou une politique provinciale/territoriale, et la notification des demandeurs lorsque des données sont bloquées en raison de directives de consentement.</p>
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR1-11

ID	BR1-11
Description	<p>Une solution de RDP-CA doit limiter l'échange de renseignements médicaux à ce qui est cliniquement nécessaire et suffisant, conformément à la législation applicable et à la spécification RDP-CA.</p> <p>Note : Par exemple, le clinicien pourra créer le RDP-CA avec un sous-ensemble des domaines de données défini dans la spécification d'interopérabilité du RDP-CA.</p>
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR1-12

ID	BR1-12
Description	<p>Une solution de RDP-CA doit pouvoir indiquer au consommateur de RDP-CA (p. ex. un PS) que de l'information sur le sujet de soins a été omise ou masquée conformément à des directives de consentement et des politiques provinciales/territoriales.</p>
Type	Obligatoire

Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR1-13

ID	BR1-13
Description	Une solution de RDP-CA doit donner au patient/sujet de soins un droit d'accès à son RDP conformément aux politiques et aux dispositions législatives de la province ou du territoire.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR1-14

ID	BR1-14
Description	Une solution de RDP-CA doit limiter l'accès aux producteurs et aux consommateurs de RDP-CA autorisés.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

6.5.2 Exigences syntaxiques et sémantiques

Exigences d'interopérabilité syntaxiques et sémantiques : Conditions syntaxiques et sémantiques nécessaires pour que les données échangées entre les systèmes de dossiers médicaux puissent être interprétées correctement et que leur signification puisse être établie sans ambiguïté.

Le tableau suivant présente une vue d'ensemble des exigences d'interopérabilité syntaxique et sémantique. Pour en savoir plus sur chaque exigence, cliquez sur l'identifiant de la règle opérationnelle (BR).

ID	Description	Type	Sous-catégorie
BR2-01	Une solution de RDP-CA doit permettre à un PS autorisé de créer/produire un RDP fondé sur le Guide d'implantation FHIR du RDP-CA.	Obligatoire	Interopérabilité
BR2-02	Une solution de RDP-CA doit respecter les normes d'interopérabilité syntaxique, sémantique/terminologique et de contenu établies dans le Guide d'implantation FHIR du RDP-CA.	Obligatoire	Interopérabilité

BR2-01

ID	BR2-01
Description	Une solution de RDP-CA doit permettre à un PS autorisé de créer/produire un RDP fondé sur le Guide d'implantation FHIR du RDP-CA.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR2-02

ID	BR2-02
Description	Une solution de RDP-CA doit respecter les normes d'interopérabilité syntaxique, sémantique/terminologique et de contenu établies dans le Guide d'implantation FHIR du RDP-CA.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

6.5.3 Exigences techniques

Exigences techniques : Conditions requises pour qu'un système de dossiers médicaux transmette des données à un autre système de dossiers médicaux et pour que le système récepteur accuse réception des données utiles.

Le tableau suivant présente une vue d'ensemble des exigences techniques d'interopérabilité et liées aux solutions. Pour en savoir plus sur chaque exigence, cliquez sur l'identifiant de la règle opérationnelle (BR).

ID	Description	Type	Sous-catégorie
BR3-09	<p>Une solution de RDP-CA devrait respecter les normes minimales de l'industrie sur les mécanismes de contrôle de l'accès et de sécurité en fonction du rôle, notamment définir le niveau de sécurité et le profil d'autorisation de tous les acteurs autorisés et faire le mappage de chaque utilisateur avec un ou plusieurs rôles et de chaque rôle avec une ou plusieurs fonctions du système, selon les normes provinciales/territoriales et les exigences du système.</p> <p>Note : Par exemple, les normes provinciales/territoriales sur le contrôle de l'accès fondé sur le rôle devraient tenir compte de normes telles que ISO 22600-1:2014, qui décrit les scénarios et les paramètres cruciaux de l'échange d'informations d'un domaine de politique à un autre, et ISO 22600-2:2014, qui décrit et explique de manière plus détaillée les architectures et les modèles sous-jacents de la gestion des privilèges et du contrôle d'accès nécessaires à la sécurisation de l'échange de données incluant la représentation formelle des politiques.</p>	Recommandée	Solutions
BR3-01	Une solution de RDP-CA doit permettre de consigner et de communiquer l'identité du sujet de soins du RDP.	Obligatoire	Interopérabilité
BR3-02	Une solution de RDP-CA doit permettre de consigner et de communiquer l'identité de l'auteur autorisé du RDP-CA.	Obligatoire	Interopérabilité
BR3-04	Une solution de RDP-CA doit permettre de visualiser les différentes versions d'un RDP et de fournir une version antérieure sur demande, conformément aux politiques provinciales/territoriales.	Obligatoire	Interopérabilité

BR3-05	Une solution de RDP-CA pourrait permettre de produire un RDP-CA dans un format transférable (p. ex. PDF) accessible aux patients/sujets de soins.	Optionnelle	Interopérabilité
BR3-06	Une solution de RDP-CA devrait respecter les normes minimales locales/provinciales/territoriales relativement à l'authentification (p. ex. authentification multifactorielle) des utilisateurs autorisés.	Recommandée	Solution
BR3-07	Une solution de RDP-CA devrait, lorsque c'est possible, séparer les fonctions et les domaines de responsabilité pour réduire les possibilités de modification non autorisée ou d'utilisation inappropriée de RPS, conformément aux normes provinciales/territoriales. Note : Par exemple, des contrôles d'accès appropriés devraient être en place pour séparer les fonctions des acteurs autorisés qui ont accès aux composantes hébergées du RDP afin de réduire les possibilités de modification non autorisée ou d'utilisation inappropriée de RPS et de données de système critiques pour la sécurité, conformément aux normes provinciales/territoriales.	Recommandée	Solution
BR3-08	Une solution de RDP-CA doit protéger les renseignements médicaux en transit, conformément aux normes de cryptage provinciales/territoriales. Note : Par exemple, les normes de cryptage provinciales/territoriales devraient porter sur des concepts d'algorithmes et de protocoles cryptographiques, ainsi que sur la gestion des clés de cryptage durant la transmission des RPS pour maintenir la confidentialité et l'intégrité du RDP.	Obligatoire	Interopérabilité

BR3-10	<p>Une solution de RDP-CA devrait respecter les normes provinciales/territoriales en ce qui a trait à la création de journaux d'audit sécurisés qui enregistrent toutes les activités d'accès, de modification ou de divulgation liées à l'information du RDP-CA. Cela comprend les activités des producteurs, des consommateurs et des demandeurs de RDP-CA.</p>	Recommandée	Solution
	<p>Note : Par exemple, les normes provinciales/territoriales sur la tenue d'enregistrements d'audit sécurisés appropriés devraient permettre de journaliser les événements liés aux RPS, comme l'accès au RDP (y compris l'accès à des données confidentielles), la création du RDP, les changements apportés au RDP, la traçabilité du consentement, les dérogations aux directives de consentement et d'autres activités liées au RDP.</p>		
BR3-11	<p>Une solution de RDP-CA devrait pouvoir enregistrer le contenu des journaux d'audit sécurisés, conformément aux normes provinciales/territoriales ou aux exigences du système.</p>	Recommandée	Solution
	<p>Note : Par exemple, les normes provinciales/territoriales ou les exigences du système relatives aux journaux d'audit sécurisés devraient tenir compte du schéma et du contenu des journaux du RDP tels que l'ID utilisateur des acteurs autorisés, le rôle de l'utilisateur, l'organisation de l'utilisateur qui accède au RDP (à tout le moins dans les cas où une personne accède à l'information pour le compte de plusieurs organisations), l'ID de patient du sujet des données (patient/personne), la fonction de l'utilisateur qui accède au RDP, un timbre-horodateur, dans le cas d'une dérogation pour accéder à des dossiers ou des portions de dossier bloqués ou masqués, la raison de la dérogation, et dans le cas de la modification de directives de consentement effectuée par un décideur substitut, l'identité de cette personne.</p>		
BR3-12	<p>Une solution de RDP-CA pourrait permettre d'anonymiser le RDP-CA conformément aux exigences locales/provinciales/territoriales.</p>	Optionnelle	Solution
BR3-13	<p>Une solution de RDP-CA doit permettre d'identifier un RDP-CA par un identifiant unique.</p>	Obligatoire	Interopérabilité
BR3-14	<p>Une solution de RDP-CA devrait pouvoir extraire des éléments de données du RDP-CA de la source de données locale de l'auteur du RDP-CA.</p>	Recommandée	Solution
BR3-15	<p>Une solution de RDP-CA pourrait permettre de convertir des documents structurés (p. ex. selon la norme FHIR) en documents non structurés (p.</p>	Optionnelle	Solution

ex. PDF), et de convertir des documents structurés en d'autres documents structurés (p. ex. CDA).

BR3-16	Une solution de RDP-CA doit créer le RDP-CA dans un format structuré conforme à la norme FHIR R4 (v4.0.1) + JSON et XML.	Obligatoire	Interopérabilité
BR3-17	Une solution de RDP-CA devrait protéger les renseignements sur la santé au repos conformément aux normes de cryptage provinciales/territoriales. Note : Par exemple, les normes de cryptage provinciales/territoriales devraient porter sur des concepts d'algorithmes et de protocoles cryptographiques, ainsi que sur la gestion des clés de cryptage pour maintenir la confidentialité et l'intégrité du RDP.	Recommandée	Solution

BR3-01

ID	BR3-01
Description	Une solution de RDP-CA doit permettre de consigner et de communiquer l'identité du sujet de soins du RDP.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR3-02

ID	BR3-02
Description	Une solution de RDP-CA doit permettre de consigner et de communiquer l'identité de l'auteur autorisé du RDP-CA.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR3-03

ID	BR3-03
Description	Une solution de RDP-CA doit permettre d'envoyer un RDP en identifiant un PS destinataire et le lieu/l'adresse correspondant.

Type	Obligatoire
Statut	PROVISIOIRE FUTURE
Sous-catégorie	Interopérabilité

BR3-04

ID	BR3-04
Description	Une solution de RDP-CA doit permettre de visualiser les différentes versions d'un RDP et de fournir une version antérieure sur demande, conformément aux politiques provinciales/territoriales.
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR3-05

ID	BR3-05
Description	Une solution de RDP-CA pourrait permettre de produire un RDP-CA dans un format transférable (p. ex. PDF) accessible aux patients/sujets de soins.
Type	Optionnelle
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR3-06

ID	BR3-06
Description	Une solution de RDP-CA devrait respecter les normes minimales locales/provinciales/territoriales relativement à l'authentification (p. ex. authentification multifactorielle) des utilisateurs autorisés.
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solution

BR3-07

ID	BR3-07
Description	<p>Une solution de RDP-CA devrait, lorsque c'est possible, séparer les fonctions et les domaines de responsabilité pour réduire les possibilités de modification non autorisée ou d'utilisation inappropriée de RPS, conformément aux normes provinciales/territoriales.</p> <p>Note : Par exemple, des contrôles d'accès appropriés devraient être en place pour séparer les fonctions des acteurs autorisés qui ont accès aux composantes hébergées du RDP afin de réduire les possibilités de modification non autorisée ou d'utilisation inappropriée de RPS et de données de système critiques pour la sécurité, conformément aux normes provinciales/territoriales.</p>
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solution

BR3-08

ID	BR3-08
Description	<p>Une solution de RDP-CA doit protéger les renseignements médicaux en transit, conformément aux normes de cryptage provinciales/territoriales.</p> <p>Note : Par exemple, les normes de cryptage provinciales/territoriales devraient porter sur des concepts d'algorithmes et de protocoles cryptographiques, ainsi que sur la gestion des clés de cryptage durant la transmission des RPS pour maintenir la confidentialité et l'intégrité du RDP.</p>
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR3-09

ID	BR3-09
Description	<p>Une solution de RDP-CA devrait respecter les normes minimales de l'industrie sur les mécanismes de contrôle de l'accès et de sécurité en fonction du rôle, notamment définir le niveau de sécurité et le profil d'autorisation de tous les acteurs autorisés et faire le mappage de chaque utilisateur avec un ou plusieurs rôles et de chaque rôle avec une ou plusieurs fonctions du système, selon les normes provinciales/territoriales et les exigences du système.</p> <p>Note : Par exemple, les normes provinciales/territoriales sur le contrôle de l'accès fondé sur le rôle devraient tenir compte de normes telles que ISO 22600-1:2014, qui décrit les scénarios et les paramètres cruciaux de l'échange d'informations d'un domaine de politique à un autre, et ISO 22600-2:2014, qui décrit et explique de manière plus détaillée les architectures et les modèles sous-jacents de la gestion des privilèges et du contrôle d'accès nécessaires à la sécurisation de l'échange de données incluant la représentation formelle des politiques.</p>
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solution

BR3-10

ID	BR3-10
Description	<p>Une solution de RDP-CA devrait respecter les normes provinciales/territoriales en ce qui a trait à la création de journaux d'audit sécurisés qui enregistrent toutes les activités d'accès, de modification ou de divulgation liées à l'information du RDP-CA. Cela comprend les activités des producteurs, des consommateurs et des demandeurs de RDP-CA.</p> <p>Note : Par exemple, les normes provinciales/territoriales sur la tenue d'enregistrements d'audit sécurisés appropriés devraient permettre de journaliser les événements liés aux RPS, comme l'accès au RDP (y compris l'accès à des données confidentielles), la création du RDP, les changements apportés au RDP, la traçabilité du consentement, les dérogations aux directives de consentement et d'autres activités liées au RDP.</p>
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solution

BR3-11

ID	BR3-11
Description	<p>Une solution de RDP-CA devrait pouvoir enregistrer le contenu des journaux d'audit sécurisés, conformément aux normes provinciales/territoriales ou aux exigences du système.</p> <p>Note : Par exemple, les normes provinciales/territoriales ou les exigences du système relatives aux journaux d'audit sécurisés devraient tenir compte du schéma et du contenu des journaux du RDP tels que l'ID utilisateur des acteurs autorisés, le rôle de l'utilisateur, l'organisation de l'utilisateur qui accède au RDP (à tout le moins dans les cas où une personne accède à l'information pour le compte de plusieurs organisations), l'ID de patient du sujet des données (patient/personne), la fonction de l'utilisateur qui accède au RDP, un timbre-horodateur, dans le cas d'une dérogation pour accéder à des dossiers ou des portions de dossier bloqués ou masqués, la raison de la dérogation, et dans le cas de la modification de directives de consentement effectuée par un décideur substitut, l'identité de cette personne.</p>
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solution

BR3-12

ID	BR3-12
Description	Une solution de RDP-CA pourrait permettre d'anonymiser le RDP-CA conformément aux exigences locales/provinciales/territoriales.
Type	Optionnelle
Statut	APPROUVÉE
Sous-catégorie	Solution

BR3-13

ID	BR3-13
Description	Une solution de RDP-CA doit permettre d'identifier un RDP-CA par un identifiant unique.
Type	Obligatoire
Statut	ÉBAUCHE
Sous-catégorie	Interopérabilité

BR3-14

ID	BR3-14
Description	Une solution de RDP-CA devrait pouvoir extraire des éléments de données du RDP-CA de la source de données locale de l'auteur du RDP-CA.
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solution

BR3-15

ID	BR3-15
Description	Une solution de RDP-CA pourrait permettre de convertir des documents structurés (p. ex. selon la norme FHIR) en documents non structurés (p. ex. PDF), et de convertir des documents structurés en d'autres documents structurés (p. ex. CDA).
Type	Optionnelle
Statut	APPROUVÉE
Sous-catégorie	Solution

BR3-16

ID	BR3-16
Description	Une solution de RDP-CA doit créer le RDP-CA dans un format structuré conforme à la norme FHIR R4 (v4.0.1) + JSON et XML
Type	Obligatoire
Statut	APPROUVÉE
Sous-catégorie	Interopérabilité

BR3-17

ID	BR3-17
Description	<p>Une solution de RDP-CA devrait protéger les renseignements sur la santé au repos conformément aux normes de cryptage provinciales/territoriales.</p> <p>Note : Par exemple, les normes de cryptage provinciales/territoriales devraient porter sur des concepts d'algorithmes et de protocoles cryptographiques, ainsi que sur la gestion des clés de cryptage pour maintenir la confidentialité et l'intégrité du RDP.</p>
Type	Recommandée
Statut	APPROUVÉE
Sous-catégorie	Solution