# Spécification d’interopérabilité CA:FeX

## (*Canadian FHIR Exchange*, ou échange FHIR canadien)

Version : 1.0.0

Type : version de mise à l’essai

Date de la version : 17 octobre 2022

Inforoute Santé du Canada

# Table des matières

# 1 Spécification d'interopérabilité CA:FeX

## 1.1 Introduction

L'interopérabilité permet à l'information de circuler librement entre des solutions et appareils hétérogènes. Lorsque les diverses parties du réseau de la santé sont interopérables, elles « parlent la même langue ». L'interopérabilité améliore la continuité des soins, la collaboration entre les professionnels de la santé et l'accès des patients à leur information médicale. De plus, en éliminant le cloisonnement des données, elle réduit l'inefficience et la redondance dans le réseau de la santé.

Jamais la connexion, la collaboration et la communication n'ont été aussi importantes pour le réseau de la santé. En raison de la hausse de l'utilisation des solutions de santé numériques, il est désormais indispensable d'assurer un partage électronique sûr et efficace de l'information dans tout le cercle des soins. Mais pour continuer à améliorer les soins de santé au Canada, l'interopérabilité s'impose – un réseau connecté est un réseau en meilleure santé.

Pour aider les provinces et territoires, Inforoute Santé du Canada (Inforoute) facilite diverses initiatives de collaboration pancanadienne visant à faire progresser l'interopérabilité. Même s'il y a encore de nombreux obstacles à l'interopérabilité, la spécification CA:FeX – dérivée de la norme d'échange d'information FHIR d'HL7 – fournit une structure normalisée pour le partage des données vitales sur le patient entre les professionnels de la santé et entre ces derniers et le patient. L'échange d'information basé sur la norme FHIR est similaire à l'échange d'information sur la santé (EIS) et remplit les mêmes objectifs.

L'Office of the National Coordinator for Health Information Technology (ONC) des États-Unis définit l'EIS comme suit :

> *[Traduction]*
> *L'échange d'information sur la santé (EIS) permet aux médecins, aux infirmières, aux pharmaciens, aux autres professionnels de la santé et au patient concerné d'accéder de manière appropriée à l'information médicale vitale du patient et de la partager par voie électronique sécurisée, ce qui contribue à améliorer la rapidité, la qualité, la sûreté et le coût des soins. Bien que l'EIS ne remplace pas la communication entre le professionnel de la santé et le patient, il améliore grandement l'exhaustivité des dossiers médicaux (ce qui peut avoir un effet important sur les soins), puisque les antécédents, les médicaments pris par le patient et d'autres renseignements sont examinés conjointement pendant les consultations. L'échange approprié et rapide de l'information vitale sur le patient permet d'éclairer la prise de décisions au point d'intervention, d'éviter les réadmissions, la répétition inutile des analyses et examens et les erreurs liées aux médicaments et, enfin, d'améliorer les diagnostics.*

## 1.2 Public cible

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

- les personnes intéressées par l'intégration des systèmes d'information sur la santé et des flux de tâches;
- les services des TI des établissements de santé;
- le personnel technique des fournisseurs de solutions cliniques;
- les experts qui participent à l'élaboration des normes;
- les développeurs de logiciels.

## 1.3 But

Le but du présent document est le suivant :

- présenter deux cas d'utilisation de l'EIS basé sur FHIR;
- décrire un ensemble d'exigences détaillées concernant les acteurs, les transactions et les liens avec les profils et normes applicables;
- préciser les patrons d'implantation qui permettent l'échange d'information clinique à l'aide de CA:FeX;
- décrire l'ensemble d'exigences qui complète les profils IHE et FHIR requis par la spécification CA:FeX, qui comporte des contraintes canadiennes.

## 1.4 Glossaire des termes et abréviations

Le tableau suivant fournit la liste des termes et des abréviations que vous retrouverez dans les spécifications d'interopérabilité pancanadiennes (RDP-CA, CA:FeX) et/ou dans l'information sur le prototypage et la validation.

| Terme/abréviation | Définition |
|---|---|
| Acteurs IHE | Les acteurs IHE (p. ex. professionnel de la santé, DME, DSE, etc.) ont pour rôle de produire et/ou de gérer l'information et/ou d'effectuer une action en fonction de l'information, dans le contexte d'un profil IHE.<br><br>(Source : https://wiki.ihe.net/index.php/Actors) |
| Architecture de référence (AR) | Modèle évolutif de disponibilité des services qui prend en charge un vaste écosystème d'interopérabilité ne se limitant pas aux résumés du dossier du patient. Il a pour but de faciliter le dialogue, la collaboration et la convergence de multiples intervenants vers l'adoption de normes ouvertes communes. Il s'agit d'une vue technique conceptuelle qui fournit un vocabulaire commun ainsi qu'un ensemble d'acteurs et de transactions qui représentent les composantes habituelles d'un écosystème de santé numérique (solutions des secteurs public et privé). L'AR associe des composantes fondamentales provenant d'organismes internationaux d'élaboration de normes à des patrons d'implantation développés au Canada. |
| ATNA | Le profil ATNA (*Audit Trail and Node Authentication*, ou piste d'audit et authentification de nœuds) précise les éléments fondamentaux de toute forme de systèmes sécurisés : authentification des nœuds, authentification des utilisateurs, journalisation des événements (audit) et cryptage des télécommunications. Il est également utilisé pour indiquer que d'autres propriétés de sécurité interne – contrôle d'accès, contrôle de configuration, restriction de privilèges, etc. – sont fournies.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html) |
| Auteur | Professionnel de la santé qui rédige et/ou modifie des données cliniques, p. ex. un résumé du dossier du patient. |
| Base de données sur les produits pharmaceutiques (BDPP) | Base de données qui contient l'information sur les médicaments dont la vente est autorisée par Santé Canada. La BDPP est automatiquement mise à jour tous les soirs et indique la disponibilité des médicaments au Canada. |
| CA:FeX (*Canadian FHIR Exchange*, ou échange FHIR canadien) | Spécification d'interopérabilité visant à faciliter l'implantation de patrons d'échange FHIR RESTful qui ont été développés à partir de la norme de référence FHIR et qui peuvent être appliqués à une infrastructure non FHIR existante tout aussi facilement qu'à des serveurs FHIR. |
| CA:FMT (*Canadian Formatting Service*, ou service de formatage canadien) | Spécification qui permet de convertir des documents en différents formats (p. ex. de FHIR à PDF, à CDA, etc.). |
| Centre de médecine familiale | Le Collège des médecins de famille du Canada définit le centre de médecine familiale (CMF) comme suit :<br><br>« Le CMF est une pratique de médecine de famille définie par ses patients comme l'endroit où ils se sentent le plus à l'aise de parler de leur santé personnelle et familiale, ainsi que de leurs problèmes de santé. (…) Un CMF sert de point central pour la coordination et la continuité des soins liés à tous |

| Terme/abréviation | Définition |
|---|---|
| | les services médicaux que ses patients reçoivent dans la communauté médicale. »<br><br>Ce concept est présenté plus en détail dans le document *Une vision pour le Canada : La pratique de la médecine familiale - Le Centre de médecine de famille*, publié par le Collège des médecins de famille du Canada. |
| Consommateur | Système d'information sur la santé ou de dossiers médicaux (DME, SIS, SIC, DSP, portail-patients, DSE) qui permet à un professionnel de la santé autorisé ou à un patient/sujet de soins d'accéder à un document clinique (p. ex. RDP-CA) ou de le recevoir. |
| Couche d'accès à l'information sur la santé (CAIS) | Spécification d'interface pour l'infostructure de DSE qui définit les composantes des services, les rôles des services, le modèle d'information et les normes de messagerie nécessaires à l'échange de données du DSE et à l'exécution de profils d'interopérabilité entre les services de DSE.<br><br>(Source : https://www.infoway-inforoute.ca/fr/component/edocman/292-architecture-sdse-rapport-complet/view-document, page 360) |
| CT | Le profil d'intégration *Consistent Time* (CT) (synchronisation du temps) permet de bien synchroniser les horloges et les horodateurs des nombreux ordinateurs d'un réseau. Ce profil spécifie une synchronisation comportant une erreur médiane inférieure à 1 seconde. Cela suffit dans la plupart des cas.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-7.html) |
| Dépôt de documents (local ou central) | Voir la définition de Dépôt de données cliniques (local ou central). |
| Dépôt de données cliniques (local ou central) | Aussi appelé « Dépôt de documents cliniques ». Espace de stockage partagé pour les documents cliniques qui peut être hébergé localement (c.-à-d. par le producteur de données) ou dans l'infrastructure centrale et auquel les utilisateurs autorisés peuvent accéder. |
| Dépôt FHIR® | Dépôt basé sur FHIR et utilisé pour le stockage des données cliniques. |
| Domaines IHE | Les domaines IHE sont responsables de l'élaboration et de la tenue à jour des cadres techniques (*IHE Technical Frameworks*) qui décrivent les profils d'intégration. Chaque domaine gère les profils d'intégration dans une discipline particulière des soins de santé (p. ex. les soins virtuels).<br><br>(Source : https://wiki.ihe.net/index.php/Domains) |
| Dossier de santé électronique (DSE) | Solution clinique qui contient un ensemble de données numériques sécurisées et confidentielles sur la santé du patient. Ces données peuvent être partagées entre différents milieux de soins/systèmes cliniques intégrés. Le DSE améliore l'échange et l'interprétation de l'information médicale par les professionnels de la santé qui traitent le patient. Exemples de DSE :<br><br>• CareConnect est le DSE sécurisé et à accès en lecture seule de la Colombie-Britannique. Il offre en tout temps aux professionnels de la santé une vue intégrée à l'échelle provinciale de l'information médicale centrée sur le patient, afin de faciliter la prestation des soins dont il a besoin.<br>• HEALTHe NL est le DSE de Terre-Neuve-et-Labrador. Il fournit des données exactes et fiables qui permettent d'améliorer la prestation des soins, la prise de décisions et l'élaboration des politiques ainsi que d'accroître la reddition de comptes, la stabilité et l'efficacité au sein du |

| Terme/abréviation | Définition |
|---|---|
| | réseau provincial de la santé.<br>• Alberta Netcare est le nom de tous les projets rattachés au DSE provincial, système électronique sécurisé et confidentiel regroupant l'information sur la santé des patients sous la forme de dossiers patients uniques, complets et intégrés.<br>• Autres systèmes cliniques : dans certaines autorités sanitaires, d'autres systèmes cliniques peuvent faire office de DSE, car ils conservent les résumés du dossier du patient. |
| Dossier de santé électronique longitudinal | Dossier patient unique et complet composé de données provenant de nombreuses sources dans le continuum des soins de santé. |
| Échange d'information sur la santé (EIS) | L'échange d'information sur la santé (EIS) permet aux médecins, aux infirmières, aux pharmaciens, aux autres professionnels de la santé et au patient concerné d'accéder de manière appropriée à l'information médicale vitale du patient et de la partager par voie électronique sécurisée, ce qui contribue à améliorer la rapidité, la qualité, la sûreté et le coût des soins.<br><br>Bien que l'EIS ne remplace pas la communication entre le professionnel de la santé et le patient, il améliore grandement l'exhaustivité des dossiers médicaux (ce qui peut avoir un effet important sur les soins), puisque les antécédents, les médicaments pris par le patient et d'autres renseignements sont examinés conjointement pendant les consultations.<br><br>L'échange efficace et rapide de l'information vitale sur le patient permet d'éclairer la prise de décisions au point d'intervention; d'éviter les réadmissions, la répétition inutile des analyses et examens et les erreurs liées aux médicaments; et, enfin, d'améliorer les diagnostics.<br><br>(Source : https://www.healthit.gov/topic/health-it-and-health-information-exchange- basics/what-hie) |
| Ensemble de données extensible du RDP-CA | Contenu du RDP-CA pouvant être augmenté afin de refléter un cas d'utilisation du RDP-CA qui complète les cas d'utilisation primaires.<br><br>*Note : L'ensemble de données est dit « extensible » parce qu'on peut y ajouter des domaines de données, comme les antécédents familiaux. |
| Exigences d'interopérabilité opérationnelle/ juridique | Conditions permettant à des organisations indépendantes les unes des autres d'exécuter un processus ou de fournir un service en collaboration. |
| Exigences d'interopérabilité syntaxique/sémantique | 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 d'interopérabilité technique | 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. |
| Exigences opérationnelles non testables | Exigences opérationnelles qui ne sont pas directement rattachées à un profil IHE dans la spécification du RDP-CA (p. ex. exigences à prendre en considération ou destinées à guider les responsables de l'implantation du RDP-CA). |

| Terme/abréviation | Définition |
|---|---|
| Exigences opérationnelles testables | Exigences opérationnelles qui sont directement rattachées à un profil IHE dans la spécification du RDP-CA. |
| Fast Healthcare Interoperability Resources (FHIR®) | Cadre de normes de nouvelle génération créé par HL7. Alliant les meilleures caractéristiques des produits V2, V3 et CDA d'HL7 aux plus récentes normes du Web, FHIR® se distingue par sa grande applicabilité.<br><br>(Source : http://www.hl7.org/implement/standards/fhir/) |
| Gazelle | Gazelle est une suite d'outils virtuels, développée par IHE Europe, qui sert à la réalisation de tests d'interopérabilité. Elle permet aux organisations gouvernementales et aux fournisseurs de valider le rôle qu'ils joueront dans un écosystème et leur capacité à satisfaire aux exigences d'interopérabilité. La suite met à leur disposition plusieurs options en libre-service d'autotest et d'innovation pour tester la conformité de leurs systèmes avec les profils d'intégration représentés. |
| Health Level Seven (HL7) | Fondé en 1987, Health Level Seven (HL7) est un organisme à but non lucratif dont le mandat est de fournir un cadre de travail exhaustif et des normes pour l'échange, l'intégration, la transmission et l'extraction d'information électronique sur la santé pour soutenir la pratique clinique ainsi que la gestion, la prestation et l'évaluation des services de santé.<br><br>(Source : http://www.hl7.org/about/index.cfm?ref=nav) |
| ID | Identifiant (de patient, de client, de ressource, etc.) |
| Infrastructure centrale | Infrastructure qui recueille l'information médicale provenant des organisations participantes et qui la stocke dans un emplacement centralisé. L'infrastructure offre également des mécanismes de contrôle d'accès. En général, l'infrastructure centrale relève de la province ou du territoire. |
| Integrating the Healthcare Enterprise (IHE) | IHE est une initiative menée par des professionnels de la santé et des représentants de l'industrie et qui vise à améliorer le partage de l'information entre les systèmes informatiques du secteur de la santé. IHE préconise l'utilisation coordonnée de normes reconnues, comme DICOM et FHIR, pour répondre aux besoins cliniques de la manière la plus propice à l'optimisation des soins. Les systèmes développés en conformité avec les exigences d'IHE communiquent mieux entre eux, sont plus faciles à implanter et permettent au personnel soignant d'utiliser plus efficacement l'information.<br><br>(Source : https://www.ihe.net/) |
| Interopérabilité | L'interopérabilité permet à l'information de circuler librement entre des solutions et appareils hétérogènes. Lorsque les diverses parties du réseau de la santé sont interopérables, elles « parlent la même langue ». L'interopérabilité améliore la continuité des soins, la collaboration entre les professionnels de la santé et l'accès des patients à leur information médicale. En éliminant le cloisonnement des données, elle réduit l'inefficience et la redondance dans le réseau de la santé.<br><br>Jamais la connexion, la collaboration et la communication n'ont été aussi importantes pour le réseau de la santé. En raison de la hausse de l'utilisation des solutions de santé numériques, il est désormais indispensable d'assurer un partage électronique sûr et efficace de l'information dans tout le cercle des soins. Mais pour continuer à améliorer les soins de santé au Canada, l'interopérabilité s'impose – un réseau connecté est un réseau en meilleure |

| Terme/abréviation | Définition |
|---|---|
| | santé.<br><br>Vous trouverez plus d'information à ce sujet sur la page *Interopérabilité* du site Web d'Inforoute. |
| IUA | Le profil *Internet User Authorization* (IUA) (autorisation de l'utilisateur Internet) prend en charge l'autorisation des transactions réseau lors de l'utilisation des transports HTTP RESTful. IHE a créé des profils d'autorisation pour les services Web et les transactions basées sur SOAP, tandis que le profil IUA est un profil d'autorisation pour les transactions HTTP RESTful.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-34.html) |
| Mandataire du patient | Personne ou entité autorisée à agir au nom d'un patient/sujet de soins. Il peut s'agir d'un parent d'enfant à charge, d'un parent d'adulte à charge, d'une personne ayant une procuration, etc. |
| MHD | Le profil *Mobile access to Health Documents* (MHD) (accès mobile aux documents médicaux) définit une interface normalisée (interface de programmation d'application, ou API) pour l'échange de documents cliniques entre appareils mobiles, afin que l'environnement de déploiement des applications mobiles soit homogène et réutilisable.<br><br>(Source : https://profiles.ihe.net/ITI/MHD/index.html) |
| Numéro d'identification de médicament (DIN) | Numéro à huit chiffres, généré par ordinateur, que Santé Canada attribue à chaque produit médicamenteux avant qu'il soit commercialisé au Canada. |
| P et T | Provinces et territoires |
| PDQm | Le profil *Patient Demographics Query for Mobile* (PDQm) (requête de données démographiques de patients pour appareils mobiles) définit une interface RESTful allégée vers un fournisseur de données démographiques de patients qui utilise des technologies facilement accessibles aux applications mobiles et aux applications allégées sur navigateur.<br><br>(Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-38.html) |
| PIXm | Le profil *Patient Identifier Cross-Reference for Mobile* (PIXm) (références croisées des identifiants du patient pour appareils mobiles) fournit des transactions RESTful pour les applications mobiles et les applications allégées sur navigateur, transactions qui permettent de créer, de mettre à jour ou de supprimer des dossiers patients dans un gestionnaire de références croisées des identifiants du patient (*Patient Identifier Cross-Reference Manager*) et d'interroger celui-ci pour la recherche des identifiants interdomaines d'un patient.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-41.html) |
| PMIR | Le profil *Patient Master Identity Registry* (PMIR) (registre de l'identité maîtresse du patient) prend en charge la création, la mise à jour et la dépréciation des données relatives à l'identité maîtresse du patient, ainsi que l'abonnement aux notifications signalant les modifications apportées à l'identité maîtresse, en utilisant les ressources de la norme FHIR et les transactions RESTful.<br><br>(Source : https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_PMIR.pdf) |

| Terme/abréviation | Définition |
|---|---|
| Portail-patient | Point d'accès Web sécurisé qui donne au patient un accès sécurisé à ses renseignements personnels sur la santé (RPS) et à d'autres services de santé numériques en libre-service. Un portail-patient peut être hébergé sur une solution de DME. |
| Producteur | Système (DME, SIS, SIC, DSP ou DSE) qui crée/produit un document clinique (p. ex. RDP-CA) à la suite d'une requête d'un professionnel de la santé autorisé, d'un sujet de soins/patient ou d'un autre système autorisé. |
| Professionnel de la santé (PS) | Personne qui exerce une profession réglementée dans le domaine de la santé (médecin, infirmière, dentiste, pharmacien). |
| Profils d'intégration IHE | Les profils d'intégration IHE apportent une solution aux problèmes d'interopérabilité qui se posent dans les tâches cliniques courantes, représentées dans les cas d'utilisation. Les profils d'intégration décrivent en détail les spécifications techniques qui sous-tendent l'implantation des normes pertinentes en vue d'assurer un flot ininterrompu d'information entre différentes applications logicielles qui interviennent dans un cas d'utilisation spécifique.<br><br>Les profils indiquent comment les systèmes informatiques peuvent fournir un soutien intégré à un flux clairement défini, chaque profil prenant en charge une tâche clinique donnée dans un domaine clinique particulier. Les profils IHE peuvent être utilisés pour une implantation progressive de systèmes dans différents domaines et la mise en place graduelle d'applications de santé électroniques interopérables.<br><br>(Source : https://www.ihe-europe.net/about-us/faq) |
| Projetathon | Étape importante et bonne pratique de mise à l'essai et de validation d'une spécification, où les responsables de l'implantation collaborent pour tester leurs solutions en utilisant une méthodologie et des outils qui accélèrent l'interopérabilité. Un projetathon donne l'occasion aux participants de tester leurs systèmes entre eux et par rapport à un environnement de référence. Il leur permet aussi de mettre en commun leurs connaissances pratiques. |
| Répertoire canadien des médicaments (RCM) | Terminologie relative aux médicaments destinée à être utilisée dans les solutions de santé numériques au Canada, entre autres la solution nationale d'ordonnances électroniques (PrescripTIon[MC]). |
| Résumé du dossier du patient pancanadien (RDP-CA) | Résumé électronique du dossier du patient destiné à être utilisé au point d'intervention et qui comprend un ensemble minimal de données médicales, en conformité avec les spécifications applicables. Le RDP-CA est un extrait du dossier du patient pris à un moment précis et qui contient un ensemble normalisé de données cliniques et contextuelles (rétrospectives, simultanées, prospectives), dont les données minimales nécessaires et suffisantes pour déterminer le traitement d'un patient au point d'intervention. Il est indépendant des problèmes de santé du patient, des spécialités médicales et des traitements. |
| Résumé international du dossier médical du patient (IPS, pour *International Patient Summary*) | Ensemble d'éléments de données minimal et non exhaustif défini par la norme ISO/EN 17269 et implanté à l'aide des normes CDA et FHIR d'HL7. Cet ensemble forme un document de synthèse clinique qui peut être utilisé dans le cadre de soins planifiés ou non, localement ou à l'étranger. Le profil IPS précise les données requises et les critères de conformité nécessaires des cas d'utilisation d'un résumé international du dossier médical du patient.<br><br>(Source : https://wiki.ihe.net/index.php/International_Patient_Summary_(IPS)) |
| SIS | Système d'information sur la santé |

| Terme/abréviation | Définition |
|---|---|
| Soins locaux non planifiés | Soins non planifiés donnés à un résident du Canada dans/par le réseau canadien de la santé. Cela inclut les soins fournis par les organismes gouvernementaux fédéraux, provinciaux et territoriaux, ainsi que les soins pangouvernementaux. |
| Soins locaux planifiés | Soins planifiés donnés à un résident du Canada dans/par le réseau canadien de la santé. Cela inclut les soins fournis par les organismes gouvernementaux fédéraux, provinciaux et territoriaux, ainsi que les soins pangouvernementaux. |
| Soins transfrontaliers non planifiés | Soins non planifiés donnés à un résident du Canada dans/par un autre pays. |
| Soins transfrontaliers planifiés | Soins planifiés donnés à un résident du Canada dans/par un autre pays. |
| Solution clinique | Toute combinaison d'actifs et de processus de technologie de l'information sur la santé qui permet la communication, la gestion et le traitement final des données cliniques entre un producteur et un consommateur. Les solutions cliniques peuvent être constituées de divers systèmes producteurs et consommateurs, notamment le DME, le SIS, le SIC, le DSP, le DSE ou toute combinaison de ceux-ci. |
| Solution de RDP-CA | Toute combinaison d'actifs et de processus de technologie de l'information sur la santé qui permet la création, la communication, la gestion et le traitement final d'un RDP-CA entre un producteur et un consommateur de RDP-CA. Les solutions de RDP-CA peuvent être constituées de divers systèmes producteurs et consommateurs, notamment le DME, le SIS, le SIC, le DSP, le DSE ou toute combinaison de ceux-ci. |
| Spécification du RDP-CA | Spécification implantable et testable basée sur le profil IPS d'IHE et sur le guide d'implantation de l'IPS d'HL7.<br><br>Vous trouverez plus d'information sur la spécification du RDP-CA ici. |
| SUT | Système à tester, système à l'essai |
| SVCM | Le profil *Sharing Valuesets, Codes and Maps* (SVCM) (partage d'ensembles de valeurs, de codes et de mappages) définit une interface allégée par laquelle les systèmes informatiques du réseau de la santé peuvent extraire une nomenclature uniforme gérée de manière centralisée et des mappages entre les systèmes de codes basés sur la spécification FHIR.<br><br>(Source : https://wiki.ihe.net/index.php/Sharing_Valuesets,_Codes_and_Maps_(SVCM)) |
| Système de dossiers de santé | Terme générique qui peut désigner un système de dossiers médicaux, un système d'information sur la santé (SIS), un système d'information clinique (SIC), un système de dossiers de santé électroniques (DSE) ou un système de dossiers de santé personnels (DSP). Il décrit aussi de manière générale les acteurs susceptibles de produire et/ou de consommer un RDP-CA. Les patrons d'implantation adoptés par les provinces et territoires détermineront les types de systèmes utilisés pour la création, la visualisation, la consommation et la gestion des résumés du dossier du patient. |
| Terminologie | Ensemble de concepts identifiables de manière unique et auxquels sont associées des représentations, des désignations et des significations. |
| Test de conformité | Processus d'évaluation structuré visant à garantir qu'une solution ou un système clinique implante correctement une spécification particulière (p. ex. la spécification du RDP-CA), c'est-à-dire que l'implantation a été faite en |

| Terme/abréviation | Définition |
|---|---|
| | conformité avec les paramètres indiqués dans la spécification en question. |
| Transactions IHE | Interactions entre des acteurs qui communiquent l'information requise au moyen de messages normalisés (p. ex. requête de recherche de patient, envoi du résumé du dossier du patient).<br><br>(Source : https://wiki.ihe.net/index.php/PCC_TF-1/About) |
| XDM | Le profil *Cross-Enterprise Document Media Interchange* (XDM) (échange média de documents entre organisations) assure l'échange de documents à l'aide d'une structure commune de fichiers et de répertoires sur plusieurs types de supports classiques. Ce profil permet au patient d'utiliser un support physique pour transporter ses documents médicaux. Il rend également possible la transmission de documents médicaux de personne à personne par courrier électronique. Le profil XDM prend en charge le transfert de données concernant plusieurs patients au sein d'un même échange de données.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-16.html) |
| XDS | Le profil *Cross-Enterprise Document Sharing* (XDS) (échange de documents entre organisations) facilite l'enregistrement et la distribution des dossiers de santé électroniques des patients et l'accès à ceux-ci dans tous les établissements de santé.<br><br>(Source : https://profiles.ihe.net/ITI/TF/Volume1/ch-10.html) |

## 1.5 Préface

La spécification d’interopérabilité CA:FeX (*Canadian FHIR Exchange*, ou échange FHIR canadien) vise à faciliter l’adoption de patrons d’échange FHIR RESTful élaborés à partir de la norme de référence FHIR et pouvant être appliqués à une infrastructure non FHIR existante aussi facilement qu’ils peuvent l’être à des serveurs FHIR.

La version actuelle de CA:FeX est fondée sur un cadre d’échange de documents FHIR RESTful, implantable via un certain nombre de structures et de patrons FHIR. La spécification CA:FeX vise à exposer aux responsables de l'implantation certains des choix actuellement possibles lorsqu’on utilise FHIR, allant du plus simple au plus avancé. Au fil du temps, la spécification d'interopérabilité CA:FeX évoluera vers un profil d'intégration à part entière (semblable aux profils internationaux actuels, présentés plus loin) dont les indications sur les patrons d'échange FHIR RESTful seront plus exhaustives que celles qui existent pour le moment.

Le champ d’application de la spécification CA:FeX pourrait un jour s'étendre au-delà de l'échange de documents pour englober une nature plus atomique de l'échange d'information sur la santé. Cela dépendra des différentes phases prévues par la feuille de route de la spécification CA:FeX, de l'évolution des besoins du marché canadien de la santé et des nouvelles tendances au sein de la communauté internationale de l'échange d'information sur la santé FHIR.

Actuellement, les indications que fournissent les profils IHE portent essentiellement sur le développement des capacités d’échange de documents, soit au sein d’infrastructures non FHIR, soit par l'utilisation restreinte des ressources FHIR. Or, compte tenu de l'évolution des besoins du marché canadien, ces profils pourraient ne pas être suffisants pour l'échange de documents à l'aide d’un cadre FHIR RESTful. Voici les deux principaux profils IHE qui ont été envisagés et certaines de leurs limites :

- *Cross-Enterprise Document Sharing (XDS*) : Ce profil IHE fournit une spécification normalisée pour l’échange de documents et dont l'application est limitée aux infrastructures non FHIR. Bien qu'il ait été envisagé, le profil XDS n'est pas considéré comme une option dans l'architecture de référence (AR), car les intervenants canadiens tendent vers l'adoption d'approches plus modernes basées sur FHIR.
- *Mobile Access to Health Documents (MHD) :* Ce profil IHE est conçu pour faciliter l'utilisation de la norme FHIR pour la communication et l'échange de documents et peut, facultativement, servir de mandataire aux systèmes qui utilisent XDS. Le profil MHD utilise des ressources FHIR de type *DocumentReference* comme méthode de base pour la recherche de documents. Afin qu’il puisse être utilisé sans égard à la manière dont les informations sont stockées (p. ex. infrastructure XDS, FHIR ou autre système de stockage), ce profil applique des contraintes aux ressources FHIR de type *DocumentReference*. Il comporte néanmoins une limite : un document doit être soumis au format binaire de FHIR (*Binary Resources*), ce qui exclut l'utilisation d'une ressource *Bundle* de type *Document* pour représenter les documents. De plus, ce profil implique un processus d'extraction de documents en plusieurs étapes (génération de liste/recherche, suivie de l'extraction) qui pourrait ne pas être la seule méthode que les responsables de l'implantation adoptent à l'avenir.

Un survol des guides d'implantation de FHIR RESTful montre que ceux qui traitent de l'échange de documents (guides relatifs à l'US Core, l'IPA, PACIO, l'IPS, etc.) décrivent maintenant un patron basé sur la ressource *DocumentReference* et/ou l'opération *$docRef*, comme dans le cas du profil MHD. Ces guides s'en tiennent toutefois à une méthode d'interrogation unidirectionnelle qui consiste à renvoyer des pointeurs vers le contenu du document, où qu'il soit stocké et quel que soit son format (binaire ou assemblage). Des paramètres de recherche et des opérations FHIR ont été créés pour augmenter les capacités de ce patron afin qu'il soit plus facile d'extraire ce qui a été demandé et d'obtenir des documents au format attendu sans devoir modifier le modèle de données/type de document sous-jacent ainsi que les pratiques de cycle de vie.

Dans le contexte du marché canadien, il semble que le niveau de préparation des responsables de l'implantation en ce qui touche les patrons d'échange décrits dans les guides d'implantation de FHIR publiés par HL7 International, notamment l'*US Core Implementation Guide*, ne soit pas approprié dans l'état actuel des choses. C'est pourquoi des patrons d'échange plus simples ont été envisagés comme solutions de rechange viables. L'une de ces solutions, qui est justement le but de la mise à l'essai de la spécification CA:FeX v1.0.0, consiste à s'en tenir à l'échange de documents non binaires et à utiliser les paramètres de recherche FHIR appropriés en fonction des ressources *Bundle* et *Composition* pour rechercher et extraire les documents.

Les versions antérieures de la spécification CA:FeX décrivaient des nouveaux patrons d'utilisation de la ressource *DocumentReference* et des opérations FHIR (CA:FeX 2B, CA:FeX 3B, capacités de pointe (*Cutting Edge Capabilities*)) pour rechercher et extraire les documents dans les dépôts hybrides. Étant donné que l'écosystème actuel se concentre sur la prise en charge des documents FHIR et que les options sont encore testées et évaluées par la communauté d'échange de documents FHIR, ces patrons seront abordés dans une prochaine version de la spécification CA:FeX. À mesure que les spécifications internationales gagneront en maturité et que le marché canadien évoluera, la spécification CA:FeX proposera des solutions plus perfectionnées pour l'échange d'information sur la santé afin de faire converger les intervenants canadiens dans la même direction.

Étant donné que le marché poursuivra son développement, il sera possible à l'avenir d'englober un ensemble plus large de cas d'utilisation qui couvrirait des capacités d'échange d'une information plus atomique.

Parallèlement aux travaux liés à la spécification CA:FeX, Inforoute facilite une initiative de collaboration nationale destinée à élaborer la spécification d'interopérabilité du résumé du dossier du patient pancanadien (RDP-CA), spécification implantable et testable fondée sur le profil IPS d'IHE et sur le guide d'implantation de l'IPS d'HL7. La spécification du RDP-CA renvoie à la spécification CA:FeX comme patron d'implantation facultatif pour la soumission, la recherche et l'extraction d'un résumé du dossier du patient.

## 1.5.1 Contexte

La spécification d'interopérabilité CA:FeX est publiée en ligne dans un espace public de l'outil InfoScribe d'Inforoute, et elle est aussi téléchargeable au format PDF ici. InfoScribe est un outil Web qui permet aux provinces et territoires ainsi qu'aux fournisseurs de créer et de publier de manière collaborative des exigences et spécifications cliniques pour des solutions d'interopérabilité. Les équipes peuvent y consigner et y partager du contenu, des fichiers, des idées, des spécifications, des maquettes, des diagrammes et des projets et y tenir des discussions. Chaque version de la spécification CA:FeX paraîtra en ligne et sous forme de document téléchargeable sur InfoScribe.

## 1.5.2 Introduction à IHE

Integrating the Healthcare Enterprise (IHE) est une initiative internationale destinée à promouvoir l'utilisation de normes garantissant l'interopérabilité entre les systèmes de technologie de l'information sur la santé (TIS) et assurant l'utilisation efficace des DME. Elle offre un forum aux professionnels de la santé, aux experts en TIS et à d'autres intervenants de plusieurs domaines cliniques et opérationnels afin qu'ils s'entendent sur les solutions normalisées à utiliser pour résoudre les problèmes critiques d'interopérabilité.

IHE a essentiellement pour rôle de créer des guides d'implantation, les « profils IHE ». IHE publie chaque profil au terme d'un processus bien défini d'examen public et de mise à l'essai, puis intègre les profils ayant atteint le stade de texte définitif (*Final Text*) dans un cadre technique IHE.

### 1.5.3 Survol des sections du document

Le présent document contient les sections suivantes :

| Section | Description | Public cible |
|---|---|---|
| **Spécification d’interopérabilité CA:FeX** | Cette section présente la spécification CA:FeX, qui est implantable, testable et dérivée des guides d’implantation de FHIR d’HL7. Elle définit les éléments de base qui sous-tendent le patron d’implantation de l'échange d'information sur la santé (EIS) basé sur FHIR. Ces éléments de base sont configurables afin de tenir compte des particularités de chaque province et territoire. La spécification CA:FeX, conforme aux meilleures pratiques à l’échelle mondiale, contient toute l'information dont les responsables de l’implantation ont besoin pour développer les composantes nécessaires à la création, à la consommation et au partage de données cliniques, et elle peut s'appliquer aux systèmes d'information existants et nouveaux. | Développeurs de solutions |
| **Cas d’utilisation et définitions** | Cette section présente le contexte global des éléments d’ordre clinique et opérationnel ainsi que les aspects liés à l’interopérabilité et au développement de solutions qui sont ressortis durant l’élaboration de la spécification CA:FeX. Elle cerne le problème lié aux soins de santé que la spécification CA:FeX vient résoudre et inclut des cas d’utilisation et des exigences d’interopérabilité qui renvoient au contenu de l’architecture de référence (AR), laquelle définit les acteurs et les interactions propres à la spécification CA:FeX. | Chefs de la technologie, dirigeants principaux de l'information, chefs de l’information médicale, P et T et fournisseurs |
| **Échange de documents FHIR** | Cette section présente des méthodes d'implantation des transactions CA:FeX destinées à l'échange de documents à l'aide d’API FHIR RESTful. Lorsque le contenu aura été peaufiné, il formera un guide d’implantation de FHIR à part entière. | Développeurs de solutions |

La section *Spécification d'interopérabilité CA:FeX* est divisée en sous-sections :

- ***Introduction*, et *Préface* :** Ces deux sous-sections offrent une entrée en matière. Elles résument le contexte, le but et la portée du document et expliquent d'autres points fondamentaux qui éclaireront les néophytes au sujet de la spécification CA:FeX et de ses liens avec d'autres spécifications dans l'écosystème de la santé numérique au Canada.
- ***Principes de confidentialité et de sécurité* :** Cette sous-section renvoie à un document récemment publié par Inforoute, *La confidentialité, un outil d'interopérabilité*, qui se veut une introduction au concept de l'interopérabilité et qui fait un survol des lois sur la protection des renseignements personnels sur la santé (RPS) au Canada, avant de proposer quelques approches pratiques pour préserver la confidentialité dans un environnement interopérable. Cette sous-section énonce aussi les facteurs de sécurité à prendre en considération par ceux qui implantent la spécification CA:FeX.
- ***Survol des cas d'utilisation* :** Cette sous-section décrit les cas d'utilisation, dont les contraintes et les hypothèses de conception ainsi que les flux d'information, que couvre la spécification CA:FeX. Elle comporte également des scénarios qui illustrent les flux possibles en contexte canadien.
- ***Exigences d'interopérabilité de base* :** Cette sous-section précise les exigences d'interopérabilité de base de la spécification CA:FeX associées à un patron d'implantation de l'EIS basé sur FHIR. Elle montre aussi les mappages des acteurs des cas d'utilisation avec les acteurs techniques de la spécification d'interopérabilité CA:FeX et avec les services qu'ils prennent en charge, mappages qui correspondent aux flux représentés dans les diagrammes de séquence ici.
- ***Conformité relative aux acteurs CA:FeX* :** Cette sous-section précise les exigences de conformité relatives aux acteurs visés par la spécification CA:FeX.
- ***Acteurs et transactions CA:FeX* :** Cette sous-section résume les acteurs et les transactions visés par la spécification CA:FeX.
- ***Diagrammes de séquence CA:FeX* :** Cette sous-section illustre la manière dont les patrons d'implantation CA:FeX et les profils IHE doivent être appliqués pour répondre aux besoins en interopérabilité du patron d'implantation de l'EIS basé sur FHIR. Les diagrammes regroupent les acteurs et les transactions rattachés à divers profils, dont ceux liés à la spécification CA:FeX, pour refléter la portée des cas d'utilisation.
- ***Indications sur les groupements d'acteurs CA:FeX et de profils IHE* :** Cette sous-section donne des indications sur les groupements d'acteurs CA:FeX et de profils IHE qui permettent de générer d'autres fonctionnalités comme la sécurité du réseau, l'authentification, l'autorisation, l'audit et d'autres.
- ***Indications sur l'audit des transactions CA:FeX* :** Cette sous-section donne des indications relativement à l'audit de chacune des transactions de la spécification CA:FeX.

## 1.5.4 Convention de versionnage

Les versions de la spécification d'interopérabilité CA:FeX seront conservées comme le prévoit le modèle de publication des spécifications d'interopérabilité, présenté ici.

## 1.5.5 Mots-clés des niveaux d'obligation

Les mots-clés suivants indiquent les niveaux d'obligation associés aux exigences opérationnelles de la spécification d'interopérabilité CA:FeX :

- **Doit :** désigne un élément **obligatoire ou requis**, qui doit impérativement être respecté.
- **Devrait :** désigne un élément **recommandé**, c'est-à-dire dont l'implantation est considérée comme une bonne pratique, mais sans être obligatoire (facultatif).
- **Pourrait :** désigne un élément **optionnel** dont l'implantation est permise, mais pas obligatoire.
- **Ne doit pas :** désigne une action ou un élément **interdit**/non autorisé.

Vous trouverez d'autre information sur les exigences opérationnelles de la spécification d'interopérabilité CA:FeX dans la section *Cas d'utilisation et définitions*.

## 1.5.6 Méthodologie

La spécification d'interopérabilité CA:FeX a été élaborée à partir de recherches internationales et à la suite de

consultations avec des experts en la matière d'HIE. Puis, afin de la peaufiner, nous l'avons fait valider auprès des intervenants provinciaux et territoriaux et des fournisseurs participants dans le cadre de réunions de la table de coordination et de la table de direction, d'ateliers et de rencontres individuelles.

### 1.5.7 Approche relative aux cas d'utilisation

L'approche retenue pour l'élaboration des cas d'utilisation de la spécification CA:FeX comprenait les étapes suivantes :

- **Définir les éléments fondamentaux :** Définir les cas d'utilisation, les scénarios et les exigences opérationnelles de base pour le patron d'implantation de l'EIS basé sur FHIR.
- **Collaborer :** Collaborer avec les intervenants provinciaux et territoriaux, les organisations et les fournisseurs participants ainsi qu'avec des experts cliniques et des experts techniques pour développer et détailler des artéfacts.
- **Examiner :** Procéder à un examen des artéfacts et recueillir des commentaires préliminaires dans le cadre d'ateliers et par d'autres moyens.
- **Publier :** Publier les artéfacts et solliciter l'avis d'un plus large éventail d'intervenants.
- **Recommander :** Recommander l'approbation d'artéfacts.
- **Itérer :** Continuer de peaufiner les cas d'utilisation en fonction des tests et des priorités.

### 1.5.8 Cycle de publication

Le cycle de publication de la spécification d'interopérabilité CA:FeX comprend un processus d'examen et de rétroaction en plusieurs étapes, présenté ici.

## 1.6 Principes de confidentialité et de sécurité

### 1.6.1 Principes de confidentialité

Inforoute a publié un document intitulé *La confidentialité, un outil d'interopérabilité*, qui fournit une introduction à l'interopérabilité, fait un survol des lois sur la protection des renseignements personnels sur la santé au Canada (RPS) et propose des approches pratiques de la protection des données médicales en situation d'interopérabilité. Plus particulièrement, le document aborde le rôle que joue la protection des renseignements personnels dans la création de systèmes d'information sur la santé interopérables et déconstruit le mythe selon lequel les lois sur la protection des renseignements personnels empêchent le partage des données des patients. Enfin, il fournit des conseils pour le partage des données médicales en toute sécurité, avec le consentement du patient, et présente les responsabilités des deux parties dans un tel échange.

Vous pouvez télécharger le document en cliquant sur ce lien : *La confidentialité, un outil d'interopérabilité : Introduction à la protection des renseignements personnels sur la santé et à l'interopérabilité*

### 1.6.2 Principes de sécurité

La norme *Fast Healthcare Interoperability Resources* (FHIR) n'est pas un protocole de sécurité, pas plus qu'elle ne définit une fonctionnalité de sécurité. Elle établit par contre des protocoles d'échange et des modèles de contenu qui doivent être utilisés avec différents protocoles de sécurité fondés sur d'autres normes.

Les transactions FHIR visées par le patron d'implantation CA:FeX incluent souvent de l'information sur les patients susceptible d'être exploitée par des personnes ou organisations malveillantes qui en compromettraient la confidentialité. Pour cette raison, toutes les transactions FHIR doivent être dûment sécurisées, par la restriction de l'accès (nombre limité de personnes autorisées), la protection des données en transit et la prise de mesures d'audit appropriées.

Les responsables de l'implantation DEVRAIENT être bien au fait des principes de sécurité associés aux transactions FHIR (http://hl7.org/fhir/R4/security.html), surtout en ce qui touche les éléments suivants :

- Communications
- Authentification
- Autorisation/contrôle de l'accès
- Journaux d'audit
- Signature numérique
- Étiquettes de sécurité
- Description textuelle

Par ailleurs, de nombreuses transactions FHIR reposant sur HTTP REST comprendront des paramètres d'interrogation tels que des identifiants, des quasi-identifiants ou des données médicales sensibles. Par exemple, il arrive couramment que l'identifiant du patient soit utilisé comme paramètre dans une requête. Dans ce patron d'URL, les paramètres d'interrogation sont généralement visibles dans le journal d'audit du serveur ou dans l'historique du navigateur. Il faut donc atténuer le risque que présente cette visibilité directement dans la conception du système ou dans ses modalités d'exécution, notamment par la protection des journaux au même titre que les données sensibles ou par la configuration d'autres mesures dans le système pour prévenir une exposition de l'information.

## 1.7 Survol des cas d'utilisation de la spécification CA:FeX

### 1.7.1 Survol des cas d'utilisation

La présente section décrit deux cas d'utilisation du patron d'implantation de l'EIS basé sur FHIR, dont les contraintes et hypothèses de conception ainsi que les flux d'information visés par la spécification d'interopérabilité CA:FeX. On y présente également des scénarios qui illustrent les flux possibles dans le contexte de la santé numérique au Canada.

### 1.7.2 Portée

La version actuelle de la spécification CA:FeX s'applique aux cas d'utilisation suivants :

- UC-01 Créer et soumettre un document
- UC-02 Rechercher et extraire un document

Ces cas sont présentés en détail dans la section *Cas d'utilisation et définitions*.

### 1.7.3 Acteurs des cas d'utilisation et services

Les acteurs des cas d'utilisation et les services pris en charge dans le cadre de la spécification sont décrits ci-dessous. D'autre information à ce sujet figure dans la section *Exigences d'interopérabilité de base*.

**Acteurs des cas d'utilisation et descriptions**

| Acteur | Description/définition |
|---|---|
| Producteur | Système (DME, SIS, SIC, DSP ou DSE) qui crée/produit des données cliniques à la suite d'une requête d'un professionnel de la santé autorisé, d'un sujet de soins/patient ou d'un autre système autorisé. |
| Consommateur | Système (DME, SIS, SIC, DSP, portail-patients, DSE) qui permet à un professionnel de la santé autorisé ou à un sujet de soins/patient d'accéder à des données cliniques (p. ex. RDP-CA) ou de les recevoir. |
| Dépôt de données cliniques (local ou central) | Espace de stockage partagé pour les documents cliniques qui peut être hébergé localement (c.-à-d. par le producteur de données) ou dans l'infrastructure centrale et auquel les utilisateurs autorisés peuvent |

| Acteur | Description/définition |
|---|---|
| | accéder. |
| Infrastructure centrale | Infrastructure qui recueille l'information médicale provenant des organisations participantes et qui la stocke dans un emplacement centralisé. L'infrastructure offre également des mécanismes de contrôle d'accès. En général, l'infrastructure centrale relève de la province ou du territoire. |

**Mappage des acteurs des cas d'utilisation**

| Acteur | UC-01 | UC-02 |
|---|---|---|
| Producteur | x | |
| Consommateur | | x |
| Dépôt de données cliniques (local ou central) | x | x |
| Infrastructure centrale | x | x |

## 1.8 Exigences d'interopérabilité de base

### 1.8.1 Mappage des acteurs avec les exigences d'interopérabilité

Une description fonctionnelle des acteurs des cas d'utilisation et des services qu'ils prennent en charge figure dans la section *Cas d'utilisation et définitions*. Les services sont requis (R) ou optionnels (O). Les tableaux 1 et 2 ci-dessous montrent le mappage des acteurs des cas d'utilisation avec les acteurs techniques et les services qu'ils prennent en charge. Les trois premières colonnes mentionnent les acteurs des cas d'utilisation, le ou les services connexes et leur optionalité (R ou O). Les quatre autres colonnes (4 à 7) indiquent les modalités de mappage des acteurs des cas d'utilisation avec les exigences d'interopérabilité (acteurs techniques, optionalité et profils) qui doivent être implantées pour permettre aux systèmes d'échanger de l'information sur la santé dans ces cas d'utilisation. Le mappage de ces divers éléments correspond aux flux représentés dans les diagrammes de séquence.

Pour chaque acteur d'un cas d'utilisation, il faut implanter toutes les exigences (certaines sont optionnelles) mentionnées dans la deuxième moitié du tableau (colonnes 4 à 7), à savoir les acteurs techniques, les profils IHE et les normes terminologiques ou autre. Les acteurs techniques sont mappés avec un profil IHE (PDQm, PMIR, etc.) ou avec une « capacité » de CA:FeX, et les renvois figurent dans la dernière colonne. Par contre, les tableaux ne montrent pas toutes les combinaisons possibles de profils et de transactions IHE pour un patron d'implantation particulier. Par exemple, le service « Identification du patient » peut utiliser le profil PIXm au lieu du profil PDQm si le patron d'implantation préféré est PIXm/PMIR.

**Versionnage**

La présente spécification est évolutive; le cycle de publication suppose qu'un certain degré de changement se produira d'une version à l'autre (voir toute l'information sur le modèle de publication ici). Nous mettrons en place un processus pour surveiller les changements apportés aux profils IHE afin qu'ils soient pris en compte dans les versions futures de la spécification d'interopérabilité CA:FeX, comme le prévoit notre feuille de route de l'interopérabilité.

**Versions publiées**

Voici les versions publiées des profils IHE requis et optionnels dont il est question dans la présente spécification. Pour plus d'information, référez-vous à la v0.1.1 de l'AR :

- Profil IUA : Révision 2.1 - mise à l'essai
- Profil PDQm : v2.3.0 : mise à l'essai basée sur FHIR R4
- Profil PMIR : Révision 1.3 – mise à l'essai

**Légende**

R = Requis

O = Optionnel

## 1.8.2 Tableau 1. Exigences d'interopérabilité (conformité) pour le cas d'utilisation 1 : Créer et soumettre un document

| **CAS D'UTILISATION 1 : Créer et soumettre un document** | | | **RENVOIS AUX EXIGENCES D'INTEROPÉRABILITÉ (PROFILS, NORMES, SOUS-SECTIONS DE LA PRÉSENTE SPÉCIFICATION)** | | | |
|---|---|---|---|---|---|---|
| ACTEUR DU CAS D'UTILISATION | SERVICE PRIS EN CHARGE | OPT | ACTEUR TECHNIQUE | OPT | PROFIL/ NORME | RENVOIS |
| Producteur | Authentification de l'utilisateur | O | Client (p. ex. DME) | O | *Internet User Authorization* (IUA) | Se référer à la sous-section *Groupement avec le profil IUA* de la section *Indications sur les groupements d'acteurs CA:FeX et de profils IHE*. |
| | Identification du patient | O | Client (p. ex. DME) | O | Utiliser les normes existantes dans le système clinique. | N/A |
| | | O | Consommateur de données démographiques du patient | O | PDQm | Se référer à la section sur le profil PDQm dans la v0.1.1 de l'AR. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Extraction des données cliniques (ID du patient) | R | Client (p. ex. DME) | R | Utiliser les normes existantes dans le système clinique. | N/A |
| | Assemblage et affichage du document | R | Client (p. ex. DME) | R | Utiliser les normes existantes dans le système clinique. | N/A |
| | Omission ou masquage des données selon la politique de la province/du territoire | O | Client (p. ex. DME) | O | Exigence provinciale/ territoriale | N/A |
| | Enregistrement du document dans le dépôt de données cliniques | R | Client (p. ex. DME) | R | Utiliser les normes existantes dans le système clinique. | N/A |
| | | R | Source de données | R | CA:FeX | Se référer à la sous-section *Soumettre un document* de la section *Échanger des documents FHIR*. |
| Dépôt de données cliniques (central) | Enregistrement de la ressource *Bundle* dans le dépôt de données cliniques | R | Destinataire de données | R | CA:FeX | Se référer à la sous-section *Soumettre un document* de la section *Échanger des documents FHIR*. |
| Infrastructure centrale | Identification du patient | O | Registre d'ID du patient | O | PMIR | Se référer à la section sur le profil PMIR dans la v0.1.1 de l'AR. |

### 1.8.3 Tableau 2. Exigences d'interopérabilité (conformité) pour le cas d'utilisation 2 : Rechercher et extraire un document

| **CAS D'UTILISATION 2 : Rechercher et extraire un document** | | | **RENVOIS AUX EXIGENCES D'INTEROPÉRABILITÉ (PROFILS, NORMES, SOUS-SECTIONS DE LA PRÉSENTE SPÉCIFICATION)** | | | |
|---|---|---|---|---|---|---|
| ACTEUR DU CAS D'UTILISATION | SERVICE PRIS EN CHARGE | OPT | ACTEUR TECHNIQUE | OPT | PROFIL/ NORME | RENVOIS |
| Consommateur | Authentification de l'utilisateur | O | Client (p. ex. DME) | O | *Internet User Authorization* (IUA) | Se référer à la sous-section *Groupement le profil IUA* de la section *Indications sur les groupements d'acteurs CA:FeX et de profils IHE*. |
| | Identification du patient | O | Client (p. ex. DME) | O | Utiliser les normes existantes dans le système clinique. | N/A |
| | | O | Consommateur de données démographiques du patient | O | PDQm | Se référer à la section sur le profil PDQm dans la v0.1.1 de l'AR. |
| | Requête de recherche de document (ID du patient) | R | Client (p. ex. DME) | R | Utiliser les normes existantes dans le système clinique. | N/A |
| | Requête de document (ID de la ressource) | R | Client (p. ex. DME) | R | Utiliser les normes existantes dans le système clinique. | N/A |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Obtention d'une ressource *Bundle* de type *Searchset* | R | Consommateur de données | R | CA:FeX | Se référer à la sous-section *Rechercher un document* de la section *Échanger des documents FHIR*. |
| | Obtention d'une ressource *Bundle* de type *Document* | R | Consommateur de données | R | CA:FeX | Se référer à la sous-section *Extraire un document* de la section *Échanger des documents FHIR*. |
| Dépôt de données cliniques (central) | Extraction des ressources du dépôt de données cliniques | R | Répondeur de données | R | CA:FeX | Se référer à la sous-section *Rechercher un document* de la section *Échanger des documents FHIR*. |
| | Extraction d'une ressource *Bundle* du dépôt de données cliniques | R | Répondeur de données | R | CA:FeX | Se référer à la sous-section *Extraire un document* de la section *Échanger des documents FHIR*. |
| Infrastructure centrale | Identification du patient | O | Registre d'ID du patient | O | PMIR | Se référer à la section sur le profil PMIR de la v0.1.1 de l'AR. |

## 1.9 Conformité relative aux acteurs

Pour qu'un système soit jugé conforme à la spécification d'interopérabilité CA:FeX, il faut en démontrer la conformité par rapport à au moins l'un des acteurs d'un cas d'utilisation (première colonne du Tableau 1 et du Tableau 2 de la section *Exigences d'interopérabilité de base*). Un système pourrait être déclaré conforme pour un ou plusieurs des quatre acteurs suivants :

- Producteur
- Consommateur
- Dépôt de données cliniques (local ou central)
- Infrastructure centrale

Les rôles de « producteur » et de « consommateur » incomberont essentiellement aux fournisseurs de DME, tandis que les rôles de « dépôt de données cliniques » et « infrastructure centrale » relèveront des fournisseurs de DME ou bien de la province/du territoire, selon l'approche d'implantation retenue. De même, un portail-patients pourrait faire office de « consommateur », auquel cas ce rôle serait assumé par un

fournisseur ou la province/le territoire, selon ce que prévoient ses politiques en matière d'accès du patient/sujet de soins à ses RPS.

Pour confirmer que le système peut prendre entièrement en charge la v1.0.0 de la spécification d'interopérabilité CA:FeX, il faut en démontrer la conformité relativement à chaque acteur et transaction pour lesquels le système est censé être conforme.

### 1.9.1 Contraintes relatives aux acteurs des cas d'utilisation

La présente section décrit certaines des contraintes de conception devant être appliquées aux acteurs des cas d'utilisation lorsqu'on développe les fonctionnalités qui permettent la prise en charge des services avec lesquels ces acteurs ont mappés.

**Note** : Les paragraphes qui suivent portent uniquement sur les contraintes applicables aux acteurs et aux transactions visés par la spécification d'interopérabilité CA:FeX (voir la section *Acteurs et transactions CA:FeX*). Deux services clés sont pris en charge par CA:FeX :

- Enregistrer un document dans le dépôt de données cliniques
- Extraire un document du dépôt de données cliniques

Les contraintes de conception exposées plus bas sont nécessaires à l'implantation de ces deux services à l'aide d'API RESTful fondées sur CA:FeX et FHIR. Leur prise en charge est rendue possible grâce à trois transactions RESTful :

| Service pris en charge | Transactions FHIR RESTful |
|---|---|
| Enregistrer un document dans le dépôt de données cliniques | 1. Soumettre des données [CA:FeX-1] |
| Extraire un document du dépôt de données cliniques | 2. Rechercher des données [CA:FeX-2] |
| | 3. Extraire des données [CA:FeX-3] |

#### Enregistrer un document dans le dépôt de données cliniques

Les acteurs « producteur » et « dépôt de données cliniques » du cas d'utilisation sont requis pour l'implantation du service *Enregistrer un document dans le dépôt de données cliniques*.

Ces acteurs doivent utiliser la transaction **Soumettre des données [CA:FeX-1]** pour exécuter une requête de type *Soumettre des données* depuis une source de données jusqu'à un destinataire de données.

**Soumettre des données [CA:FeX-1]**

Ce message correspond à une requête, par une source de données, de transfert d'un document FHIR à un destinataire de données. La requête est reçue par un destinataire de données, qui stocke le document FHIR et répond par un code HTTP.

*Événement déclencheur*

Lorsqu'une source de données doit soumettre un ou plusieurs documents FHIR à un destinataire de données (dépôt de données cliniques).

*Sémantique du message*

Ce message consiste en une requête HTTP POST ciblant le point d'extrémité « submit-data » pour demander le transfert des métadonnées et des documents sous la forme d'une transaction FHIR. La source de données doit initier une transaction FHIR qui utilise une action de « création » (*create*) en envoyant une requête HTTP POST composée d'une ressource FHIR. Le corps du message HTTP doit prendre en charge le type de média « application/fhir+json » et devrait prendre en charge le type de média « application/fhir+xml ». D'autre

information sur ce patron d'implantation FHIR figure dans la sous-section *Soumettre un document* de la section *Échanger des documents FHIR*.

*Actions attendues*

Le destinataire de données doit accepter les types de média « application/fhir+json » et « application/fhir+xml ». À la réception de la requête, le destinataire de données doit valider les ressources et envoyer l'un des codes de réponse HTTP et un message OperationOutcome, s'il y a lieu. D'autre information à ce sujet figure dans la sous-section *Gestion des réponses* de la section *Échanger des documents FHIR*.

## Extraire le document du dépôt de données cliniques

Les acteurs « consommateur » et « dépôt de données cliniques (central) » du cas d'utilisation sont requis pour l'implantation du service *Extraire un document du dépôt de données cliniques*.

Ces acteurs doivent utiliser les transactions **Rechercher des données [CA:FeX-2]** et **Extraire des données [CA:FeX-3]** pour trouver des métadonnées et extraire un document clinique.

### Rechercher des données [CA:FeX-2]

Ce message consiste en une requête à l'aide de paramètres (interrogation paramétrée) par un consommateur de données qui recherche des documents FHIR. La requête est reçue par un répondeur de données qui envoie une ressource *Bundle* contenant les résultats correspondant aux paramètres de recherche.

Le consommateur de données pourrait utiliser les méthodes HTTP GET ou HTTP POST. Le répondeur de données doit donc prendre en charge ces deux méthodes.

*Événement déclencheur*

Lorsqu'un consommateur de données doit trouver une liste de ressources FHIR *Bundle* ou extraire des documents qui sont censés comprendre une combinaison de ressources FHIR « assemblées » (*Composition*) et « binaires » (*Binary*).

*Sémantique du message*

Le consommateur de données exécute une requête HTTP ciblant le point d'extrémité du répondeur de données (dépôt FHIR).

Le consommateur de données pourrait utiliser les méthodes HTTP GET ou HTTP POST. Le répondeur de données doit donc prendre en charge l'une et l'autre.

GET [base]/[resourcetype]?name=value&...

POST [base]/[type]/_search{?[parameters]{&_format=[mime-type]}}

*Paramètres de recherche*

Les paramètres de recherche suivants sont généralement utilisés pour l'extraction de documents.

D'autres paramètres de recherche propres aux exigences d'un cas d'utilisation ou d'un guide d'implantation (p. ex. RDP-CA) pourront être définis au besoin par les responsables de l'implantation.

| Paramètre de recherche | Appliqué à… | Description |
|---|---|---|
| timestamp (*estampille temporelle*) | bundle.timestamp | Ce paramètre de type date précise le moment où la ressource FHIR *Bundle* a été créée. Voir la page http://hl7.org/fhir/R4/search.html#date pour plus d'information sur le paramètre de type date. |

| | | |
|---|---|---|
| patient.identifier (*identifiant du patient*) | bundle.composition.patient.identifier | Ce paramètre de type jeton précise un identifiant associé au patient auquel le document est assigné. L'utilisation de bundle.composition.patient.identifier suit la méthode de recherche en chaîne FHIR. |
| type | bundle.composition.type | Ce paramètre de type jeton précise le type de document (LOINC, si possible). L'utilisation de bundle.composition.type suit la méthode de recherche en chaîne FHIR. |
| status (*statut*) | bundle.composition.status | Ce paramètre de type jeton précise le statut de la composition. L'utilisation de bundle.composition.status suit la méthode de recherche en chaîne FHIR. |
| author (*auteur*) | bundle.composition.author | Ce paramètre de type référence indique l'auteur du document (personne et/ou système). L'utilisation de bundle.composition.author suit la méthode de recherche en chaîne FHIR. |
| date | bundle.composition.date | Ce paramètre de type date précise le moment où la référence du document créée. L'utilisation de bundle.composition.date suit la méthode de recherche en chaîne FHIR. |

Vous trouverez d'autre information sur ce patron d'implantation FHIR et des options de patrons de recherche de documents dans la sous-section *Rechercher un document* de la section *Échanger des documents FHIR*.

*Actions attendues*

Le répondeur de données doit traiter la requête et envoyer des résultats qui correspondent aux critères de recherche. La norme FHIR sert à coder les réponses au format XML ou JSON.

Vous trouverez d'autre information à ce sujet dans la sous-section *Gestion des réponses* de la section *Échanger des documents FHIR*.

*Principes de sécurité*

Le répondeur de données DOIT rejeter toute requête non autorisée en envoyant le code d'erreur HTTP 401 *Unauthorized* (non autorisé). Dans le cadre de cette transaction, le répondeur ne devrait pas envoyer de l'information à laquelle le consommateur de données n'est pas autorisé à accéder (l'autorisation vaut également pour le système, l'application et l'utilisateur, conformément à la politique locale, à la directive de consentement du patient et aux couches de sécurité). Le répondeur pourrait cependant envoyer une ressource *Bundle* qui contient les résultats de recherche avec des éléments de type *Reference* auxquels le consommateur de données pourrait ne pas avoir accès. Autrement dit, l'autorisation d'accès ne doit s'appliquer qu'au contenu de la ressource *Bundle*, et il pourrait y avoir des renvois (URL) vers du contenu auquel l'accès n'est pas autorisé. Cela est considéré comme approprié, car le consommateur de données devrait extraire le contenu vers lequel renvoient ces URL, et, à ce moment-là, la décision d'autoriser ou non l'accès serait prise en fonction du contexte et du contenu. Ainsi, il est possible pour un consommateur de données d'obtenir des ressources qui renvoient à des données qu'il n'est pas autorisé à extraire. Par conséquent, les URL doivent être formulées avec soin pour éviter d'exposer des données sensibles dans cette valeur.

**Extraire des données [CA:FeX-3]**

Ce message correspond à une requête, par un consommateur de données, d'extraction de documents à l'aide

d'un ID de ressources qui est connu du dépôt de données cliniques. La requête est reçue par un répondeur de données, qui transmet le document FHIR demandé ou un code de réponse HTTP.

Ce message consiste en une requête HTTP GET pour extraire, du dépôt central de données cliniques, le document FHIR demandé.

*Événement déclencheur*

Lorsque qu'un consommateur de données doit extraire un document FHIR.

*Sémantique du message*

Le consommateur de données envoie une requête HTTP GET au serveur à partir d'un ID de ressource déjà connu du répondeur de données. Le répondeur de données transmet alors soit une ressource *Bundle* dont l'ID avait déjà été utilisé dans une recherche/extraction antérieure, soit une pièce jointe dans une ressource de type *DocumentReference* ou binaire (*Binary Resource*).

GET [base]/[resourcetype]?name=value&...

Vous trouverez d'autre information sur ce patron d'implantation FHIR et des options de patrons de recherche de documents dans la sous-section *Rechercher un document* de la section *Échanger des documents FHIR*.

*Actions attendues*

Le répondeur de données doit traiter la requête GET et répondre en envoyant le document FHIR correspondant à l'ID inclus dans la requête. Il doit aussi envoyer en réponse le code HTTP 200 (*OK*). Le corps du message doit comprendre le contenu du document demandé.

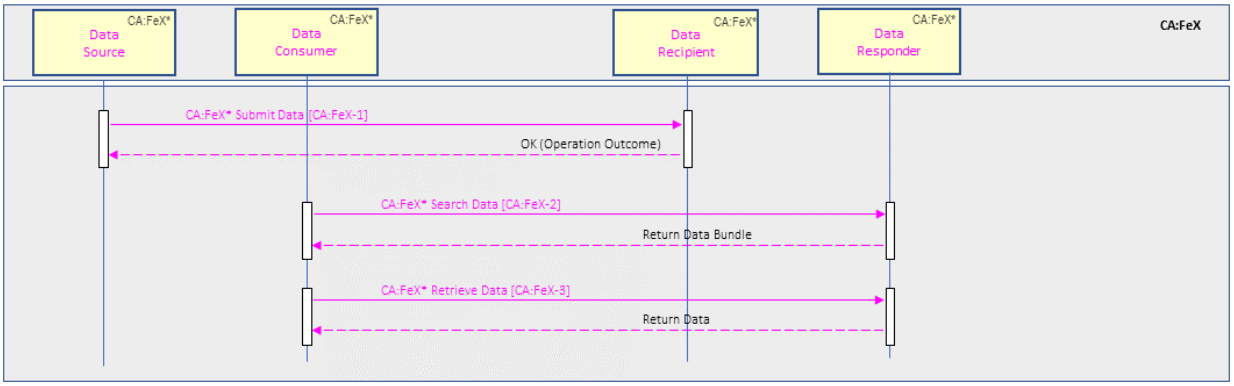
Vous trouverez d'autre information à ce sujet dans la sous-section *Gestion des réponses* de la section *Échanger des documents FHIR*.

*Principes de sécurité*

Le répondeur de données DOIT rejeter toute requête non autorisée en envoyant le code d'erreur HTTP 401 *Unauthorized* (non autorisé). Dans le cadre de cette transaction, le répondeur ne devrait pas envoyer de l'information à laquelle le consommateur de données n'est pas autorisé à accéder.

## 1.10 Acteurs et transactions CA:FeX

Ce diagramme illustre les acteurs et transactions visés par la spécification d'interopérabilité CA:FeX.




La spécification d'interopérabilité CA:FeX définit trois transactions principales, qui se déclinent en sous-transactions (voir le tableau ci-dessous) s'appliquant à des circonstances particulières. Référez-vous à la section *Échanger des documents FHIR* pour plus d'information sur les sous-transactions.

| ID de transaction | Description | Note |
|---|---|---|

| | | |
|---|---|---|
| CA:FeX-1 | Soumettre des données | |
| CA:FeX-2 | CA:FeX-2A : Rechercher un document dans un dépôt de documents FHIR assemblés | |
| | CA:FeX-2B : Rechercher un document dans un dépôt de documents hybrides | Sous-transaction envisagée |
| CA:FeX-3 | CA:FeX-3A : Extraire un document d'un dépôt de documents FHIR assemblés | |
| CA:FeX-3 | CA:FeX-3B : Extraire un document d'un dépôt de documents FHIR hybrides | Sous-transaction envisagée |

## 1.11 Diagrammes de séquence CA:FeX

Les diagrammes de séquence CA:FeX illustrent la manière dont les patrons d'implantation CA:FeX et les profils IHE doivent être appliqués pour répondre aux besoins en interopérabilité du patron d'implantation de l'EIS basé sur FHIR. Les diagrammes regroupent les acteurs et les transactions rattachés à divers profils, dont ceux liés à la spécification CA:FeX, pour refléter la portée des cas d'utilisation.

### 1.11.1 Diagramme de séquence d'UC-01 : Créer et soumettre un document

**Scénario :** La solution clinique A extrait un document d'un dépôt central de données cliniques.

**Hypothèse :** Le document est stocké dans un dépôt central de données cliniques.

Le diagramme de séquence du cas d'utilisation UC-01 illustre l'option consistant à utiliser la spécification d'interopérabilité CA:FeX pour enregistrer des données (documents) dans un dépôt central de données cliniques et extraire des données (documents) d'un dépôt central de données cliniques. Ce scénario comprend deux acteurs : une source de données et un destinataire de données. Il utilise l'opération FHIR *Soumettre des données*.

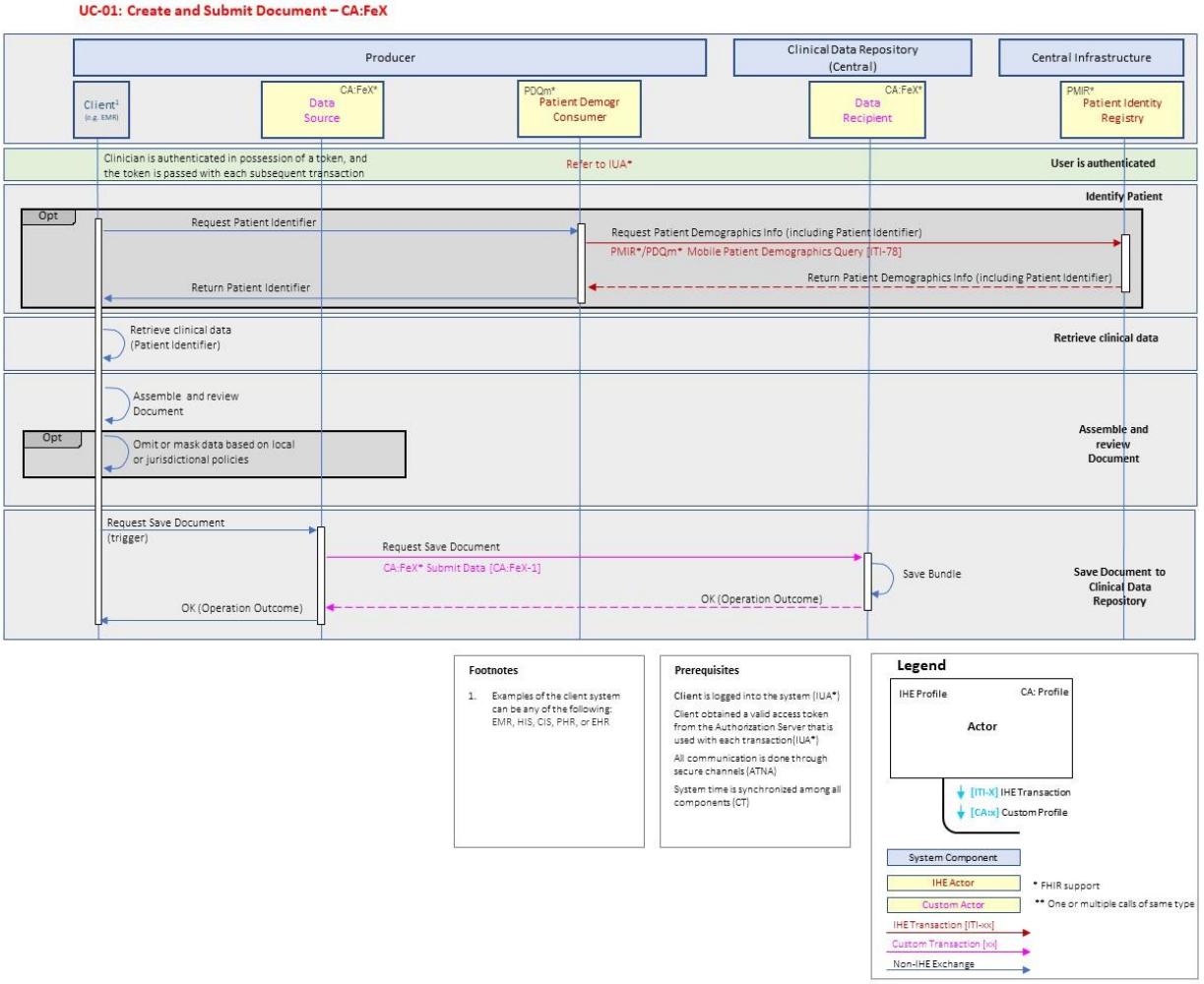
**Précisions concernant le diagramme de séquence d'UC-01**

Voici quelques précisions qui faciliteront la lecture du diagramme de séquence :

- Le diagramme de séquence montre la façon dont les différents acteurs normalisés d'un système devraient interagir pour effectuer les transactions normalisées spécifiques, et l'ordre dans lequel les transactions et les interactions se produisent lorsque le cas d'utilisation UC-01 de la spécification CA:FeX est exécuté.
- La légende dans le coin inférieur droit décrit les composants du système, les acteurs et les transactions qui sont nécessaires à l'exécution du cas d'utilisation.
- Le couloir vert offre une vue simplifiée des acteurs et des transactions requis par les profils fondamentaux, présentés ici, auxquels s'ajoutent des profils qui ne figurent pas explicitement dans le diagramme (ATNA, CT, etc.) mais qui sont inclus dans une note en encadré. Il s'agit de conditions préalables pour le cas d'utilisation, et on présume qu'elles auront été remplies.
- Les couloirs bleus regroupent la séquence de processus (ainsi que les acteurs et les transactions requis pour chacun des processus) qui doit être observée pour l'exécution du cas d'utilisation. Il faut lire ces couloirs de gauche à droite et de haut en bas.
- Les encadrés avec des notes en rouge signalent des points importants et fournissent davantage de contexte.
- Pour plus d'information sur les profils IHE de base et les indications sur l'implantation au Canada, référez-vous à la v0.1.1 de l'AR.

**Autres précisions**

Les diagrammes de séquence d'UC-01 et d'UC-02 ne montrent pas toutes les combinaisons possibles de profils et de transactions IHE pour chaque patron d'implantation. Par exemple, une transaction ITI-83 peut être utilisée à la place d'une transaction ITI-78 si le patron d'implantation préféré est PIXm/PMIR.




## 1.11.2 Diagramme de séquence d'UC:02 : Rechercher et extraire un document

**Scénario:** La solution clinique A extrait des données cliniques d'un dépôt central de données cliniques.

**Hypothèse :** Les données cliniques sont stockées dans un dépôt central de données cliniques.

Le diagramme de séquence du cas d'utilisation UC-02 illustre l'option consistant à utiliser la spécification d'interopérabilité CA:FeX pour enregistrer des données (documents) dans un dépôt central de données cliniques et extraire des données (documents) d'un dépôt central de données cliniques. Ce scénario comprend deux acteurs : un consommateur de données et un répondeur de données. Il utilise les opérations FHIR *Rechercher des données* et *Extraire des données*.

**Précisions concernant le diagramme de séquence d'UC-02**

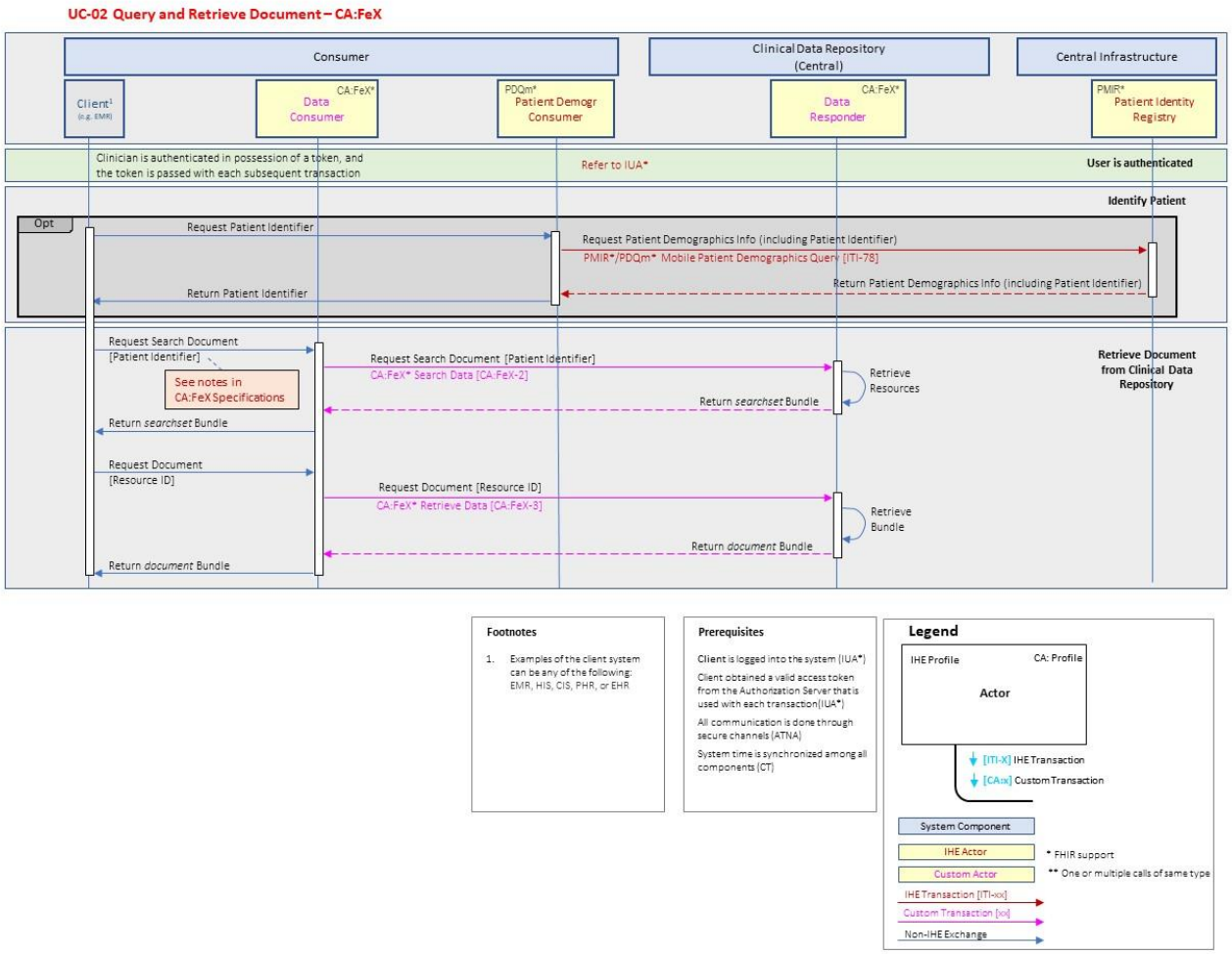
Voici quelques précisions qui faciliteront la lecture du diagramme de séquence :

- Le diagramme de séquence montre la façon dont les différents acteurs normalisés d'un système devraient interagir pour effectuer les transactions normalisées spécifiques, et l'ordre dans lequel les transactions et les interactions se produisent lorsque le cas d'utilisation UC-02 de la spécification CA:FeX est exécuté.

- Le rôle du consommateur de données varie selon le type de client :
  - Si le client est un PS, le consommateur de données est une solution clinique (p. ex. un DME) utilisée par le PS pour demander et obtenir l'accès à un document clinique qui serait extrait du dépôt de données cliniques.
  - Si le client est un patient, le consommateur de données est un portail-patient utilisé par le patient/sujet de soins pour demander et obtenir l'accès à un document clinique qui serait extrait du dépôt de données cliniques.
- La légende dans le coin inférieur droit décrit les composants du système, les acteurs et les transactions qui sont nécessaires à l'exécution du cas d'utilisation.
- Le couloir vert offre une vue simplifiée des acteurs et des transactions requis par les profils fondamentaux, présentés ici, auxquels s'ajoutent des profils qui ne figurent pas explicitement dans le diagramme (ATNA, CT, etc.) mais qui sont inclus dans une note en encadré. Il s'agit de conditions préalables pour le cas d'utilisation, et on présume qu'elles auront été remplies.
- Les couloirs bleus regroupent la séquence de processus (ainsi que les acteurs et les transactions requis pour chacun des processus) qui doit être observée pour l'exécution du cas d'utilisation. Il faut lire ces couloirs de gauche à droite et de haut en bas.
- Les encadrés avec des notes en rouge signalent des points importants et fournissent davantage de contexte.
- Pour plus d'information sur les profils IHE de base et les indications sur l'implantation au Canada, référez-vous à la v0.1.1 de l'AR.

**Autres précisions**

Les diagrammes de séquence d'UC-01 et d'UC-02 ne montrent pas toutes les combinaisons possibles de profils et de transactions IHE pour chaque patron d'implantation. Par exemple, une transaction ITI-83 peut être utilisée à la place d'une transaction ITI-78 si le patron d'implantation préféré est PIXm/PMIR.




## 1.12 Indications sur les groupements d'acteurs CA:FeX et de profils IHE

Cette section fournit des indications sur les groupements d'acteurs CA:FeX et de profils IHE qui permettent de générer d'autres fonctionnalités comme la sécurité du réseau, l'authentification, l'autorisation, l'audit et d'autres.

### 1.12.1 Groupement avec le profil CT

Le profil CT (*Consistnt Time*, ou synchronisation du temps) permet de bien synchroniser les horloges et les horodateurs des ordinateurs d'un réseau. Pour générer cette fonctionnalité, on groupe les acteurs CA:FeX avec des acteurs du profil CT.

Pour des indications sur l'implantation du profil CT en contexte canadien, référez-vous à la section *Indications sur l'implantation du profil CT au Canada* de la v0.1.1 de l'AR.

Une fois groupé, l'acteur CA:FeX implantera les transactions et/ou les modules requis dans CA:FeX, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| **Acteur CA:FeX** | **Acteur avec lequel il est groupé** |
|---|---|
| Source de données | CT / Time Client (client de temps) |

| Acteur CA:FeX | Acteur avec lequel il est groupé |
|---|---|
| Destinataire de données | CT / Time Client (client de temps) |
| Consommateur de données | CT / Time Client (client de temps) |
| Répondeur de données | CT / Time Client (client de temps) |

## 1.12.2 Groupement avec le profil IUA

Le profil IUA (*Internet User Authorization*, ou autorisation de l'utilisateur Internet) prend en charge l'authentification de l'utilisateur et de l'application ainsi que les décisions d'autorisation connexes. Pour générer cette fonctionnalité, on groupe les acteurs CA:FeX avec des acteurs du profil IUA.

Pour des indications sur l'implantation du profil IUA en contexte canadien, référez-vous à la section *Indications sur l'implantation du profil IUA au Canada* de la v0.1.1 de l'AR.

Une fois groupé, l'acteur CA:FeX implantera les transactions et/ou les modules requis dans CA:FeX, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| Acteur CA:FeX | Acteur avec lequel il est groupé |
|---|---|
| Source de données | IUA / Authorization Client (client d'autorisation) |
| Destinataire de données | IUA / Resource Server (serveur de ressources) |
| Consommateur de données | IUA / Authorization Client (client d'autorisation) |
| Répondeur de données | IUA / Resource Server (serveur de ressources) |

**Lorsqu'ils sont groupés avec l'acteur « Authorization Client » (client d'autorisation) du profil IUA**, **les acteurs « source de données » et « consommateur de données » de CA:FeX** utiliseront la transaction *Get Access Token* [ITI-71] pour demander un jeton d'accès (champ d'application équivalent) au serveur d'autorisation (*IUA Authorization Server*).

L'acteur CA:FeX pourra ainsi soumettre la transaction CA:FeX correspondante en combinaison avec la transaction *Incorporate Access Token* [ITI-72].

**Lorsqu'ils sont groupés avec l'acteur « Resource Server » (serveur de ressources) du profil IUA, les acteurs « destinataire de données » et « répondeur de données »** exigeront l'ajout du jeton d'accès (*Incorporate Access Token* [ITI-72]) dans toutes les requêtes de transactions CA:FeX, appliqueront la décision d'autorisation dans le jeton et pourraient appliquer des politiques autres que celles du serveur d'autorisation, notamment des règles de consentement ou règles métier.

Ce groupement offre d'autres fonctionnalités en matière de sécurité et de confidentialité :

- les transactions sont combinées aux transactions IUA exigeant des jetons d'accès
- la définition du champ d'application de chaque transaction permet d'activer des exigences et des fonctionnalités supplémentaires

| Acteur | Transaction | Champ d'application IUA/OIDC |
|---|---|---|
| Source de données | Soumettre des données [CA:FeX-1] | CAFEX-1 |

| Acteur | Transaction | Champ d'application IUA/OIDC |
|---|---|---|
| Destinataire de données | Soumettre des données [CA:FeX-1] | CAFEX-1 |
| Consommateur de données | Rechercher des données [CA:FeX-2] | CAFEX-2 |
| | Extraire des données [CA:FeX-3] | CAFEX-3 |
| Répondeur de données | Rechercher des données [CA:FeX-2] | CAFEX-2 |
| | Extraire des données [CA:FeX-3] | CAFEX-3 |

Chaque champ d'application autorise pleinement la transaction CA:FeX et permet implicitement d'exécuter des opérations CRUD/S (créer, lire, mettre à jour, supprimer/rechercher) pour un patient donné qui sont prises en charge par les transactions CA:FeX correspondantes.

Il est possible de préciser davantage un champ d'application dans des situations propres à un domaine ou à un projet; ce champ d'application s'ajouterait à celui qui est défini ici.

## 1.12.3 Groupement avec CA:Sec

L'AR fournit des indications sur l'implantation, en contexte canadien, des éléments du profil ATNA destinés à sécuriser le réseau. Pour plus d'information à ce sujet, référez-vous à la section *Indications sur l'implantation de CA:Sec* de la v0.1.1 de l'AR**.**

L'élément CA:Sec (*Canadian Network Security*, ou sécurité du réseau canadien) définit des capacités permettant d'assurer la sécurité des communications du réseau. Pour générer cette fonctionnalité, on groupe les acteurs CA:FeX avec un acteur CA:Sec.

Une fois groupé, l'acteur CA:FeX implantera les transactions et/ou les modules requis dans CA:FeX, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| Acteur CA:FeX | Acteur avec lequel il est groupé |
|---|---|
| Source de données | CA:Sec / Secure Application (application sécurisée) |
| Destinataire de données | CA:Sec / Secure Application (application sécurisée) |
| Consommateur de données | CA:Sec / Secure Application (application sécurisée) |
| Répondeur de données | CA:Sec / Secure Application (application sécurisée) |

**Lorsqu'ils sont groupés avec l'acteur « Secure Application » (application sécurisée) de CA:Sec, les acteurs CA:FeX** utiliseront la transaction *Authenticate Node* [ITI-19] pour sécuriser les communications entre les acteurs.

## 1.12.4 Groupement avec CA:Aud

L'AR fournit des indications sur l'implantation, en contexte canadien, des éléments du profil ATNA nécessaires à l'audit des transactions. Pour plus d'information à ce sujet, référez-vous à la section *Indications sur l'implantation de CA:Aud* de la v0.1.1 de l'AR**.**

L'élément CA:Aud (*Canadian Audit Trail*, ou piste d'audit canadien) définit des capacités de journalisation

d'événements à des fins d'audit. Pour générer cette fonctionnalité, on groupe les acteurs CA:FeX avec des acteurs CA:Aud.

Une fois groupé, l'acteur CA:FeX implantera les transactions et/ou les modules requis dans CA:FeX, ***en plus de toutes*** les transactions exigées pour l'acteur avec lequel il est groupé (deuxième colonne).

| Acteur CA:FeX | Acteur avec lequel il est groupé |
|---|---|
| Source de données | CA:Aud / Audit Creator (créateur d'enregistrements d'audit) |
| Destinataire de données | CA:Aud / Audit Creator (créateur d'enregistrements d'audit) |
| Consommateur de données | CA:Aud / Audit Creator (créateur d'enregistrements d'audit) |
| Répondeur de données | CA:Aud / Audit Creator (créateur d'enregistrements d'audit) |

**Lorsqu'ils sont groupés avec l'acteur « Audit Creator » (créateur d'enregistrements d'audit) de CA:Aud, les acteurs CA:FeX** utiliseront la transaction *Record Audit Event* [ITI-20] pour envoyer les messages du journal des événements d'audit à un dépôt d'enregistrements d'audit (*Audit Record Repository*).

## 1.13 Principes d'audit des transactions CA:FeX

Pour la prise en charge des activités d'audit, il est recommandé de grouper les acteurs CA:FeX avec des acteurs CA:Aud (voir la sous-section *Groupement avec CA:Aud* de la section *Indications sur les groupements d'acteurs CA:FeX et de profils IHE*.

Il est également possible d'utiliser des méthodes autres que les profils IHE pour enregistrer les messages d'audit, méthodes qui ne nécessitent pas de groupement avec les acteurs CA:Aud.

Les critères d'audit sont définis pour chaque acteur d'une transaction CA:FeX.

### 1.13.1 Audit d'une transaction *Soumettre des données* [CA:FeX-1]

Les critères d'audit sont semblables à ceux appliqués aux autres transactions IHE destinées à l'exportation de documents, comme la transaction *MHD Provide Document Bundle* [ITI-65].

#### Audit de la source de données

Lorsqu'il est groupé avec les acteurs « Secure Node » ou « Secure Application » (application sécurisée) du profil ATNA, l'acteur « Source de données » pourra enregistrer un événement d'audit pour la transaction *Soumettre des données* (*Submit Data Source Audit Event Log*).

*Liens terminologiques*

| Chemin d'accès | Conformité | Ensemble de valeurs/codes |
|---|---|---|
| AuditEvent.language | preferred (lien recommandé) | CommonLanguages<br>**Max Binding**: AllLanguages |
| AuditEvent.type | extensible (lien extensible) | Patron : 110106 *Export* (Exporter) |

| | | |
|---|---|---|
| AuditEvent.subtype | extensible (lien extensible) | Patron : CA:FeX-1 *Submit Data* (Soumettre des données) |
| AuditEvent.action | required (lien requis) | Patron : R |
| AuditEvent.outcome | required (lien requis) | AuditEventOutcome |
| AuditEvent.purposeOfEvent | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent.type | extensible (lien extensible) | ParticipationRoleType |
| AuditEvent.agent.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataSource.type | extensible (lien extensible) | Patron : 110153 *Source Role ID* (ID du rôle de la source) |
| AuditEvent.agent:dataSource.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataSource.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataSource.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataSource.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataRecipient.type | extensible (lien extensible) | Patron : 110152 *Destination Role ID* (ID du rôle du destinataire) |
| AuditEvent.agent:dataRecipient.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataRecipient.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataRecipient.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataRecipient.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.source.type | extensible (lien extensible) | AuditEventSourceType |
| AuditEvent.entity.type | extensible (lien extensible) | AuditEventEntityType |

| | | |
|---|---|---|
| AuditEvent.entity.role | extensible (lien extensible) | AuditEventEntityRole |
| AuditEvent.entity.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:patient.type | extensible (lien extensible) | Patron : 1 *Person* (Personne) |
| AuditEvent.entity:patient.role | extensible (lien extensible) | Patron : 1 *Patient* |
| AuditEvent.entity:patient.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:patient.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:submissionSet.type | extensible (lien extensible) | Patron : 2 *System Object* (Objet système) |
| AuditEvent.entity:submissionSet.role | extensible (lien extensible) | Patron : 20 *Job* (Travail) |
| AuditEvent.entity:submissionSet.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:submissionSet.security Label | extensible (lien extensible) | All Security Labels |

## Audit du destinataire de données

Lorsqu'il est groupé avec les acteurs « Secure Node » (nœud sécurisé) ou « Secure Application » (application sécurisée) du profil ATNA, l'acteur « Destinataire de données » pourra enregistrer un événement d'audit pour la transaction *Soumettre des données* (*Submit Data Recipient Audit Event Log*).

*Liens terminologiques*

| **Chemin d'accès** | **Conformité** | **Ensemble de valeurs/codes** |
|---|---|---|
| AuditEvent.language | preferred (lien recommandé) | CommonLanguages<br>**Max Binding**: AllLanguages |
| AuditEvent.type | extensible (lien extensible) | Patron : 110107 *Import* (Importer) |
| AuditEvent.subtype | extensible (lien extensible) | Patron : CA:FeX-1 *Submit Data* (Soumettre des données) |
| AuditEvent.action | required (lien requis) | Patron : C |
| AuditEvent.outcome | required (lien requis) | AuditEventOutcome |
| AuditEvent.purposeOfEvent | extensible (lien extensible) | PurposeOfUse |

| | | |
|---|---|---|
| AuditEvent.agent.type | extensible (lien extensible) | ParticipationRoleType |
| AuditEvent.agent.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataSource.type | extensible (lien extensible) | Patron : 110153 *Source Role ID* (ID du rôle de la source) |
| AuditEvent.agent:dataSource.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataSource.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataSource.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataSource.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataRecipient.type | extensible (lien extensible) | Patron : 110152 *Destination Role ID* (ID du rôle du destinataire) |
| AuditEvent.agent:dataRecipient.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataRecipient.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataRecipient.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataRecipient.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.source.type | extensible (lien extensible) | AuditEventSourceType |
| AuditEvent.entity.type | extensible (lien extensible) | AuditEventEntityType |
| AuditEvent.entity.role | extensible (lien extensible) | AuditEventEntityRole |
| AuditEvent.entity.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |

| | | |
|---|---|---|
| AuditEvent.entity.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:patient.type | extensible (lien extensible) | Patron : 1 *Person* (Personne) |
| AuditEvent.entity:patient.role | extensible (lien extensible) | Patron : 1 *Patient* |
| AuditEvent.entity:patient.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:patient.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:submissionSet.type | extensible (lien extensible) | Patron : 2 *System Object* (Objet système) |
| AuditEvent.entity:submissionSet.role | extensible (lien extensible) | Patron : 20 *Job* (Travail) |
| AuditEvent.entity:submissionSet.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:submissionSet.security Label | extensible (lien extensible) | All Security Labels |

## 1.13.2 Audit d'une transaction *Rechercher des données* [CA:FeX-2]

Les critères d'audit sont semblables à ceux appliqués à la transaction *MHD Find Document References* [ITI-67].

### Audit du consommateur de données

Lorsqu'il est groupé avec les acteurs « Secure Node » (nœud sécurisé) ou « Secure Application » (application sécurisée) du profil ATNA, l'acteur « Consommateur de données » pourra enregistrer un événement d'audit pour la transaction *Rechercher des données* (*Search Data Consumer Audit Event Log*).

*Liens terminologiques*

| **Chemin d'accès** | **Conformité** | **Ensemble de valeurs/codes** |
|---|---|---|
| AuditEvent.language | preferred (lien recommandé) | CommonLanguages<br>**Max Binding**: AllLanguages |
| AuditEvent.type | extensible (lien extensible) | Patron : 110112 *Query* (Interrogation, ou Requête) |
| AuditEvent.subtype | extensible (lien extensible) | Patron : CA:FeX-2 « *Search Data* » (Rechercher des données) |
| AuditEvent.action | required (lien requis) | Patron : E |
| AuditEvent.outcome | required (lien requis) | AuditEventOutcome |

| | | |
|---|---|---|
| AuditEvent.purposeOfEvent | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent.type | extensible (lien extensible) | ParticipationRoleType |
| AuditEvent.agent.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataConsumer.type | extensible (lien extensible) | Patron : 110153 *Source Role ID* (ID du rôle de la source) |
| AuditEvent.agent:dataConsumer.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataConsumer.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataConsumer.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataConsumer.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataResponder.type | extensible (lien extensible) | Patron : 110152 *Destination Role ID* (ID du rôle du destinataire) |
| AuditEvent.agent:dataResponder.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataResponder.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataResponder.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataResponder.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.source.type | extensible (lien extensible) | AuditEventSourceType |
| AuditEvent.entity.type | extensible (lien extensible) | AuditEventEntityType |
| AuditEvent.entity.role | extensible (lien extensible) | AuditEventEntityRole |

| | | |
|---|---|---|
| AuditEvent.entity.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:patient.type | extensible (lien extensible) | Patron : 1 *Person* (Personne) |
| AuditEvent.entity:patient.role | extensible (lien extensible) | Patron : 1 *Patient* |
| AuditEvent.entity:patient.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:patient.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:queryParameters.type | extensible (lien extensible) | Patron : 2 *System Object* (Objet système) |
| AuditEvent.entity:queryParameters.role | extensible (lien extensible) | Patron : 24 *Query* (Interrogation, ou Requête) |
| AuditEvent.entity:queryParameters.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:queryParameters.securityLabel | extensible (lien extensible) | All Security Labels |

## Audit du répondeur de données

Lorsqu'il est groupé avec les acteurs « Secure Node » (nœud sécurisé) ou « Secure Application » (application sécurisée) du profil ATNA, l'acteur « Répondeur de données » pourra enregistrer un événement d'audit pour la transaction *Rechercher des données* (*Search Data Responder Audit Event Log*).

*Liens terminologiques*

| **Chemin d'accès** | **Conformité** | **Ensemble de valeurs/codes** |
|---|---|---|
| AuditEvent.language | preferred (lien recommandé) | CommonLanguages<br>**Max Binding**: AllLanguages |
| AuditEvent.type | extensible (lien extensible) | Patron : 110112<br>*Query* (Interrogation, ou Requête) |
| AuditEvent.subtype | extensible (lien extensible) | Patron : CA:FeX-2 « *Search Data* » (Rechercher des données) |
| AuditEvent.action | required (lien requis) | Patron : E |
| AuditEvent.outcome | required (lien requis) | AuditEventOutcome |

| | | |
|---|---|---|
| AuditEvent.purposeOfEvent | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent.type | extensible (lien extensible) | ParticipationRoleType |
| AuditEvent.agent.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataConsumer.type | extensible (lien extensible) | Patron : 110153 *Source Role ID* (ID du rôle de la source) |
| AuditEvent.agent:dataConsumer.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataConsumer.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataConsumer.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataConsumer.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataResponder.type | extensible (lien extensible) | Patron : 110152 *Destination Role ID* (ID du rôle du destinataire) |
| AuditEvent.agent:dataResponder.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataResponder.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataResponder.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataResponder.purpose<br>OfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.source.type | extensible (lien extensible) | AuditEventSourceType |
| AuditEvent.entity.type | extensible (lien extensible) | AuditEventEntityType |
| AuditEvent.entity.role | extensible (lien extensible) | AuditEventEntityRole |

| | | |
|---|---|---|
| AuditEvent.entity.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:patient.type | extensible (lien extensible) | Patron : 1 *Person* (Personne) |
| AuditEvent.entity:patient.role | extensible (lien extensible) | Patron : 1 *Patient* |
| AuditEvent.entity:patient.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:patient.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:queryParameters.type | extensible (lien extensible) | Patron : 2 *System Object* (Objet système) |
| AuditEvent.entity:queryParameters.role | extensible (lien extensible) | Patron : 24 *Query* (Interrogation, ou Requête) |
| AuditEvent.entity:queryParameters.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:queryParameters.securityLabel | extensible (lien extensible) | All Security Labels |

### 1.13.3 Audit d'une transaction *Extraire des données* [CA:FeX-3]

Les critères d'audit sont semblables à ceux appliqués à la transaction *MHD Retrieve Document* [ITI-68].

#### Audit du consommateur de données

Lorsqu'il est groupé avec les acteurs « Secure Node » (nœud sécurisé) ou « Secure Application » (application sécurisée) du profil ATNA, l'acteur « Consommateur de données » pourra enregistrer un événement d'audit pour la transaction *Extraire des données* (*Retrieve Data Consumer Audit Event Log*).

*Liens terminologiques*

| **Chemin d'accès** | **Conformité** | **Ensemble de valeurs/codes** |
|---|---|---|
| AuditEvent.language | preferred (lien recommandé) | CommonLanguages<br>**Max Binding**: AllLanguages |
| AuditEvent.type | extensible (lien extensible) | Patron : 110107 *Import* (Importer) |
| AuditEvent.subtype | extensible (lien extensible) | Patron : CA:FeX-3 *Retrieve Data* (Extraire des données) |
| AuditEvent.action | required (lien requis) | Patron : C |
| AuditEvent.outcome | required (lien requis) | AuditEventOutcome |

| | | |
|---|---|---|
| AuditEvent.purposeOfEvent | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent.type | extensible (lien extensible) | ParticipationRoleType |
| AuditEvent.agent.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataConsumer.type | extensible (lien extensible) | Patron : 110153 *Source Role ID* (ID du rôle de la source) |
| AuditEvent.agent:dataConsumer.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataConsumer.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataConsumer.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataConsumer.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataResponder.type | extensible (lien extensible) | Patron : 110152 *Destination Role ID* (ID du rôle du destinataire) |
| AuditEvent.agent:dataResponder.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataResponder.medi | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataResponder.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataResponder.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.source.type | extensible (lien extensible) | AuditEventSourceType |
| AuditEvent.entity.type | extensible (lien extensible) | AuditEventEntityType |

| | | |
|---|---|---|
| AuditEvent.entity.role | extensible (lien extensible) | AuditEventEntityRole |
| AuditEvent.entity.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:patient.type | extensible (lien extensible) | Patron : 1 *Person* (Personne) |
| AuditEvent.entity:patient.role | extensible (lien extensible) | Patron : 1 *Patient* |
| AuditEvent.entity:patient.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:patient.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:documentUniqueId.what.type | extensible (lien extensible) | ResourceType |
| AuditEvent.entity:documentUniqueId.type | extensible (lien extensible) | Patron : 2 *System Object* (Objet système) |
| AuditEvent.entity:documentUniqueId.role | extensible (lien extensible) | Patron : 3 *Report* (Rapport) |
| AuditEvent.entity:documentUniqueId.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:documentUniqueId.securityLabel | extensible (lien extensible) | All Security Labels |

## Audit du répondeur de données

Lorsqu'il est groupé avec les acteurs « Secure Node » (nœud sécurisé) ou « Secure Application » (application sécurisée) du profil ATNA, l'acteur « Répondeur de données » pourra enregistrer un événement d'audit pour la transaction *Rechercher des données* (*Search Data Responder Audit Event Log*).

*Liens terminologiques*

| **Chemin d'accès** | **Conformité (type de lien)** | **Ensemble de valeurs/codes** |
|---|---|---|
| AuditEvent.language | preferred (lien recommandé) | CommonLanguages<br>**Max Binding**: AllLanguages |
| AuditEvent.type | extensible (lien extensible) | Patron : 110106 *Export* (Exporter) |
| AuditEvent.subtype | extensible (lien extensible) | Patron : CA:FeX-3 *Retrieve Data* (Extraire des données) |

| | | |
|---|---|---|
| AuditEvent.action | required (lien requis) | Patron : R |
| AuditEvent.outcome | required (lien requis) | AuditEventOutcome |
| AuditEvent.purposeOfEvent | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent.type | extensible (lien extensible) | ParticipationRoleType |
| AuditEvent.agent.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataConsumer.type | extensible (lien extensible) | Patron : 110153 *Source Role ID* (ID du rôle de la source) |
| AuditEvent.agent:dataConsumer.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataConsumer.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataConsumer.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataConsumer.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.agent:dataResponder.type | extensible (lien extensible) | Patron : 110152 *Destination Role ID* (ID du rôle du destinataire) |
| AuditEvent.agent:dataResponder.role | example (lien à titre d'exemple seulement) | SecurityRoleType |
| AuditEvent.agent:dataResponder.media | extensible (lien extensible) | MediaTypeCode |
| AuditEvent.agent:dataResponder.network.type | required (lien requis) | AuditEventAgentNetworkType |
| AuditEvent.agent:dataResponder.purposeOfUse | extensible (lien extensible) | PurposeOfUse |
| AuditEvent.source.type | extensible (lien extensible) | AuditEventSourceType |

| | | |
|---|---|---|
| AuditEvent.entity.type | extensible (lien extensible) | AuditEventEntityType |
| AuditEvent.entity.role | extensible (lien extensible) | AuditEventEntityRole |
| AuditEvent.entity.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:patient.type | extensible (lien extensible) | Patron : 1 *Person* (Personne) |
| AuditEvent.entity:patient.role | extensible (lien extensible) | Patron : 1 *Patient* |
| AuditEvent.entity:patient.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:patient.securityLabel | extensible (lien extensible) | All Security Labels |
| AuditEvent.entity:documentUniqueId.what.type | extensible (lien extensible) | ResourceType |
| AuditEvent.entity:documentUniqueId.type | extensible (lien extensible) | Patron : 2 *System Object* (Objet système) |
| AuditEvent.entity:documentUniqueId.role | extensible (lien extensible) | Patron : 3 *Report* (Rapport) |
| AuditEvent.entity:documentUniqueId.lifecycle | extensible (lien extensible) | ObjectLifecycleEvents |
| AuditEvent.entity:documentUniqueId.securityLabel | extensible (lien extensible) | All Security Labels |

# 2 Cas d'utilisation et définitions

La présente section décrit les cas d'utilisation et les scénarios de flux de tâches qui s'appliquent à l'échange de documents cliniques entre différentes solutions. Comme l'implantation des éléments des cas d'utilisation pourrait varier d'une province et d'un territoire à un 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 ou un patient utilisateur de solution clinique (DME, portail-patient ou autre) et un système dans le contexte de l'EIS, autrement dit, les flux ou la « conversation » entre un système et ses utilisateurs (participants). À noter qu'un « participant » peut être une personne ou un système. Les interactions sont définies en détail dans les diagrammes de séquence.

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.

## 2.1 Index des cas d'utilisation

Le tableau suivant mentionne les cas d'utilisation (identifiant, nom et description) qui ont été jugés prioritaires au terme de l'analyse de l'environnement pancanadien. D'autres cas seront définis dans des versions subséquentes de la spécification.

**La présente version de la spécification CA:FeX couvre les cas d'utilisation UC-01 et UC-02.**

| ID du cas d'utilisation | Nom du cas d'utilisation | Description du cas d'utilisation |
|---|---|---|
| UC-01 | Créer et soumettre un document | Un PS, dans n'importe quel milieu de soins, ajoute de l'information clinique au dossier du patient afin qu'elle soit utilisée au point d'intervention par d'autres PS autorisés. |
| UC-02 | Rechercher et extraire un document | Un PS, dans n'importe quel milieu de soins, recherche et extrait de la documentation clinique afin de l'utiliser au point d'intervention, ou un patient recherche et extrait de la documentation clinique pour avoir une copie de ses RPS. |

## 2.2 Niveaux d'obligation associés aux éléments

| Priorité | Définition |
|---|---|
| DOIT | Désigne un élément **obligatoire** ou **requis**. |
| DEVRAIT | Désigne un élément **recommandé**, dont l'implantation est considérée comme une bonne pratique, mais sans être obligatoire (facultatif). |

## 2.3 UC-01 Créer et soumettre un document

**Description**

Un professionnel de la santé (PS), dans n'importe quel milieu de soins, ajoute de l'information clinique au dossier du patient afin qu'elle soit utilisée au point d'intervention par d'autres PS autorisés.

**Scénario**

Un patient consulte 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 soumettre cette nouvelle information au réseau (dépôt de données cliniques) afin de la rendre accessible aux autres PS susceptibles de prodiguer des soins au patient.

**Déclencheurs, préconditions, postconditions**

Les points suivants donnent des exemples de déclencheurs, de préconditions et de postconditions liés au téléversement d'information clinique dans un dépôt de données cliniques. 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 ajoute de l'information clinique à son dossier.
- Le PS reçoit d'autres renseignements concernant un patient qu'il souhaite partager avec d'autres PS. Par exemple, il reçoit les résultats d'analyses d'un patient ou met à jour la liste des problèmes de santé d'un patient.

**Préconditions**

- La documentation clinique porte un ID unique associé au patient (p. ex. ID du registre des clients) pour être téléversée au dépôt de données cliniques et extraite par d'autres PS.
- Dans les provinces et territoires où il faut obtenir le consentement explicite du patient pour partager son information clinique :
    - Le patient donne ou a déjà donné son consentement au versement de son information clinique dans le dépôt de données cliniques.

**Postconditions**

- La nouvelle information clinique est enregistrée dans le dépôt de données cliniques.
- Les PS autorisés peuvent visualiser ces nouveaux renseignements médicaux ou recevoir une notification selon laquelle de nouveaux renseignements ont été ajoutés au dossier du patient.

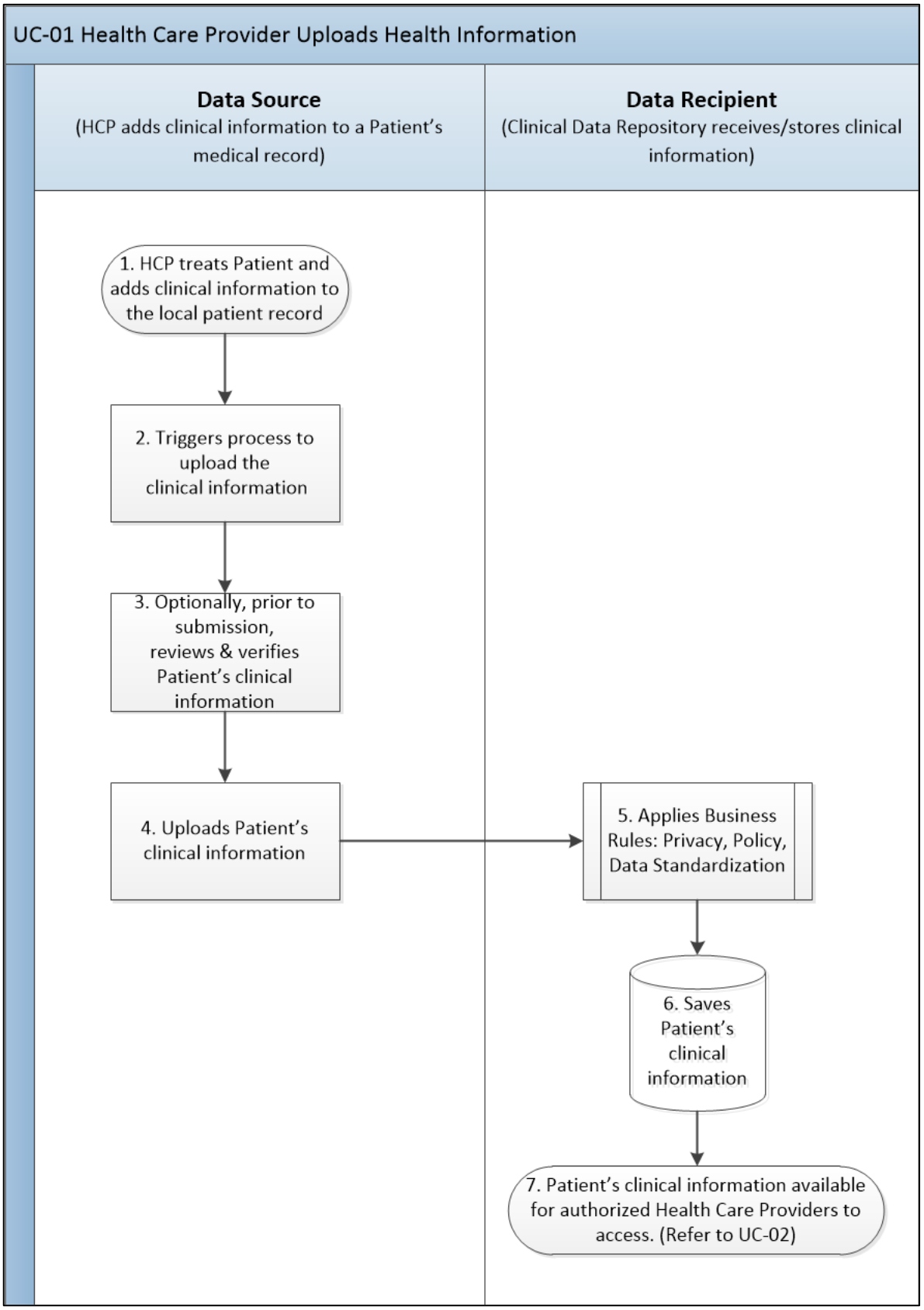
**Cas d'utilisation – participants et diagramme**

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

- Source de données (PS qui ajoute de l'information clinique au dossier du patient via sa solution clinique, p. ex. un DME)
- Destinataire de données (dépôt de données cliniques qui reçoit/stocke l'information clinique du patient)

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-01 : Un PS ajoute de l'information clinique au dossier du patient**



**Cas d'utilisation – flux primaire**

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

1. Le PS traite le patient et ajoute de l'information clinique au dossier médical du patient dans sa solution clinique locale (p. ex. DME, SIS).
2. Le PS décide de partager les nouveaux renseignements médicaux qu'il a recueillis. Il déclenche le téléversement de cette information dans le dépôt de données cliniques.
3. Optionnellement, le PS vérifie l'information avant de la partager/téléverser dans le dépôt de données cliniques.
4. Le PS envoie/téléverse l'information clinique au dépôt de données cliniques.
5. Le dépôt de données cliniques applique les règles opérationnelles (p. ex. normalisation des données, confidentialité, politiques, etc.).
   Par exemple :
   a. Il valide les données (p. ex. le PS est identifié et peut soumettre de l'information clinique, le patient est identifié, etc.).
      i. Il vérifie s'il existe déjà des renseignements médicaux associés au même patient/déjà soumis par le même PS – application des règles de remplacement/d'archivage.
6. Le dépôt de données cliniques enregistre l'information clinique.
   a. Il répond au système émetteur (celui qui a soumis l'information) pour lui indiquer si la soumission a été acceptée (information clinique enregistrée) ou non (requête erronée).
7. Le nouvelle information clinique est accessible aux PS autorisés (voir le cas d'utilisation UC-02 : PS qui recherche/extrait un document).

**Cas d'utilisation – autre flux**

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

- Étape 3 : Le PS peut sauter l'étape de la vérification de l'information clinique, ce qui permet à la solution clinique de partager/téléverser automatiquement l'information dans le dépôt de données cliniques.
- Étape 3 : Après avoir vérifié l'information clinique, le PS décide de modifier les renseignements médicaux au dossier local du patient avant de téléverser l'information clinique au dépôt de données cliniques.
- Étape 4 : Après avoir soumis l'information clinique, le PS se rend compte qu'il y a des renseignements médicaux erronés ou manquants. Il pourra corriger l'information et la téléverser à nouveau dans le dépôt de données cliniques.
- Étape 4 : Après avoir soumis l'information clinique, le PS se rend compte qu'elle concerne un autre patient. Le PS pourra retirer/supprimer l'information clinique qu'il avait soumise dans le dépôt de données cliniques.

**Cas d'utilisation – exigences**

Les exigences rattachées au cas d'utilisation UC-01 sont les suivantes.

| Nº | Catégorie | Description des exigences |
|---|---|---|
| 1 | Écriture | L'API FHIR DOIT être capable d'accepter des opérations d'écriture pour permettre la création de nouveaux documents cliniques dans le dépôt central de données cliniques. |
| 2 | Réponse | L'API FHIR DOIT être capable d'envoyer une réponse selon laquelle l'information clinique a été enregistrée dans le dépôt central de données cliniques. |

| | | |
|---|---|---|
| 3 | Réponse | L'API FHIR DOIT être capable d'envoyer une réponse selon laquelle l'information clinique n'a pas été enregistrée dans le dépôt central de données cliniques (HTTP 400 *Bad Request* – requête erronée) |

## 2.4 UC-02 Rechercher et extraire un document

**Description**

Un professionnel de la santé (PS), dans n'importe quel milieu de soins, recherche et extrait de la documentation clinique afin de l'utiliser au point d'intervention, ou un patient recherche et extrait de la documentation clinique pour avoir une copie de ses RPS.

**Scénario**

Les scénarios suivants ne sont que des exemples. D'autres scénarios pourraient être implantés dans les provinces et territoires.

**1) Un PS, dans n'importe quel milieu de soins, recherche et extrait de la documentation clinique afin de l'utiliser au point d'intervention.**

Un patient consulte 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 professionnel de la santé recueille les renseignements du patient et lance une recherche dans sa solution clinique (p. ex. DME) pour voir s'il n'existerait pas déjà de l'information clinique au sujet du patient (il lance une recherche dans son réseau pour trouver de la documentation clinique qui a été créée et partagée par un autre PS). Après avoir trouvé des documents cliniques associés au patient, le PS consulte et utilise l'information qu'ils renferment pour traiter le patient.

**2) Un patient (ou un sujet de soins) accède à ses RPS pour les visualiser ou en obtenir une copie.**

Un patient aimerait accéder à ses RPS, ou voudrait que son proche aidant y accède, pour se tenir au courant et participer activement à ses soins.

**Déclencheurs, préconditions, postconditions**

Les points suivants donnent des exemples de déclencheurs, de préconditions et de postconditions liés à la recherche et à l'extraction de documents cliniques dans un dépôt de données cliniques. Ils ne couvrent pas tous les scénarios de flux de tâches qui pourraient être implantés dans les provinces et territoires.

**Déclencheurs**

Scénario 1 :

- Le patient consulte un PS.
- 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).

Scénario 2 :

- Le patient, ou son proche aidant désigné, visualise ses RPS pour se tenir au courant.
- Le patient aimerait obtenir une copie de ses RPS pour les avoir en voyage.

- Le patient aimerait obtenir une copie de ses RPS pour les transmettre à un autre PS.

**Préconditions**

Scénario 1 :

- Le PS est connecté à sa solution clinique (p. ex. DME).
- La solution clinique du PS est connectée/reliée au dépôt de données cliniques.

Scénario 2 :

- Dans les provinces et territoires où le patient a appliqué une directive de consentement à son information clinique, le PS se conforme aux politiques de confidentialité en vigueur.
- Le patient peut accéder à son dossier médical via un portail-patient provincial/territorial.
- Ou, le patient a autorisé un proche aidant à accéder à son dossier médical.

**Postconditions**

Scénario 1 :

- Le PS visualise et utilise les documents cliniques dans le cadre de la prestation de soins au patient.

Scénario 2 :

- Le patient, ou son proche aidant désigné, visualise ses RPS et, optionnellement, en obtient une copie.
- Le patient, ou son proche aidant désigné, transmet ses RPS à un autre PS pour assurer la continuité des soins.

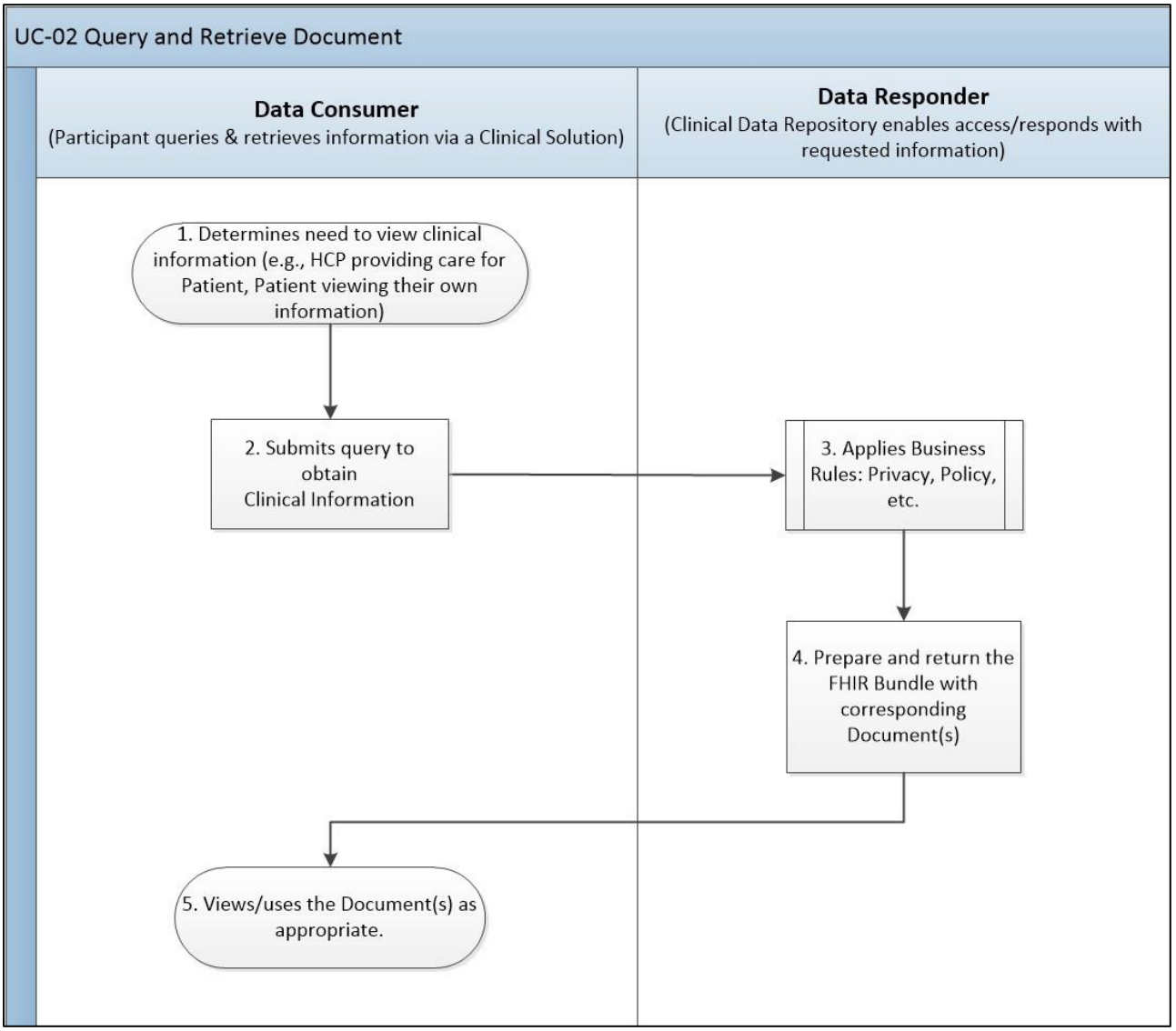
**Cas d'utilisation – participants et diagramme**

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

- Consommateur de données (solution clinique, p. ex. DME qu'utilise le PS pour rechercher et extraire des documents cliniques dans un dépôt de données cliniques; portail-patient utilisé par le patient/sujet de soins pour rechercher et extraire des documents cliniques dans un dépôt de données cliniques)
- Répondeur de données (système de dossiers médicaux agissant comme un dépôt de données cliniques qui reçoit la requête et qui répond par l'envoi les documents cliniques demandés)

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 : Un PS, ou un patient, recherche et extrait de la documentation clinique




**Cas d'utilisation – flux primaire**

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

1. Le participant (PS ou patient/sujet de soins) a besoin de visualiser de l'information clinique.
2. Le participant lance une requête d'accès (recherche/interrogation) à l'information clinique depuis sa solution clinique.
3. Le dépôt de données cliniques applique les règles opérationnelles/politiques en vigueur (validation de l'identité du demandeur).
4. Le dépôt de données cliniques prépare et envoie la ressource FHIR *Bundle* contenant les documents cliniques correspondant à la requête.
5. Le participant visualise/utilise les documents cliniques dans le cadre de la prestation de soins au patient ou pour prendre connaissance des RPS.

**Cas d'utilisation – autre flux**

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

- Étape 3 : La spécification CA:FeX ne prend pas en charge les services de gestion du consentement du patient pour le moment, mais cet aspect figure dans la feuille de route et ferait l’objet d’un cas d’utilisation distinct dans lequel le patient aurait appliqué une directive de consentement dont le PS devrait prendre en considération avant d’accéder à l’information clinique du patient. Il se peut que des provinces/territoires aient déjà mis en place des services de gestion du consentement du patient et il faudra en tenir compte au moment de l'implantation dans les administrations concernées.

**Cas d’utilisation – exigences**

Voici les exigences qui seront prises en compte dans ce cas d’utilisation.

| Nº | Catégorie | Description des exigences |
|---|---|---|
| 1 | Requête | L’API FHIR DOIT être capable d’exécuter des requêtes à partir de l’identifiant du patient. |
| 2 | Requête | L’API FHIR DOIT être capable d’exécuter des requêtes portant sur une période donnée. |
| 3 | Requête | L’API FHIR DEVRAIT être capable d’exécuter des requêtes portant sur le type de document (*Document Type*) que veut extraire le PS. |
| 4 | Requête | L’API FHIR DEVRAIT être capable d’accepter des requêtes provenant d’un portail-patients ou de tout autre système permettant au patient de lancer une requête pour accéder à ses RPS. |
| 5 | Réponse | L’API FHIR DOIT être capable de répondre à des requêtes d’extraction de l’information clinique lancées par un patient voulant accéder à ses RPS. |

# 3 Échanger des documents FHIR

Les transactions ci-dessous représentent une solution initiale aux cas d'utilisation et sont appelées à évoluer, notamment en fonction des commentaires de la communauté des utilisateurs et à mesure que les cas d'utilisation seront peaufinés et que d'autres seront ajoutés. Nous encourageons la communauté à fournir des commentaires sur cette nouvelle spécification.

## 3.1 Survol

HL7 caractérise un document par les propriétés suivantes :

- Persistance (*Persistence*) – Un document est persistant au fil du temps, c'est-à-dire que son contenu ne change pas d'un moment à un autre. L'information qu'il contient a été enregistrée à un moment précis dans le temps.
- Entièreté (*Wholeness*) – Un document est une unité complète d'information. Des parties du document pourraient être créées ou modifiées séparément, ou être authentifiées ou certifiées authentiques, mais le document serait encore considéré comme un tout et traité dans son entièreté.
- Intendance (*Stewardship*) – Un document est gardé tout au long de sa vie par un intendant ou un gardien, c'est-à-dire une organisation ou une personne à laquelle on en a confié la garde.
- Contexte (*Context*) – Un document clinique établit par défaut le contexte de son contenu.
- Possibilité d'authentification (*Potential for authentication*) – Un document clinique est un assemblage d'information dont l'authenticité peut être certifiée.

La présente spécification définit un document comme un dossier (manuscrit, imprimé ou électronique) qui regroupe l'information sur l'état de santé ou les soins fournis à un patient et qui existe dans un but ou pour un flux de tâches particulier. Ce document est à distinguer des données médicales qu'il pourrait contenir, car il ajoute des éléments de contexte et des métadonnées qui indiquent la manière dont les données médicales ont été consignées et les raisons pour lesquelles elles l'ont été.

À titre d'exemple, un document peut être un sommaire au congé, des notes sur les antécédents et l'état de santé actuel du patient, un rapport d'imagerie médicale ou un résumé du dossier du patient.

### Champ d'application

La spécification d'interopérabilité CA:FeX s'applique pour l'instant à l'échange de documents FHIR (et leurs ressources respectives). Par la suite, on étendra sa portée afin qu'elle couvre l'échange de ressources FHIR individuellement et indépendamment du flux associé à un document (p. ex. extraction de l'information sur les médicaments délivrés dans les trois dernières années).

Même si la norme FHIR d'HL7 définit la structure d'un document créé et assemblé au format FHIR (voir la page Web *FHIR Composition Resource*), il importe de signaler qu'elle peut aussi servir à l'échange de documents structurés selon d'autres formats, p. ex. le format binaire de FHIR (*Binary Resources*).

La spécification a été développée pour permettre un premier cycle d'implantation où des utilisateurs mettront à l'essai ses transactions pour échanger le RDP-CA sous la forme d'un document FHIR. En optant pour le RDP-CA comme terrain d'essai, on s'assure que la spécification est en mesure de répondre à des exigences qui pourront être extrapolées à d'autres types de documents FHIR.

**Note :** Les versions antérieures de la présente spécification incluaient d'autres transactions (CA:FeX 2B, CA:FeX 3B) censées couvrir les interactions avec des dépôts hybrides (p. ex. dépôts qui prennent en charge à la fois les documents FHIR natifs et les anciens documents binaires). Toutefois, ces transactions seront abordées dans une version future de la spécification CA:FeX, car elles nécessitent des cycles supplémentaires de rétroaction et de test par les utilisateurs avant d'être mises à l'essai.

La version actuelle de la spécification d’interopérabilité CA:FeX fournit l’information relative aux transactions suivantes :

| ID de transaction | Description |
|---|---|
| CA:FeX-1 | Soumettre des données |
| CA:FeX-2 | CA:FeX-2A : Rechercher un document dans un dépôt de documents FHIR assemblés |
| CA:FeX-3 | CA:FeX-3A : Extraire un document d’un dépôt de documents FHIR assemblés |

## 3.2 Version FHIR

Le contenu FHIR de la présente spécification est fondé sur la version 4 de FHIR (v4.0.1). Voir la page Web *FHIR Release 4*.

## 3.3 Soumettre un document

### Champ d’application

Cette capacité est actuellement limitée à la possibilité de soumettre de nouveaux documents FHIR.

Bien qu'il existe de nombreuses façons de modéliser et d'échanger des documents FHIR, la présente version de la spécification s’en tient aux patrons d’échange qui seront utilisés, dans le premier cycle d'implantation, par des utilisateurs qui s'attendent à ce que le RDP-CA soit transmis sous la forme d’un document FHIR. Le résumé du dossier du patient est un type de document relativement nouveau, qui n’a jamais vraiment été implanté et qui a été modélisé comme un document FHIR.

Un document FHIR est une ressource *Bundle* de type *Document* qui contient une ressource *Composition* en première entrée et, dans des entrées additionnelles, des renvois vers des ressources clés. Voir la page Web *Documents*.

### 3.3.1 Non inclus

La spécification CA:FeX est évidemment appelée à évoluer. Elle couvrira au fil du temps de nouveaux types de documents et d’architectures, de sorte que ses versions subséquentes fourniront des indications sur les cas d’utilisation s’y rapportant.

Les pratiques de gestion du cycle de vie des résumés du dossier du patient à l'échelle mondiale, pancanadienne et provinciale/territoriale sont encore en cours d'élaboration. Par conséquent, les indications relatives à la gestion, à la vérification, au remplacement et à la dépréciation des documents ne sont pas incluses dans la présente version, mais elles figureront dans les prochaines.

**Note :** Cela n'empêche pas les premiers utilisateurs de CA:FeX de définir leurs pratiques de gestion des documents et de commencer à les appliquer dans leurs propres spécifications.

> ⓘ **Info**
> Les responsables de l'implantation qui prévoient prendre en charge des cas d'utilisation qui supposent l'utilisation de plusieurs résumés du dossier du patient dans le temps doivent néanmoins se familiariser avec les limites que la norme FHIR quant à l'immuabilité des documents. Une fois assemblé sous la forme d'une ressource *Bundle* de type *Document*, le document est immuable – son contenu ne pourra jamais être modifié – et l'ID du document ne pourra jamais être réutilisé. Notez que le document peut être représenté en XML ou en JSON et être reconverti en ces deux formats ou voir son codage de caractères modifié, tout en restant le même document. Toutefois, le contenu auquel il fait directement référence et la présentation du document ne peuvent pas être modifiés de manière substantielle (au point de changer le sens clinique du contenu). Tout document supplémentaire dérivé de la même composition DOIT avoir un ID de document différent. Voir la page https://www.hl7.org/fhir/documents.html#content.

### 3.3.2 Cas d'utilisation

Le cas d'utilisation CA:FeX qui exploite cette capacité est le suivant :

- UC-01 : Créer et soumettre un document

### 3.3.3 Transaction CA:FeX

Cette capacité décrit l'implantation de la transaction *Soumettre des données* (CA:FeX-1) de la spécification CA:FeX illustrée dans le diagramme de séquence d'UC-01 : Créer et soumettre un document.

### 3.3.4 Opérations HTTP

Cette capacité est exploitable au moyen de requêtes HTTP POST. Les responsables de l'implantation sont censés se familiariser avec la manière d'exécuter des interactions « create » (*créer*) à l'aide du cadre d'API FHIR RESTful.

Voir la sous-section *Acteurs et transactions CA:FeX* pour plus d'information sur les opérations HTTP prises en charge.

**HTTP POST**

Une interaction « create » (*créer*) est exécutée au moyen d'une opération POST dans un cadre RESTful :

POST [base]/[type]{?_format=[mime-type]}

**Types de contenu et codage**

Les types de contenu « application/fhir+json » ou « application/fhir+xml » sont permis.

### 3.3.5 Patrons de soumission de documents

Le patron optimal de soumission de documents pour une implantation est déterminé par un certain nombre de facteurs, notamment ceux-ci : présence/absence d'une architecture XDS ou XCA; objectifs organisationnels à court et à long terme en ce qui a trait à FHIR; actifs actuels et hiérarchie des capacités; rôle dans l'écosystème d'échange d'information sur la santé; degré de préparation des acteurs à adopter FHIR, etc. Ces facteurs sont abordés plus en détail dans le livre blanc sur la spécification CA:FeX. Les patrons décrits ci-dessous s'appliquent uniquement aux destinataires de données qui s'attendent à ce que les sources de données soumettent des documents à partir de points d'extrémité FHIR.

Certains responsables de l'implantation peuvent choisir d'utiliser les données reçues via les flux de tâches existants et de les convertir en FHIR, surtout si leurs systèmes de dossiers médicaux électroniques ne sont pas prêts à échanger des données au format FHIR. D'autres types d'implantation peuvent reposer sur la création d'un document FHIR « à la demande » en réponse à une requête. Les deux méthodes sont des pratiques parfaitement légitimes qui ne nécessitent pas de point d'extrémité pour la soumission. *Ces patrons*

*de création constitueront une capacité distincte dans une version ultérieure.*

### Soumission directe d'une ressource *Bundle* de type *Document* (document FHIR)

Un destinataire de données qui veut recevoir un document FHIR d'une source de données doit au moins prendre en charge la soumission d'un document FHIR dans le cadre d'une requête HTTP POST ciblant un point d'extrémité « [base]/Bundle ».

Cela permettra de créer (interaction « create ») la nouvelle ressource *Bundle* dans un emplacement attribué par le serveur; le serveur attribuera également un ID à cette ressource. (*Note : ce patron ne prend pas en charge l'interaction « conditional create », qui permet de créer la ressource seulement si elle n'existe pas dans le serveur.)*

Conformément à ce que prévoit la norme FHIR pour l'interaction HTTP « create » :

- Le corps de la requête DOIT être une ressource FHIR valide (dans ce cas-ci, une ressource *Bundle* conforme à la version 4 de FHIR).
- La ressource n'a pas besoin d'avoir un élément « id » (c'est l'un des rares cas où une ressource existe sans élément « id »). Si un ID est attribué, le serveur NE DOIT PAS en tenir compte.
- Si le corps de la requête inclut un élément « meta », le serveur NE DOIT PAS tenir compte des valeurs existantes pour « versionId » et « lastUpdated ». Le serveur DOIT fournir les bonnes nouvelles valeurs pour « id », « meta.versionId » et « meta.lastUpdated ».
- Le serveur est autorisé à examiner et à modifier les autres valeurs de métadonnées, mais DEVRAIT s'abstenir de le faire; voir la note *Resource Metadata* (métadonnées de ressources) pour la description des métadonnées.
- Un serveur DEVRAIT, sinon, accepter la ressource telle qu'elle a été soumise lorsqu'il en accepte la création, et renvoyer le même contenu lorsqu'elle est lue par la suite. Cependant, certains systèmes peuvent ne pas être en mesure de le faire; voir la note Transactional Integrity (intégrité transactionnelle) pour guider la discussion sur l'intégrité transactionnelle.
- Le serveur répond par le code HTTP 201 Created (créé) et DOIT aussi envoyer un entête « Location » qui contient le nouvel ID logique (logical Id) et le nouvel ID de version (version Id) de la ressource créée; référez-vous à la section *Gestion des réponses* du présent document pour plus d'explications.

### Soumission d'un document à un point d'extrémité /Bundle

Voici deux attributs clés d'un document FHIR soumis à un point d'extrémité /Bundle (sauf quelques exceptions) :

- Autonome (*Self-Contained*) – Toutes les ressources primaires utilisées dans le document doivent être incluses dans le document (voir la description de *Composition* d'un document FHIR); les autres ressources utilisées dans le document doivent également être incluses.
- Moment précis (*Point-in-time*) – Le document entier est stocké en ayant /Bundle en point d'extrémité, et le contenu n'est (généralement) pas mis à jour. Si le receveur de données, qui prend en charge le point d'extrémité /Patient hors de cette transaction, met à jour une adresse dans une ressource *Patient* sous /Patient, une ressource *Patient* dans un document ne serait pas censée refléter une telle mise à jour.

À elle seule, la soumission d'un document FHIR à un point d'extrémité /Bundle n'est pas une condition suffisante pour que ce patron soit utilisé de manière efficace pour la gestion du cycle de vie des documents. Ce patron est considéré comme une « composante fondamentale » pouvant être augmentée par a) des interactions et des opérations API, ou b) l'introduction d'une logique opérationnelle interne efficace pour déterminer l'actualité des documents.

**Note :** Bien qu'un document FHIR puisse contenir des ressources *Composition*, *Patient*, *Practitioner* ou autres, la soumission d'un document FHIR à un point d'extrémité /Bundle ne rendra pas ces ressources automatiquement accessibles à leur point d'extrémité équivalent (/Composition, /Patient, /Practitioner, etc.).

En dehors de la portée de la présente spécification, un responsable de l'implantation pourrait choisir de décomposer le document FHIR reçu et de gérer individuellement les ressources qu'il contient. Le cas échéant, il devrait tenir compte des points suivants :

- La déduplication des ressources (p. ex. lorsque la ressource *Patient* ou *Composition* d'un document est en fait la même qu'une ressource *Patient* ou *Composition* déjà connue, peut-être obtenue à partir d'un autre document).
- La fiabilité des sources des diverses ressources et l'actualité du document (p. ex. mettre à jour ou non l'adresse du patient à partir d'un document créé il y a 10 ans).
- Si et comment les mises à jour apportées aux ressources extraites sont reproduites dans le document soumis.
- Le cycle de vie du document comparé au cycle de vie des ressources (p. ex. si une ressource *Practitioner* est retirée du système cinq ans après le départ à la retraite du praticien, est-ce que le document FHIR, ou la ressource *Composition* qui en a été extraite, est toujours utilisable?).
- La persistance ou non du document soumis et des ressources extraites.

### 3.3.6 Patrons de soumission de documents : capacités de pointe pour augmenter les capacités de base

Pour l'instant, nous n'avons fait qu'un survol des capacités de pointe (p. ex. opération $document), car le but est d'obtenir l'avis des intervenants sur les patrons que nous envisageons d'inclure et de tester. Nous traiterons donc de ces capacités dans une version ultérieure de la spécification CA:FeX pour nous assurer que son contenu couvre entièrement les patrons et les capacités selon un niveau de maturité qui convient à la mise à l'essai de la spécification.

## 3.4 Rechercher un document

### 3.4.1 Champ d'application

Cette capacité prend en charge la recherche de documents à l'aide d'une interrogation paramétrée.

Plus particulièrement, elle prend en charge :

- les recherches permettant d'obtenir des données utiles, à savoir des documents FHIR qui correspondent aux paramètres fournis. Ce type d'interrogation combine la recherche et l'extraction, mais il sollicite davantage le système demandeur, qui doit gérer et filtrer un grand volume de contenu pour fournir à l'utilisateur une réponse utilisable.

**Note** : Les capacités que le répondeur prend en charge sont mentionnées dans l'énoncé des capacités (*CapabilityStatement*) que le demandeur peut extraire dans le cadre d'une requête distincte de cette recherche. La requête d'un énoncé des capacités est une condition préalable à l'interrogation d'une source. Toutefois, il n'est pas nécessaire de l'effectuer à chaque connexion, pour éviter d'imposer des coûts de performance aux clients qui interagissent avec des serveurs connus qui ne mettent pas fréquemment à jour leurs services de sécurité et/ou leurs capacités prises en charge.

### 3.4.2 Cas d'utilisation

Le cas d'utilisation CA:FeX qui exploite cette capacité est le suivant :

- UC-02 : Rechercher et extraire un document

### 3.4.3 Transaction CA:FeX

Cette capacité décrit l'implantation de la transaction *Rechercher des données* (CA:FeX-2) de la spécification

CA:FeX illustrée dans le diagramme de séquence d'UC-02 : Rechercher et extraire un document.

### 3.4.4 Opérations HTTP

Cette capacité est exploitable au moyen de requêtes HTTP GET et/ou HTTP POST. Les responsables de l'implantation sont censés se familiariser avec la manière d'exécuter des interactions « search » (*rechercher*) à l'aide du cadre d'API FHIR RESTful.

Voir la sous-section *Acteurs et transactions CA:FeX* pour plus d'information sur les opérations HTTP prises en charge.

**HTTP GET**

Dans le cas le plus simple, la recherche est exécutée au moyen d'une opération GET dans un cadre RESTful :

GET [base]/[resourcetype]?name=value&...

**HTTP POST**

Pour une opération POST dans un cadre RESTful (lire la définition d'une API RESTful), les paramètres sont une série de paires de « name=[value] » codées dans l'URL ou au format « application/x-www-form-urlencoded » :

POST [base]/[type]/_search{?[parameters]{&_format=[mime-type]}}

### 3.4.5 Patrons de recherche de documents

Bien qu'il soit possible d'avoir une variabilité des patrons de soumission de documents en fonction d'un certain nombre de facteurs (qui seront abordés plus en détail dans un futur livre blanc sur l'échange de documents FHIR), la variabilité des patrons de recherche de documents occasionne plutôt des coûts élevés pour les consommateurs de données.

La présente spécification vise essentiellement à remédier aux lacunes que les utilisateurs de FHIR constatent avec les normes d'échange de documents existantes telles que MHD et XDS (voir à ce sujet la préface du présent document). Parmi les défis auxquels ils sont confrontés, il y a la nécessité de trouver un équilibre entre l'adoption de patrons de recherche efficaces et cohérents et l'ampleur des efforts requis pour fournir des métadonnées/ressources supplémentaires (p. ex. *DocumentReference*) ayant des attributs plus puissants qui permettraient des recherches ciblées.

Sur le marché américain, les systèmes cliniques sont plus susceptibles d'utiliser des patrons de type MHD pour échanger des documents C-CDA à l'aide de FHIR, en grande partie grâce à l'implantation massive du profil XDS. Bon nombre d'organisations qui avaient déjà investi dans une infrastructure XDS ont choisi de prendre en charge une façade FHIR pour la récupération des documents C-CDA et ont utilisé le profil MHD (et les profils IHE connexes) pour ce faire. Naturellement, ces organisations réfléchissent à la manière d'adapter la configuration actuelle de leurs systèmes cliniques afin qu'ils prennent en charge la recherche et l'extraction d'autres types de documents d'une manière similaire.

Les systèmes qui s'adressent à des marchés autres que celui des États-Unis (ou les nouvelles solutions conçues entièrement selon la norme FHIR pour l'échange de documents) peuvent ne pas présenter le même contexte historique, ce qui pourrait les empêcher de générer immédiatement un investissement en ressources supplémentaires qui leur permettraient d'intégrer des modes de recherche plus attrayants. De nouvelles opérations plus légères ont été développées récemment afin d'alléger la prise en charge de ces attributs de recherche plus puissants. Cependant, ces patrons sont en pleine évolution, et leur place sur le marché canadien n'a pas encore été pleinement évaluée.

**Note :** Le patron de recherche d'un document dans un dépôt de documents FHIR assemblés (CA:FeX-2A) a fait l'objet d'un bien plus grand nombre de cycles de rétroaction et de tests au cours de projetathons que ce fut le cas pour le patron qui a été diffusé aux responsables de l'implantation de dépôts hybrides (CA:FeX-2B). Le patron relatif à CA:FeX-2B et les autres capacités avancées qui nécessiteront une rétroaction plus poussée par les responsables de l'implantation seront abordés dans une prochaine version de la spécification CA:FeX.

### 3.4.6 Patron *Rechercher un document dans un dépôt de documents FHIR assemblés* (CA:FeX-2A)

Ce patron représente le moyen le plus simple de rechercher des documents FHIR dans un dépôt qui ne repose pas sur une architecture XDS/MHD et qui n'a pas augmenté ses capacités de recherche.

Les responsables de l'implantation qui font l'essai de ce patron joueront le rôle d'un consommateur de données ou d'un répondeur de données dans une interaction où l'interrogation est structurée (à l'aide des paramètres mentionnés plus bas) et ensuite soumise à un point d'extrémité « [base]/Bundle » par une commande HTTP GET ou POST.

Les résultats de la recherche (interaction « *search* ») seront transmis dans une réponse HTTP sous la forme d'une ressource *Bundle* de type *Searchset* contenant toutes les ressources *Bundle* de type *Document* qui correspondent aux critères de recherche. Même si le point d'extrémité est /Bundle, il est attendu que le système exécutera une recherche en chaîne qui portera sur plusieurs paramètres appliqués à bundle.composition, afin de circonscrire la recherche aux documents FHIR.

Conformément à ce que prévoit la norme FHIR pour l'interaction HTTP « search » :

- En raison de la manière dont certains agents utilisateurs et mandataires traitent les requêtes GET et POST, les serveurs qui prennent en charge l'interaction « search » DOIVENT prendre en charge, outre la méthode de recherche GET, la méthode POST.
- Dans le cadre d'une requête GET, des RPS pourraient figurer dans les paramètres de recherche et donc dans les journaux HTTP. C'est pourquoi les journaux doivent être considérés comme aussi sensibles que les ressources elles-mêmes. Il s'agit d'une exigence générale, indépendamment de l'utilisation d'une requête GET – voir la page sur les exigences de sécurité de FHIR pour d'autres explications.
- Si la requête a fonctionné, le serveur DOIT envoyer le code HTTP 200 (*OK*) et une ressource *Bundle* de type = searchset qui contient les résultats de la recherche sous la forme d'une série de ressources dans un ordre défini (la série peut aussi équivaloir à zéro ressource).
- Si la requête a échoué (parce qu'elle ne peut être exécutée, et non parce qu'il n'y a pas de résultats possibles), le serveur DOIT envoyer un code HTTP 4xx ou 5xx et un message OperationOutcome. Voir la section *Gestion des réponses*.

Nous encourageons les responsables de l'implantation à lire la spécification FHIR de base pour plus d'explications sur l'interaction HTTP « search ».

#### Recherche de documents à l'aide de points d'extrémité /Bundle

Pour ce patron, il est recommandé aux responsables de l'implantation de cibler le point d'extrémité /Bundle pour obtenir tous les documents FHIR qui correspondent à leurs critères de recherche.

- Les responsables de l'implantation qui utilisent ce patron devraient envisager d'utiliser une combinaison de paramètres de recherche afin de réduire la charge de traitement des répondeurs et demandeurs.
- Si la série de résultats est longue, les serveurs devront la répartir sur plusieurs pages. Pour ce faire, ils DOIVENT utiliser la méthode décrite ici.

Ce patron de recherche ne sépare pas l'acte de recherche de l'extraction. Les clients qui souhaitent offrir à leurs utilisateurs une vue d'ensemble (listes, résumés, etc.) des documents correspondants afin de permettre l'extraction sélective des ressources *Bundle* de type *Document* devront utiliser des patrons de recherche différents ou gérer ce mode de recherche dans l'interface utilisateur de leurs solutions.

> ⓘ **Note**
> En raison des limites de l'interrogation des ressources discrètes lorsque le document est chargé sous la forme d'une ressource *Bundle* de type *Document*, les recherches sur les points d'extrémité /Composition ou d'autres ressources contenues (p. ex. ID d'une ressource *Patient*) ne fonctionneront que dans les dépôts qui a) décomposent les ressources *Bundle* soumises ou b) permettent la soumission des contenus du document à leurs points d'extrémité individuels ou par l'intermédiaire d'une ressource *Bundle* de type *Transaction* afin qu'ils puissent être récupérés. Une telle méthode exige toutefois une très grande prudence, et les responsables de l'implantation devraient être bien au fait des obligations liées au traitement des documents avant de recourir à l'une ou l'autre approche. La présente spécification ne fournit aucune indication sur ces mécanismes.

## Paramètres de recherche pris en charge

Les paramètres de recherche suivants sont utilisés de manière générique pour l'extraction de documents au moyen du point d'extrémité /Bundle. *Ils continueront d'évoluer à mesure que de nouvelles exigences et de nouveaux cas d'utilisation seront définis.*

D'autres paramètres de recherche propres aux exigences d'un cas d'utilisation ou d'un guide d'implantation pourront être définis au besoin par les responsables de l'implantation. Voir *Option 2 – Patron d'échange d'information sur la santé de FHIR conforme à CA:FeX* dans la spécification d'interopérabilité du résumé du dossier du patient pancanadien (RDP-CA) pour savoir quels paramètres parmi les suivants sont utilisés pour extraire les résumés de dossiers de patients, avec exemples à l'appui.

| Paramètres de recherche | Appliqué à… | Description |
|---|---|---|
| timestamp (*estampille temporelle*) | bundle.timestamp | Ce paramètre de type date précise le moment où le paquet (*bundle*) FHIR a été créé. Voir la page http://hl7.org/fhir/R4/search.html#date pour plus d'information sur le paramètre de type date. |
| patient.identifier (*identifiant du patient*) | bundle.composition.patient.identifier | Ce paramètre de type jeton précise un identifiant associé au patient auquel le document est assigné. L'utilisation de bundle.composition.patient.identifier suit la méthode de recherche en chaîne FHIR. |
| type | bundle.composition.type | Ce paramètre de type jeton précise le type de document (LOINC, si possible). L'utilisation de bundle.composition.type suit la méthode de recherche en chaîne FHIR. |
| status (*statut*) | bundle.composition.status | Ce paramètre de type jeton précise le statut de la composition. L'utilisation de bundle.composition.status suit la méthode de recherche en chaîne FHIR. |

ⓘ Il est possible d'utiliser d'autres paramètres de recherche qui permettront de classer et d'organiser encore mieux les ressources envoyées en réponse à une requête. Dans la spécification de base, ces autres paramètres sont appelés « paramètres de base » (*standard parameters*) et « paramètres de résultat » (*result parameters*). Pour le moment, la spécification CA:FeX n'exige pas la prise en charge de certains paramètres, car les attentes en matière de conformité avec ces paramètres dépendent de l'implantation ou sont pertinentes sous certaines conditions seulement (p. ex. le paramètre « _count » si on s'attend à ce que le serveur qui reçoit la requête réponde par l'envoi d'un gros volume de documents).

## 3.5 Extraire un document

### Champ d'application

Cette capacité prend en charge l'extraction de documents à partir d'un ID de ressource connu.

### 3.5.1 Cas d'utilisation

Le cas d'utilisation CA:FeX qui exploite cette capacité est le suivant :

- UC-02 : Rechercher et extraire un document

### 3.5.2 Transaction CA:FeX

Cette capacité décrit l'implantation de la transaction *Extraire des données* (CA:FeX-3) de la spécification CA:FeX illustrée dans le diagramme de séquence d'UC-02 : Rechercher et extraire un document.

### 3.5.3 Opérations HTTP

Cette capacité est exploitable au moyen de requêtes HTTP GET. Les responsables de l'implantation sont censés se familiariser avec la manière d'exécuter des interactions « search » (*rechercher*) à l'aide du cadre d'API FHIR RESTful.

Voir la sous-section *Acteurs et transactions CA:FeX* pour plus d'information sur les opérations HTTP prises en charge.

**HTTP GET**

Dans le cas le plus simple, l'extraction est exécutée au moyen d'une opération GET dans un cadre RESTful :

GET [base]/[resourcetype]/id

### 3.5.4 Patron d'extraction de documents

Pour ce type de patron, le demandeur doit connaître l'ID de la ressource qu'il tente d'extraire.

Selon la maturité et le champ d'application du dépôt, les points d'extrémité pris en charge peuvent se limiter à [base]/ Bundle, mais le dépôt pourrait reconnaître d'autres formats de documents qui seraient extraits à partir de différents points d'extrémité.

Les indications fournies ci-dessous portent sur l'extraction de documents FHIR directement à partir d'un dépôt de documents FHIR assemblés.

**Note :** Le patron d'extraction de documents d'un dépôt de documents FHIR assemblés (CA:FeX-3A) a fait l'objet d'un bien plus grand nombre de cycles de rétroaction et de tests au cours de projetathons que ce fut le

cas pour le patron qui a été diffusé aux responsables de l'implantation qui extraient des documents de dépôts hybrides (CA:FeX-3B). Le patron relatif à CA:FeX-3B sera abordé dans une prochaine version de la spécification CA:FeX.

### 3.5.5 Patron *Extraire un document d'un dépôt de documents FHIR assemblés* (CA:FeX-3A)

La façon la plus simple d'extraire un document FHIR est d'exécuter une interaction « read » (*lire*) avec une requête HTTP GET :

[base]/[type]/[resource id] against a [base]/Bundle endpoint.

Conformément à ce que prévoit la norme FHIR pour l'interaction HTTP « read » (*lire*) :

- Le dépôt envoie en réponse une seule occurrence dont le contenu correspond au type de ressource demandé.
- L'URL est accessible par navigateur.
- Les valeurs possibles pour l'ID logique (*logical id*) sont précisées dans le type d'ID (*id type*).
- Les ressources envoyées dans la réponse DOIVENT avoir un élément « id » dont la valeur est [id].

**Extraction de documents à l'aide de points d'extrémité /Bundle**

Pour ce patron, il est recommandé aux responsables de l'implantation de cibler le point d'extrémité /Bundle pour extraire le document FHIR à partir de l'ID de la ressource *Bundle*. Ce patron d'extraction est censé être utilisé par les responsables de l'implantation pour extraire à nouveau une ressource *Bundle* dont l'ID avait déjà été utilisé dans une recherche/extraction antérieure.

### 3.5.6 Paramètre d'extraction pris en charge

Voici un exemple de requête utilisée pour l'extraction de documents à partir d'un ID de ressource connu :

GET [base]/Bundle/[id]

## 3.6 Gestion des réponses

### 3.6.1 Codes HTTP

Les codes HTTP envoyés en réponse indiquent aux applications si une requête a fonctionné et, dans le cas contraire, la raison pour laquelle elle a échoué.

Ils sont considérés comme des codes de base qui devraient être présents dans toute API d'implantation. La documentation relative au projet d'implantation, entre autres le guide d'implantation, pourra mentionner les autres codes pris en charge par le service et fournir des précisions sur les contextes d'utilisation ou les comportements attendus des clients.

**Codes d'erreur**

Si la requête échoue (parce qu'elle ne peut être exécutée, et non parce qu'il n'y pas de résultats possibles), le système DOIT envoyer un code HTTP 4xx (erreur du client) ou 5xx (erreur de l'API/du service). Un message OperationOutcome décrivant l'erreur DEVRAIT aussi être envoyé.

| Scénario | Code HTTP | Résultat |
|---|---|---|
| La requête est effectuée avec une syntaxe incorrecte, ou elle cible une ressource ou un paramètre de recherche que l'API ne prend pas en charge. | 400 *Bad Request* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |

| | | |
|---|---|---|
| La requête est effectuée par une application n'ayant pas été authentifiée correctement. | 401 *Unauthorized* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |
| La requête est effectuée par un utilisateur authentifié, mais celui-ci n'est pas autorisé à effectuer ce genre d'opération. | 403 *Forbidden* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |
| La requête cible un type de ressource qui n'est pas prise en charge. | 404 *Not Found* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |
| La requête est effectuée à l'aide d'une méthode HTTP qui n'est pas prise en charge par le serveur pour ce type de ressource. | 405 *Method Not Allowed* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |
| La requête inclut un type de média qui n'est pas pris en charge. Par exemple, le client téléverse une image au format /svg+xml, mais le serveur n'accepte pas ce format. | 415 *Unsupported Media Type* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |
| La requête est effectuée, mais le serveur a rencontré une erreur interne durant le traitement du message de réponse. | 500 *Internal Server Error* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |
| La requête est effectuée quand le service est temporairement indisponible. | 503 *Service Unavailable* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |
| La requête est effectuée, mais le serveur qui joue le rôle de passerelle ou mandataire (*proxy*) ne reçoit pas une réponse à temps d'un serveur en amont pour terminer le traitement de la requête. | 504 *Gateway Timeout* | Le code d'erreur est envoyé dans la réponse, avec un message OperationOutcome décrivant l'erreur. |

**Codes de succès**

Si la requête est correctement formatée et qu'elle a fonctionné, l'API DOIT envoyer le code HTTP 200 (*OK*) et une ressource *Bundle* de type = *searchset* qui contient les résultats de la recherche sous la forme d'une série de ressources dans un ordre défini (la série peut aussi équivaloir à zéro ressource).

*NOTE : Les requêtes qui ne sont pas correctement effectuées mais dont les résultats ne contiennent pas de RPS obtiendront quand même en réponse un code HTTP 200 (OK).*

| **Scénario** | **Code HTTP** | **Résultat** |
|---|---|---|
| La requête est effectuée avec la bonne syntaxe, et il y a des ressources FHIR qui correspondent aux paramètres de recherche. | 200 *OK* | Le code de succès est envoyé dans la réponse, et la ressource *Bundle* envoyée dans la réponse contient des entrées correspondant aux ressources FHIR demandées. |

| | | |
|---|---|---|
| La requête a fonctionné, et une ressource FHIR a été créée sur le serveur. | 201 *Created* | Le code de succès est envoyé dans la réponse, et l'emplacement de la ressource est envoyé dans l'entête d'emplacement de la réponse. |

### 3.6.2 OperationOutcome

Les messages OperationOutcome sont utilisés pour fournir une description plus détaillée des problèmes survenus pendant l'exécution d'une opération. Les conventions générales sont les suivantes :

- Un message OperationOutcome peut être l'unique réponse à une opération (généralement accompagnée d'un code d'échec HTTP) ou peut faire partie d'un paquet indiquant des avertissements potentiels associés à la génération de la réponse de recherche.
- Si un message OperationOutcome est envoyé avec tout code autre qu'un code de succès (200), cela signifie que le problème qui est survenu est de type « erreur » ou « fatal ». Un problème qui survient avant que la requête soit exécutée est de type « fatal »; s'il survient pendant l'exécution de la requête, il est de type « erreur ».
- Un message OperationOutcomes envoyé en tant que partie d'une ressource *Bundle* contient uniquement des « avertissements » ou des « informations ». L'utilisateur doit toujours être informé de l'existence de ce type de messages et avoir la possibilité de les lire.
- L'élément « OperationOutcome.issue.code fournir une description normalisée du problème. Les systèmes PEUVENT créer une logique basée sur le code envoyé en réponse.
- Les détails du problème ou de l'avertissement se trouvent dans l'élément « issue.details.text ». Ce contenu doit toujours être affiché à l'utilisateur.
- Les valeurs « issue.details.coding », « issue.diagnostics » et « issue.location » servent à des fins de diagnostic et ne sont généralement utiles qu'au personnel du soutien technique. Il peut être judicieux de prévoir un bouton pour l'accès à cette information plutôt que de l'afficher systématiquement à l'utilisateur, car elle pourrait prêter à confusion.
- L'élément « issue.location » ne sera présent que si le problème touche une occurrence FHIR soumise c'est-à-dire qu'il ne sera pas présent si le problème concerne les paramètres de la requête, les entêtes HTTP, etc.). Il sera exprimé en XPath, que le contenu soumis ait été au format XML ou JSON.