pan-Canadian FHIR Exchange (CA:FeX) Interoperability Specifications

Version: 1.0.0

Type: Trial Implementation Candidate

Release Date: September 9, 2022

Canada Health Infoway

Table of Contents

1 CA:FeX Interoperability Specifications

1.1 Introduction

Interoperability enables information to flow seamlessly between different solutions and devices. When different parts of the health care system are interoperable with each other, they can “speak the same language.” Interoperability improves continuity of care, collaboration between health care providers and patient access to their health information. By breaking down data silos, it also reduces inefficiencies and redundancies within the health care system.

Connection, collaboration and communication have never been more important for the health care system. Increased use of digital health solutions within healthcare has highlighted the need for safe and efficient electronic sharing of information across the circle of care. Continuing to improve Canadian health care will necessitate work in interoperability — connected systems are healthier systems.

In support of the provinces and territories, Canada Health Infoway (Infoway) is facilitating a national collaborative effort to advance interoperability. While there are many interoperability-related challenges, this specification addresses standardized sharing of vital patient information for the benefit of health care providers and patients using FHIR based information exchange. This FHIR based information exchange is similar to and accomplishes the same objectives as a Health Information Exchange (HIE).

The Office of the National Coordinator for Health Information Technology (ONC) defines HIE as:

> *Electronic health information exchange (HIE) allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient’s vital medical information electronically—improving the speed, quality, safety and cost of patient care.*
> *While electronic health information exchange cannot replace provider-patient communication, it can greatly improve the completeness of patient’s records, (which can have a big effect on care), as past history, current medications and other information is jointly reviewed during visits.*
> *Appropriate, timely sharing of vital patient information can better inform decision making at the point of care and allow providers to avoid readmissions, avoid medication errors, improve diagnoses and decrease duplicate testing.*

1.2 Intended Audience

The intended audience of the CA:FeX Interoperability Specifications (Canadian FHIR Exchange (CA:FeX)), includes but is not limited to:

- Those interested in integrating healthcare information systems and workflows;
- IT departments of healthcare institutions;
- Technical staff of clinical solution vendors;
- Experts involved in standards development; and
- Software developers.

1.3 Purpose

The purpose of this document is to address the following functionality for release 1:

- Address two FHIR HIE use cases;
- Provide a detailed set of requirements (including actors, transactions and references to specific profiles and standards);
- Describe the implementation patterns that enable the exchange of clinical information using CA:FeX; and
- Describe the set of requirements that complement the set of IHE Profiles and HL7 FHIR® Profiles required by the CA:FeX specifications with Canadian specific constraints.

1.4 Glossary of Terms and Acronyms

The following table provides a list of terms and acronyms that you may encounter throughout the pan-Canadian interoperability specifications (e.g. PS-CA, CA:FeX) and/or in the prototyping and validation information.

Term / Acronym	Meaning
ATNA	The Audit Trail and Node Authentication (ATNA) Profile specifies the foundational elements needed by all forms of secure systems: node authentication, user authentication, event logging (audit), and telecommunications encryption. It is also used to indicate that other internal security properties such as access control, configuration control, and privilege restrictions are provided. (Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html)
Author (e.g., PS-CA Author)	A health care provider who authors and/or curates clinical data (e.g. Patient Summary).
Business/Legal Interoperability Requirements	Requirements that enable independent organizations to execute a collaborative process or service.
Business Requirements: Non-Testable	Business requirements that are not directly traceable to an IHE profile in the PS-CA specifications (e.g., provided for consideration and to support and provide guidance to implementers of the PS-CA).
Business Requirements: Testable	Business requirements that are directly traceable to an IHE profile in the PS-CA specifications.
CA:FeX	The CA:FeX Interoperability Specifications (Canadian FHIR Exchange (CA:FeX)) seek to promote FHIR RESTful exchange patterns, developed by industry-leading FHIR standards that can be applied on top of an existing non-FHIR infrastructure just as easily as it can be applied on top of FHIR servers.
CA:FMT	Canadian Formatting Service (CA:FMT) is a Canadian Integration Specification that provides formatting support service. It provides support for transformation of documents between different formats (e.g. from FHIR to PDF, CDA, etc.).
CCDD	The Canadian Clinical Drug Data Set (CCDD) is the drug terminology for use in digital health solutions such as electronic prescribing in Canada.
Central Infrastructure	A Central Infrastructure collects health information from participating organizations and stores the information in a centralized place. The Infrastructure also provides access control. Typically, the Central Infrastructure is under jurisdictional control.

Term / Acronym	Meaning
Clinical Data eXchange (CDX)	CDX is a clinical distribution service developed by Interior Health. Northern Health (NH) and Interior Health (IH) have collaborated to facilitate the sharing of Health Authority clinical information to participating provider EMR systems using this service. (Sources: https://infocentral.infoway-inforoute.ca/en/resources/docs/coordofcare/1406-clinical-document-exchange-bc-cdx-technical-overview-coc-sep27-16 https://www.intrahealth.com/sites/default/files/docs/Clinical-Data-eXchange-communication-from-Intrahealth-and-CDX-Team.pdf)
Clinical Data Repository	A clinical data repository is built around the HL7® FHIR®standard used for storing clinical data.
Clinical Solution	Any combination of health information technology assets and processes that enables clinical data to be communicated, managed, and dispositioned between a Producer and a Consumer. Clinical Solutions can be comprised of various Producer and Consumer systems including: EMR, HIS, CIS, PHR, EHR or any combination of these systems.
Conformance Testing	Conformance testing is a formal process of assessment focused on ensuring clinical solutions and systems accurately implement a particular specification (e.g. PS-CA Specifications) by ensuring there is conformance to the stated parameters that are being claimed in the standard.
Consumer (e.g., PS-CA Consumer)	A health records system (e.g., EMR, HIS, CIS, PHR, Patient Portal or EHR) that enables access to or receipt of a clinical document (e.g. PS-CA) by an authorized health care provider or the subject of care/patient.
Cross Border, Scheduled Care	Scheduled care of a resident of Canada that is delivered in/by another country.
Cross Border, Unscheduled Care	Unscheduled care of a resident of Canada that is delivered in/by another country.
CT	The Consistent Time Integration Profile (CT) provides a means to ensure that the system clocks and time stamps of the many computers in a network are well synchronized. This profile specifies synchronization with a median error less than 1 second. This is sufficient for most purposes. (Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-7.html)
DIN	A Drug Identification Number (DIN) is a computer-generated eight digit number assigned by Health Canada to a drug product prior to being marketed in Canada.

Term / Acronym	Meaning
Document Repository (Local or Central)	A document repository is a shared storage space for clinical documents (Patient Summaries) that can be hosted locally (i.e., at the document producer) or at the HIE Central Infrastructure and can be accessed by authorized users.
DPD	The Drug Product Database (DPD) is used to find drugs authorized for sale by Health Canada. The DPD is updated nightly and includes availability of the drug in Canada.
Electronic Health Record (EHR)	The EHR represents the Clinical Solution that contains a secure and private collection of a patient's health information in a digital format, which is shareable across different health care settings / clinical solutions that are integrated. The EHR facilitates better sharing and interpretation of health information among the health care professionals involved in the care of the patient. For example: • CareConnect is British Columbia's secure, view-only EHR solution. It offers healthcare providers access to an integrated, provincial view of patient-centric information available 24/7 to support the delivery of patient care. • HEALTHe NL is the Newfoundland & Labrador provincial EHR. HEALTHe NL will provide more accurate and reliable data to support improved health care delivery, decision-making and policy and create improved accountability, stability and efficiency in the provincial health care system. • Netcare is Alberta's name for all the projects related to the provincial EHR - a secure and confidential electronic system of Alberta patients' health information: a single, comprehensive, and integrated patient record. • Other clinical systems: In some health authorities, other clinical systems may act as an EHR, holding the patient summary information.
Extensible PS-CA Dataset	Extensible PS-CA Dataset: PS-CA content that can be extended for use in a PS-CA use case scenario that complements the primary PS-CA use cases. *Note: Extensible PS-CA Dataset refers to the addition of data domains such as Family History.
FHIR® Repository	A FHIR repository is a clinical data repository built around the HL7® FHIR® standard used for storing clinical data.
Gazelle	Gazelle is a suite of virtual tools, developed by IHE Europe used to support interoperability testing. Gazelle will allow jurisdictions and vendors an opportunity to validate the role they will be playing in an ecosystem and ensure they are able to satisfy the interoperability requirements. Gazelle offers several self-serve, self-test and innovation opportunities for jurisdictions and vendors to test their alignment to the represented integration profiles.
HCP	Health Care Provider

Term / Acronym	Meaning
Health Information Access Layer (HIAL)	An interface specification for the EHR infostructure that defines service components, service roles, information model and messaging standards required for the exchange of EHR data and execution of interoperability profiles between EHR services. (Source:https://www.infoway-inforoute.ca/en/component/edocman/resources/technical-documents/391-ehrs-blueprint-v2-full ; Page.340)
Health Information Exchange (HIE)	Electronic health information exchange (HIE) allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically—improving the speed, quality, safety and cost of patient care. While electronic health information exchange cannot replace provider-patient communication, it can greatly improve the completeness of patients' records, (which can have a big effect on care), as past history, current medications and other information is jointly reviewed during visits. Appropriate, timely sharing of vital patient information can better inform decision making at the point of care and allow providers to avoid readmissions, avoid medication errors, improve diagnoses and decrease duplicate testing. (Source: https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie)
Health Records System	A health records system may include an electronic medical records system, a hospital information system, a clinical information system, an electronic health records system or a personal health records system. The term is broadly used to describe system actors that may produce and/or consume a PS-CA. Jurisdictional implementation patterns will determine which systems are used to create, access, consume and manage patient summaries.
HIS	Health Information System
Health Level 7 (HL7®)	Founded in 1987, HL7 is a not-for-profit standards developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. (Source: http://www.hl7.org/about/index.cfm?ref=nav)
HL7® Fast Healthcare Interoperability Resources (FHIR®)	Expected to be a next generation standards framework created by HL7. FHIR® combines the best features of HL7's Version 2, Version 3 and product lines while leveraging the latest web standards and applying a tight focus on implementability. (Source: http://www.hl7.org/implement/standards/fhir/)

Term / Acronym	Meaning
Health Records System	A health records system may include an electronic medical records system, a hospital information system, a clinical information system, an electronic health records system or a personal health records system. The term is broadly used to describe system actors that may produce and/or consume a PS-CA. Jurisdictional implementation patterns will determine which systems are used to create, access, consume and manage patient summaries.
Information/ Semantic Interoperability Requirements	Requirements for syntax and semantics such that data exchanged between health record systems can be interpreted and the meaning of the data ascertained.
Integrating the Healthcare Enterprise (IHE)	IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively. (Source: https://www.ihe.net/)
IHE Actor	IHE Actors are responsible for producing, managing and/or acting on information in the context of an IHE Profile (e.g., Primary Care Provider, EMR, EHR, etc.). (Source: https://wiki.ihe.net/index.php/Actors)
IHE Domain	IHE Domains are responsible for the development and maintenance of the IHE Technical Frameworks that document the Integration Profiles. Each Domain manages Integration Profiles in a particular part of healthcare (e.g., Virtual Care). (Source: https://wiki.ihe.net/index.php/Domains)
IHE Profiles	IHE Profiles describe specific solutions to interoperability problems. Profiles specify how "Actors" use standards to address a specific healthcare use case (e.g., Medication, Allergy Intolerance, etc.). (Source: https://wiki.ihe.net/index.php/Profiles)
IHE Transactions	IHE Transactions are interactions between actors that communicate the required information through standards-based messages (e.g., patient look-up query, send patient summary information, etc.). (Source: https://wiki.ihe.net/index.php/PCC_TF-1/About)

Term / Acronym	Meaning
International Patient Summary (IPS)	The IPS is a a minimal, non-exhaustive set of data elements defined by ISO/EN 17269 and realized by HL7 in both CDA and FHIR. The IPS is a snapshot clinical document that can be used for planned or unplanned care of a person locally or across borders. It emphasizes the data required and the necessary conformance of the use cases for an international patient summary. (Source: https://wiki.ihe.net/index.php/International_Patient_Summary_(IPS))
Interoperability	Interoperability enables information to flow seamlessly between different solutions and devices. When different parts of the health system are interoperable with each other, they can "speak the same language." Interoperability improves continuity of care, collaboration between health providers and patient access to their health information. By breaking down data silos, it also reduces inefficiencies and redundancies within the health system. Connection, collaboration and communication have never been more important for the health system. Increased use of virtual care has highlighted the need for safe and efficient electronic sharing of information across the circle of care. Continuing to improve Canadian health care will necessitate work in interoperability — connected systems are healthier systems. For more information about interoperability, please visit Canada Health Infoway - Interoperability.
IUA	The Internet User Authorization (IUA) Profile provides support for authorizing network transactions when using HTTP RESTful transports. IHE has authorization profiles for the Web Services and SOAP based transactions, and this profile provides an authorization profile for the HTTP RESTful transactions. (Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-34.html)
Local, Scheduled Care	Scheduled care of a resident of Canada that is delivered in/by the Canadian health care system. This includes care provided in federal, provincial and territorial jurisdictions, as well as cross-jurisdictional care.
Local, Unscheduled Care	Unscheduled care of a resident of Canada that is delivered in/by the Canadian health care system. This includes care provided in federal, provincial and territorial jurisdictions, as well as cross-jurisdictional care.
Longitudinal Electronic Health Record	A longitudinal electronic health record is a single comprehensive patient record comprised of data from numerous data sources across the healthcare continuum.

Term / Acronym	Meaning
Medical Home	The College of Family Physicians of Canada describes the Medical Home as: "The Patient's Medical Home (PMH) is a family practice defined by its patients as the place they feel most comfortable—most at home—to present and discuss their personal and family health and medical concerns. It is the central hub for the timely provision and coordination of a comprehensive menu of health and medical services patients need." To read more about the Patient's Medical Home, please visit The College of Family Physicians of Canada's published document, A Vision for Canada - Family Practice - The Patient's Medical Home.
MHD	The Mobile access to Health Documents (MHD) Profile defines one standardized interface to health document sharing (a.k.a. an Application Programming Interface (API)) for use by mobile devices so that deployment of mobile applications is more consistent and reusable. (Source: https://profiles.ihe.net/ITI/MHD/index.html)
Patient Portal	A patient portal is a web-based access point that enables secure patient access to personal health information and other self-serve health IT services. For example, a patient portal can be hosted on an EMR solution.
Patient Proxy	An individual or entity that has the authority to act on behalf of a subject of care/ patient. Proxies can include parents of dependent children, parents of dependent adults, powers of attorney, etc.
Patient Summary-CA (PS-CA)	An electronic patient summary for use at the point of care comprised of, at minimum, the required elements of the Patient Summary-CA data set and specifications. The PS-CA is a health record extract, at a snapshot in time, comprised of a standardized collection of clinical and contextual information (retrospective, concurrent, prospective), including the minimum necessary and sufficient data to inform a patient's treatment at the point of care. The PS-CA is condition-independent and specialty-agnostic, irrespective of the condition of the patient or the treatment sought or specialty of the provider delivering care.
PDQm	The Patient Demographics Query for Mobile (PDQm) Profile defines a lightweight RESTful interface to a patient demographics supplier leveraging technologies readily available to mobile applications and lightweight browser based applications. (Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-38.html)
PIXm	The Patient Identifier Cross-reference for Mobile (PIXm) Profile provides RESTful transactions for mobile and lightweight browser-based applications to create, update and delete patient records in a Patient Identifier Cross-reference Manager and to query the Patient Identifier Cross-reference Manager for a patient's cross-domain identifiers. (Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-41.html)

Term / Acronym	Meaning
PMIR	The Patient Master Identity Registry (PMIR) Profile supports the creating, updating and deprecating of patient master identity information about a subject of care, as well as subscribing to changes to the patient master identity, using the HL7 FHIR standard resources and RESTful transactions. (Source: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_PMIR.pdf)
Producer (e.g., PS-CA Producer)	A health records system (e.g., EMR, HIS, CIS, PHR, or EHR) that creates/produces a clinical document (e.g. PS-CA) in response to a request from an authorized health care provider, the subject of care or another authorized health records system.
Projectathon	A Projectathon is an important step and a best-practice approach in testing and validation of a specification package, where implementers collaborate to test their solutions using methodology and tools that accelerate interoperability. A Projectathon provides an opportunity for participants to test their systems among themselves and against a reference environment. It is also an opportunity to collaborate among peers to enable hands-on knowledge exchange.
PS-CA Solution	Any combination of health information technology assets and processes that enables a Patient Summary-CA to be created, communicated, managed and dispositioned between a PS-CA Producer and a PS-CA Consumer. Patient Summary-CA Solutions can be comprised of various Producer and Consumer systems including: EMR, HIS, CIS, PHR, EHR or any combination of these systems.
PS-CA Specifications	**pan-Canadian Patient Summary Interoperability Specifications:** The pan-Canadian Patient Summary Interoperability Specification is an implementable, testable specification, based on the IHE International Patient Summary specification and the HL7 IPS Implementation Guide. For more information on the PS-CA Specifications, please go here.
PT	Provinces and Territories
RA	The Reference Architecture (RA) is intended as an evolving blueprint of service availability that supports a broader interoperability landscape, not limited to patient summaries. Its purpose is to facilitate multi-stakeholder dialogue, collaboration and convergence towards common, open standards. It is a conceptual technical view that provides a common vocabulary and a set of actors and transactions representing typical components in a digital health ecosystem (public and private sector solutions). It is combination of building blocks adopted from international standards development bodies and Canadian developed implementation patterns.
SUT	System Under Test

Term / Acronym	Meaning
SVCM	Sharing Valuesets, Codes and Maps (SVCM) defines a lightweight interface through which healthcare systems may retrieve centrally managed uniform nomenclature and mappings between code systems based on the HL7 Fast Healthcare Interoperability Resources (FHIR) specification. (Source: https://wiki.ihe.net/index.php/Sharing_Valuesets,_Codes_and_Maps_(SVCM))
Technical Interoperability Requirements	Requirements for one health record system to send data to another health record system and for the receiving system to acknowledge receipt of the data payload.
Terminology	Collection of uniquely identifiable concepts with associated representations, designations, associations and meanings.
XDM	Cross-Enterprise Document Media Interchange (XDM) provides document interchange using a common file and directory structure over several standard media types. This permits the patient to use physical media to carry medical documents. This also permits the use of person-to-person email to convey medical documents. XDM supports the transfer of data about multiple patients within one data exchange. (Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-16.html)
XDS	The Cross-Enterprise Document Sharing (XDS) IHE Integration Profile facilitates the registration, distribution and access across health enterprises of patient electronic health records. (Source: https://profiles.ihe.net/ITI/TF/Volume1/ch-10.html)

1.5 Preface

The CA:FeX Interoperability Specifications (Canadian FHIR Exchange (CA:FeX)) seek to promote FHIR RESTful exchange patterns, developed by industry-leading FHIR standards that can be applied on top of an existing infrastructure just as easily as it can be applied on top of FHIR servers.

The current version of CA:FeX is focused on the FHIR RESTful exchange of documents, which FHIR offers multiple structures and patterns to achieve. CA:FeX aims to provide clarity to implementers by identifying some of the choices currently available using FHIR, ranging from simple to a higher level of sophistication. As the development of CA:FeX continues, the Interoperability Specifications may evolve into a more formal Integration Profile (similar to existing international profiles reviewed below) that provides more comprehensive guidance on FHIR RESTful exchange patterns than what currently exists today.

The scope of CA:FeX may evolve beyond document-based exchange to explore a more atomic nature of health information exchange in the future. This will depend on the development of a multi-phased CA:FeX roadmap, the evolving needs of the Canadian health care market, and emerging trends within the international FHIR health information exchange community.

Upon review of legacy IHE profiles, existing guidance is either based on the enablement of document sharing within non-FHIR infrastructures or through the narrow use of FHIR resources. Given the evolving needs of the Canadian

market, these legacy profiles may not be entirely sufficient to enable the FHIR RESTful exchange of documents. Two key existing IHE profiles that were contemplated, including some of their limitations, are listed below:

- *Cross-Enterprise Document Sharing (XDS):* This IHE profile is focused on providing a standards-based specification for the sharing of documents which is limited to non-FHIR infrastructures. Note that, although considered, the XDS profile is not presented as an option within the Reference Architecture, as the Canadian landscape revealed that it is interested in adopting more modern FHIR-based approaches.
- *Mobile access to Health Documents (MHD):* This IHE profile is designed for the utilization of FHIR standard to communicate and exchange documents, including, as an option, acting as a proxy to systems that use XDS. MHD leverages FHIR resources (i.e., DocumentReference) as a standard method for clients to find a document. To ensure this IHE profile can be used without regard for how information is stored (e.g., XDS infrastructure, FHIR, or another storage system) the profile applies constraints to the FHIR DocumentReference resource. The current limitation of MHD, however, requires that a document is submitted in FHIR Binary format and does not include the use of a FHIR Bundle (of type Document) to represent documents. Further, MHD entails a multi-step document retrieval process (list/find step followed by the retrieval step) which may not be the single approach implementers will take going forward.

Through a market scan, it was observed that in line with MHD, existing RESTful driven FHIR Implementation Guides that include document exchange (e.g., US Core, IPA, PACIO, IPS, etc.) have begun utilizing a pattern, leveraging the DocumentReference Resource and/or the $docRef operation. These Implementation Guides, however, enable querying in a single way and return pointers to document content, wherever it is stored and irrespective of the format (e.g., binary or FHIR-assembled). FHIR Search Parameters and FHIR Operations have been developed to augment the capabilities of this pattern to more easily get back what was requested and enable the offering of documents in the expected format without having to change the underlying data model / document and lifecycle practices.

Within the context of the Canadian market, there is an indication that the level of readiness for exchange patterns outlined by international FHIR Implementation Guides, such as the US Core, may not be appropriate for implementers in the current state. As such, simpler exchange patterns have been explored as a viable alternative. One such alternative, that is the primary focus of CA:FeX v1.0.0 Trial Implementation, is narrowing the focus to the exchange of non-binary documents and utilizing the appropriate FHIR Search Parameters based on the Bundle and Composition Resources to search and retrieve documents.

Earlier versions of the CA:FeX specification outlined emerging patterns for using DocumentReference Resource and FHIR Operations (e.g., CA:FeX 2B, CA:FeX 3B, Cutting Edge Capabilities) to find and retrieve documents from hybrid repositories. Given the focus of the current ecosystem to start with support of FHIR Documents, and that these options are still being tested and addressed by the FHIR document exchange community, these patterns will be addressed in a future release of the CA:FeX. As international specifications mature and the Canadian market evolves, CA:FeX will dig deeper into the more sophisticated alternatives for health information exchange in order to guide the Canadian market in the same direction.

Due to the continuous development of the market, there will be an opportunity to encompass a broader set of use cases that may deal with the exchange of more atomic information going forward.

In parallel with CA:FeX, Canada Health Infoway is also facilitating a national collaborative effort to develop the pan-Canadian Patient Summary Interoperability Specifications (PS-CA), an implementable, testable specification, based on the IHE International Patient Summary specification and the HL7 IPS Implementation Guide. The PS-CA references the CA:FeX Interoperability Specifications as an optional implementation pattern for submitting, searching and retrieving a Patient Summary document.

1.5.1 Context

The CA:FeX Interoperability Specifications are published to a public space within Canada Health Infoway's InfoScribe and are also available as a downloadable document, here. InfoScribe is a web-based tool developed for jurisdictions and vendors to create, publish, and collaborate on clinical requirements and specifications for

interoperability solutions. Teams can document, share, and discuss content, files, ideas, specs, mock-ups, diagrams, and projects. A link to the online published content and the downloadable documentation will be published with each release of CA:FeX.

1.5.2 Introduction to IHE

Integrating the Healthcare Enterprise (IHE) is an international initiative to promote the use of standards to achieve interoperability among health information technology (HIT) systems and effective use of electronic health records (EHRs). IHE provides a forum for care providers, HIT experts and other stakeholders in several clinical and operational domains to reach consensus on standards-based solutions to critical interoperability issues.

The primary output of IHE is system implementation guides, called IHE profiles. IHE publishes each profile through a well-defined process of public review and Trial Implementation and gathers profiles that have reached Final Text status into an IHE Technical Framework.

1.5.3 How to Read This Document

This document contains the following sections:

Document Section	Description	Target Audience
CA:FeX Interoperability Specifications	CA:FeX is an implementable, testable specification based on HL7 FHIR Implementation Guides. It defines building blocks to enable FHIR Health Information Exchange (HIE) implementation patterns. CA:FeX building blocks are configurable to address necessary Canadian jurisdictional variances. The CA:FeX Interoperability Specifications, written in line with international best practices, contain the information necessary for an implementer to consume and develop the components necessary for creating, consuming and sharing clinical data and may be applied to existing and new information systems.	Solution Developers
Use Cases & Definitions	The Use Cases & Definitions present the broader context for clinical, business, interoperability and solution development considerations that were discovered during the development of the CA:FeX Interoperability Specifications. This section defines the healthcare problem that CA:FeX addresses and includes healthcare use cases and interoperability requirements in terms that will be traceable to the content in the Reference Architecture, which defines the actors and their interactions in scope for the CA:FeX Interoperability Specifications.	CTOs, CMIOs, CIOs, PTs and Vendors
Exchanging Documents in FHIR	The Exchanging Documents in FHIR section contains methods for implementing the CA:FeX transactions specifically for document exchange using FHIR RESTful APIs. As the content is refined and evolved it will grow into a FHIR implementation guide.	Solution Developers

Within the Pan-Canadian CA:FeX Interoperability Specifications, you can expect the following subsections:

- **Introduction & Preface:** Contains an introduction to the CA:FeX Interoperability Specifications. This section contains a summary of the context, document purpose and scope, as well as other content to help orient the first-time reader to the topic of these specifications and how they relate to other specifications in the digital health ecosystem in Canada.
- **Privacy & Security Guidance:** Provides a reference to Infoway's recently published privacy primer, Privacy as an Enabler, that provides an introduction to interoperability, an overview of Canadian privacy laws and some practical approaches to privacy for interoperability. And, it provides a high-level list of security considerations for the CA:FeX specifications.
- **Use Case Overview:** Describes the Use Cases, including design constraints and assumptions and the flows of information that will be specified in the CA:FeX Interoperability Specifications. This section also references scenarios that describe how the specified flows may be used in the Canadian context.
- **Core Interoperability Specification Requirements:** Establishes the Core Interoperability Requirements for the CA:FeX Interoperability Specifications with respect to a FHIR Health Information Exchange (HIE) implementation pattern. This section also provides mapping of use case actors to the technical actors of the CA:FeX Interoperability Specifications and the services they are supporting, which are aligned with the flow captured in the sequence diagrams included here.
- **CA:FeX Actor Conformance:** Establishes the Actor Conformance Requirements for the CA:FeX Interoperability Specifications.
- **CA:FeX Actors and Transactions:** Illustrates the abstracted actors and transactions in scope for the CA:FeX Interoperability Specifications.
- **CA:FeX Sequence Diagrams:** Provides guidance on how to apply CA:FeX implementation patterns along with other IHE profiles to address interoperability needs pertaining to FHIR Health Information Exchange (HIE) implementation pattern. They group together actors and transactions from multiple profiles including CA:FeX to address the scope of the use cases.
- **CA:FeX Cross Profile Considerations:** Provides guidance on groupings between the CA:FeX actors with other IHE profiles to achieve additional functionality such as Network Security, Authentication, Authorization, Auditing and more.
- **CA:FeX Audit Considerations:** Provides audit considerations for each of the CA:FeX transactions.

1.5.4 Document Conventions

The CA:FeX Interoperability Specifications will be versioned according to the IO Specifications Publication Model, defined here.

1.5.5 Requirements Language

The following conventions are used to specify requirement levels for the business requirements of the CA:FeX Interoperability Specifications:

- **Shall:** used to indicate a **required** requirement.
- **Should:** used to indicate that a requirement is **recommended** and should be considered as best practice for implementation, but not required (i.e., it is optional) for implementation.
- **May:** used to indicate that a requirement is permittable / **optional**, but not required for implementation.
- **Shall not:** used to indicate that an element or action is prohibited.

Additional information on the CA:FeX business requirements can be found in the Use Cases and Definitions section.

1.5.6 Methodology

The CA:FeX Interoperability Specifications have been developed based on international research and stakeholder consultations with HIE Subject Matter Advisors, where this was socialized and validated with participating

jurisdictions and vendors through Coordinating Table Meetings, Executive Table Meetings, stakeholder workshops and 1-on-1 meetings to further refine the specifications.

1.5.7 Introduction to a Use-Case Driven Approach

The following use case-driven approach was utilized in the development of the CA:FeX Interoperability Specifications:

- **Baseline:** Develop foundational Use Cases, Use Case Scenarios and Business Requirements for FHIR Health Information Exchange (HIE).
- **Collaborate:** Collaborate with jurisdictions, clinical SMEs, technical SMEs, vendors, participating organizations to develop and refine detailed artefacts.
- **Review:** Review and provide feedback into artefacts through engagement workshops and input gathering.
- **Publish:** Publish artefacts for broader stakeholder consultation.
- **Recommend:** Recommend draft artefacts for approval.
- **Iterate:** Continue to refine as per testing and priorities.

1.5.8 Release Cycle

The CA:FeX Interoperability Specifications' release cycle includes a multi-stage review and feedback process, as documented here.

1.6 Privacy & Security Guidance

1.6.1 Privacy Considerations

Infoway has developed a privacy primer, Privacy as an Enabler, that provides an introduction to interoperability, an overview of Canadian privacy laws and some practical approaches to privacy for interoperability. It delves into the role privacy plays in the creation of interoperable health systems. It addresses the myth that privacy laws mean patient data can't be shared. The primer outlines how privacy laws enable the sharing of patient data by providing guidance on how to share health data safely, with a patient's consent, and the responsibilities of both parties when patient information is shared.

Download the privacy primer here: Privacy as an Enabler: Sharing Personal Health Information for Interoperability Primer.

1.6.2 Security Considerations

Fast Healthcare Interoperability Resources (FHIR) is not a security protocol, nor does it define any security related functionality. However, FHIR does define exchange protocols and content models that need to be used with various security protocols defined elsewhere.

FHIR transactions defined as part of the CA:FeX implementation pattern often make use of patient-specific information which could be exploited by malicious actors resulting in exposure of patient data. For this reason, all FHIR transactions must be secured appropriately with access to limited authorized individuals, data protected in transit, and appropriate audit measures taken.

Implementers SHOULD be aware of security considerations associated with FHIR transactions (http://hl7.org/fhir/R4/security.html), particularly those related to:

- Communications
- Authentication
- Authorization/Access Control

- Audit Logging
- Digital Signatures
- Security Labels
- Narrative

Additionally, many FHIR transactions using HTTP REST will include query parameters that would be identifiers, quasi-identifiers, or sensitive health topics. For example, it is common for patient identifier to be a query parameter. With this URL pattern, the query parameters are typically visible in the server audit log or browser history. The risk from this visibility should be mitigated in system or operational design, by protecting the logs as sensitive data, or by designing other measures into the system to prevent inappropriate exposure.

1.7 CA:FeX Use Case Overview

1.7.1 Use Case Overview

This section describes the two Use Cases for the FHIR Health Information Exchange (HIE) Implementation Pattern, including all design constraints and assumptions as well as the flows of information that will be specified in the CA:FeX Interoperability Specifications. This section also introduces the scenarios that describe how the specified workflows may be used in the Canadian e-health context.

1.7.2 In-Scope

The following Use Cases are in scope for this release:

- UC-01 Create and Submit Document
- UC-02 Query and Retrieve Document

Use Case details can be found in the Use Cases and Definitions section.

1.7.3 Use Case Actors and Services

The Use Case Actors and the Services that are used by this specification are described below. Additional information can be found in the Core Interoperability Specifications Requirements section.

Use Case Actors and Descriptions

Actor Name	Description / Definition
Producer	A health records system (e.g., EMR, HIS, CIS, PHR, or EHR) that creates/produces clinical data in response to a request from an authorized health care provider, the subject of care or another authorized health records system.
Consumer	A health records system (e.g., EMR, HIS, CIS, PHR, Patient Portal or EHR) that enables access to or receipt of clinical data by an authorized health care provider or the subject of care/patient.
Clinical Data Repository (Local or Central)	A Clinical Data Repository is a shared storage space for clinical documents that can be hosted locally (e.g., at the data producer) or at the Central Infrastructure and can be accessed by authorized users.

Actor Name	Description / Definition
Central Infrastructure	A Central Infrastructure collects health information from participating organizations and stores the information in a centralized place. The Infrastructure also provides access control. Typically, the Central Infrastructure is under jurisdictional control.

Use Case Actor Mapping

Actor Name	UC-01	UC-02
Producer	x	
Consumer		x
Clinical Data Repository (Local or Central)	x	x
Central Infrastructure	x	x

1.8 Core Interoperability Specification Requirements

1.8.1 Actor Mapping to Interoperability Specification

The Use Case Actors and the Services they support are described at a functional level in the Use Cases and Definitions section of the CA:FeX Interoperability Specifications. Services may be Required or Optional. The Use Case Actor, Service(s) and optionality are conveyed in the first three columns of Tables 1 and 2 in the section below. The second part of the table (columns 4-7) provides the mapping for the Use Case Actor to the detailed specifications (such as Technical Actors and Optionality) that systems shall implement to exchange healthcare information in the context of these use cases. The purpose of the tables below is to map the use case actors to the technical actors and the services they are supporting. These tables are aligned with the flow captured in the sequence diagrams which are included in the Sequence Diagram section.

For a selected Use Case Actor (a single row in the table), the system shall implement all of the requirements (some optionality when allowed) listed in the second part of the table (columns 4-7). This includes the referenced healthcare profiles, the standards specified and terminology standards. For Technical Actors, which map to CA:FeX or an IHE Profile (*CA:FeX, PDQm, PMIR, etc.*), the last column provides the reference location of the specification. Links for these referenced specifications have been included in the tables below. Additionally, the below table does not showcase all of the possible combinations of IHE profiles and transactions that can be used for a particular implementation pattern. For example, 'Identify Patient' service can use PIXm in place of PDQm if the preferred implementation pattern is PIXm/PMIR.

Versioning

This is an evolving specification; the release cycle assumes some degree of change will happen across versions. (Read more about the versioning protocol here.) There will be a process in place to monitor changes in the current versions of the IHE profiles which will be incorporated in future versions of the CA:FeX Interoperability Specifications based on our interoperability roadmap.

Published Versions

The following describes the published versions in scope for the required and optional IHE Profiles that have been referenced in this specification. Refer to the Reference Architecture RA v0.1.0 DFT for details:

- IUA: Revision 2.1 - Trial Implementation
- PDQm: v2.3.0: Trial Implementation based on FHIR R4
- PMIR: Revision 1.3 – Trial Implementation

Legend

R = Required

O = Optional

1.8.2 Table 1 Interoperability Conformance Requirements for Use Case 1: Create and Submit Document

USE CASE 1: Create and Submit Document			**MAPPING TO SECTIONS FROM THIS AND REFERENCED INTEROPERABILITY SPECIFICATIONS**			
USE CASE ACTOR	SERVICE SUPPORTED	OPT	TECHNICAL ACTOR	OPT	PROFILE/ STANDARD	REFERENCED SPECIFICATION AND STANDARDS
Producer	Authenticate User	O	Client (e.g. EMR)	O	Internet User Authorization (IUA)	Refer to the Cross Profile Considerations section: Internet User Authorization (IUA) Grouping.
	Identify Patient	O	Client (e.g. EMR)	O	Use Existing Standards Employed by the Clinical System	N/A
		O	Patient Demographic Consumer	O	PDQm	Refer to PDQm within the RA v0.1.0 DFT.
	Retrieve Clinical Data (Patient Identifer)	R	Client (e.g. EMR)	R	Use Existing Standards Employed by the Clinical System	N/A

USE CASE 1: Create and Submit Document			**MAPPING TO SECTIONS FROM THIS AND REFERENCED INTEROPERABILITY SPECIFICATIONS**			
USE CASE ACTOR	SERVICE SUPPORTED	OPT	TECHNICAL ACTOR	OPT	PROFILE/ STANDARD	REFERENCED SPECIFICATION AND STANDARDS
	Assemble and Review Document	R	Client (e.g. EMR)	R	Use Existing Standards Employed by the Clinical System	N/A
	Omit or Mask Data based on Jurisdictional Policy	O	Client (e.g. EMR)	O	Jurisdictional Requirement	N/A
	Save Document to Clinical Data Repository	R	Client (e.g. EMR)	R	Use Existing Standards Employed by the Clinical System	N/A
		R	Data Source	R	CA:FeX	Refer to Submit a Document in the Exchanging Documents in FHIR section.
Clinical Data Repository (Central)	Save Bundle to Clinical Data Repository	R	Data Recipient	R	CA:FeX	Refer to Submit a Document in the Exchanging Documents FHIR section.
Central Infrastructure	Identify Patient	O	Patient Identity Registry	O	PMIR	Refer to PMIR within the RA v0.1.0 DFT.

1.8.3 Table 2 Interoperability Conformance Requirements for Use Case 2: Query and Retrieve Document

USE CASE 2: Query and Retrieve Document			**MAPPING TO SECTIONS FROM THIS AND REFERENCED INTEROPERABILITY SPECIFICATIONS**			
USE CASE ACTOR	SERVICE SUPPORTED	OPT	TECHNICAL ACTOR	OPT	PROFILE/ STANDARD	REFERENCED SPECIFICATION AND STANDARDS
Consumer	Authenticate User	O	Client (e.g. EMR)	O	Internet User Authorization (IUA)	Refer to the Cross Profile Considerations section: Internet User Authorization (IUA) Grouping.
	Identify Patient	O	Client (e.g. EMR)	O	Use Existing Standards Employed by the Clinical System	N/A
		O	Patient Demographic Consumer	O	PDQm	Refer to PDQm within the RA v0.1.0 DFT.
	Request Search Document (Patient Identifier)	R	Client (e.g. EMR)	R	Use Existing Standards Employed by the Clinical System	N/A
	Request Document (Resource ID)	R	Client (e.g. EMR)	R	Use Existing Standards Employed by the Clinical System	N/A
	Return *searchset* Bundle	R	Data Consumer	R	CA:FeX	Refer to Search for a Document in the Exchanging Documents in FHIR section.
	Return *document* Bundle	R	Data Consumer	R	CA:FeX	Refer to Retrieve a Document in the Exchanging Documents in FHIR section.

USE CASE 2: Query and Retrieve Document			**MAPPING TO SECTIONS FROM THIS AND REFERENCED INTEROPERABILITY SPECIFICATIONS**			
USE CASE ACTOR	SERVICE SUPPORTED	OPT	TECHNICAL ACTOR	OPT	PROFILE/ STANDARD	REFERENCED SPECIFICATION AND STANDARDS
Clinical Data Repository (Central)	Retrieve Resources from Clinical Data Repository	R	Data Responder	R	CA:FeX	Refer to Search for a Document in the Exchanging Documents in FHIR section.
	Retrieve Bundle from Clinical Data Repository	R	Data Responder	R	CA:FeX	Refer to Retrieve a Document in the Exchanging Documents in FHIR section.
Central Infrastructure	Identify Patient	O	Patient Identity Registry	O	PMIR	Refer to PMIR within the RA v0.1.0 DFT.

1.9 Actor Conformance

A system conforming to the CA:FeX Interoperability Specifications shall claim conformance at the level of a Use Case Actor (first columns of Table 1 and Table 2 of section Core Interoperability Specification Requirements). A system may claim conformance to one or more Use Case Actors among:

- Producer
- Consumer
- Clinical Data Repository (Local or Central)
- Central Infrastructure

Producer and Consumer use case actor roles will primarily be taken up by EMR clinical solution vendors. Clinical Data Repository and Central Infrastructure use case actor roles can be taken up either by EMR clinical solution vendors or jurisdictions depending on the implementation approach that the jurisdiction decides to adopt. Similarly, the Consumer can be a Patient Portal, in which case the use case actor can be taken up either by a vendor or jurisdiction depending on the approach and policies defined regarding patient / subject of care access to their personal health information (PHI).

In order to implement a system that fully supports the CA:FeX Interoperability Specifications v1.0.0 Trial Implementation, the system shall be able to demonstrate that it conforms to every required actor and transaction for which it is claiming conformance.

1.9.1 Constraints on Use Case Actors

The section below captures some of the design constraints on use case actors when developing functionality to support the services mapped to them.

Note: The scope of this section is limited to the constraints that are applicable to actors and transactions defined for CA:FeX Interoperability Specifications (See section CA:FeX Actors and Transactions). The two key services supported by CA:FeX are:

- Save Document to Clinical Data Repository
- Retrieve Document from Clinical Data Repository

The following section provides key design constraints for implementation of these two required services using RESTful APIs based on CA:FeX and FHIR standards. To support these two services, the following three RESTful transactions have been defined:

Service Supported	FHIR RESTful Transactions
Save Document to Clinical Data Repository	1. Submit Data [CA:FeX-1]
Retrieve Document from Clinical Data Repository	2. Search Data [CA:FeX-2]
	3. Retrieve Data [CA:FeX-3]

Save Document to Clinical Data Repository

The Producer and Clinical Data Repository Use Case Actors are required to implement the *Save Document to Clinical Data Repository* service.

These actors shall use the FHIR transaction **Submit Data [CA:FeX-1]** of CA:FeX that executes a *Submit Data request* from a Data Source to a Data Recipient.

Submit Data [CA:FeX-1]

This message involves a request by a Data Source to transfer a FHIR document to a Data Recipient. The request is received by a Data Recipient which stores the received FHIR documents and returns an HTTP response code.

Trigger Events

This method is invoked when the Data Source needs to submit one or more FHIR documents to a Data Recipient (Clinical Data Repository).

Message Semantics

This message uses the HTTP POST method on the target Submit Data endpoint to convey the metadata and the document(s) as a FHIR transaction. The Data Source shall initiate a FHIR “transaction” using a “create” action by sending an HTTP POST request method composed of a FHIR Resource. The media type of the HTTP body shall support application/fhir+json and should support application/fhir+xml. Additional information on this FHIR implementation pattern is provided in the Submit a Document section under Exchanging Documents in FHIR.

Expected Actions

The Data Recipient shall accept media types application/fhir+json and application/fhir+xml. On receipt of the submission, the Data Recipient shall validate the resources and respond with one of the HTTP response codes and an OperationOutcome, if applicable. Additional information on handling responses is provided in the Response Handling section under Exchanging Documents in FHIR.

Retrieve Document from Clinical Data Repository

The Consumer and Clinical Data Repository (Central) Use Case Actors are required to implement the *Retrieve Document from Clinical Data Repository* service.

These actors shall use the following transactions to find metadata and retrieval of identified clinical document:

- **Search Data [CA:FeX-2]**
- **Retrieve Data [CA:FeX-3]**

Search Data [CA:FeX-2]

This message involves a query request by a Data Consumer to find FHIR documents using parameterized queries. The request is received by a Data Responder which returns a Bundle containing the matching search parameters.

The Data Consumer may use HTTP GET or HTTP POST based searches. The Data Responder shall support both GET and POST based searches.

Trigger Events

When a Data Consumer needs to discover a list of FHIR Bundle Resources or retrieval of documents that are anticipated to be a mix of FHIR-assembled (Composition) and FHIR-enabled (Binary) documents.

Message Semantics

The Data Consumer executes an HTTP search request against the Data Responder endpoint (FHIR Repository).

The Data Consumer may use HTTP GET or HTTP POST based searches. The Data Responder shall support both GET and POST based searches.

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

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

Query Search Parameters

The following search parameters are used generically to support document retrieval.

Additional search parameters that are specific to the requirements for a specific use case or IGuide (e.g., PS-CA) may be further defined by those implementations.

Query Search Parameters	Applied to	Description
timestamp	bundle.timestamp	This parameter, of type date, specifies the timestamp when the FHIR bundle was created. See FHIR http://hl7.org/fhir/R4/search.html#date for use of the date search type.
patient.identifier	bundle.composition.patient.identifier	This parameter, of type token, specifies an identifier associated with the patient to which the document is assigned. This use of patient.identifier follows the FHIR Chaining Parameters search methodology.
type	bundle.composition.type	This parameter, of type token, specifies the kind of document (LOINC if possible). The use of bundle.composition.type follows the FHIR Chaining Parameters search methodology.

Query Search Parameters	Applied to	Description
status	bundle.composition.status	This parameter, of type token, specifies the status of the composition. The use of bundle.composition.status follows the FHIR Chaining Parameters search methodology.
author	bundle.composition.author	This parameter, of type reference, specifies who and/or what authored the document. The use of bundle.composition.author follows the FHIR Chaining Parameters search methodology.
date	bundle.composition.date	This parameter, of type date, specifies when this document reference was created. The use of bundle.composition.date follows the FHIR Chaining Parameters search methodology.

Additional information on this FHIR implementation pattern including Document Search Pattern options is provided in the Search for a Document section under Exchanging Documents in FHIR.

Expected Actions

The Data Responder shall process the query and return a search result matching the search criteria included in the request. The FHIR standard provides encodings for responses as either XML or JSON.

Additional information on handling responses is provided in the Response Handling section under Exchanging Documents in FHIR.

Security Considerations

Data Responder SHALL reject any unauthorized requests by returning an HTTP 401 unauthorized response code. This transaction should not return information that the Data Consumer is not authorized to access (authorization here is inclusive of system, app, and user according to local policy, patient consents, and security layering). However, the transaction may return search bundle that have Reference elements that the Data Consumer may not have access to. This is to say that the authorization need only be to the content returned in the Bundle. There may be references (URLs) for which the content is not authorized. This is considered proper as the Data Consumer would need to retrieve the content pointed to by those references, and at that time the proper authorization decision would be made on that context and content. In this way it is possible for a Data Consumer to get Resources that are pointing at data that the Data Consumer is not authorized to retrieve. Thus, the URLs used must be carefully crafted so as to not expose sensitive data in the URL value.

Retrieve Data [CA:FeX-3]

This message involves a request by a Data Consumer for retrieving known documents using the document's resource id from a Clinical Data Repository. The request is received by a Data Responder which returns the requested FHIR document(s) or returns an HTTP response code.

This message uses the HTTP GET request to retrieve the identified FHIR document(s) from the central Clinical Data Repository.

Trigger Events

This method is invoked when the Data Consumer needs to retrieve FHIR document(s).

Message Semantics

The Data Consumer sends an HTTP GET request to the server based on a known resource id from the Data Responder. This operation will return a Bundle that was previously identified in a search/or prior retrieval or an embedded attachment in DocumentReference or a Binary resource.

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

Additional information on this FHIR implementation pattern including Document Search Pattern options is provided in the Retrieve a Document section under Exchanging Documents in FHIR.

Expected Actions

The Data Responder shall process the GET request and respond with FHIR Document(s) matching the specified identifier included in the request. When the requested document is returned, the Data Responder shall respond with an HTTP Status Code 200. The HTTP message-body shall be the content of the requested document.

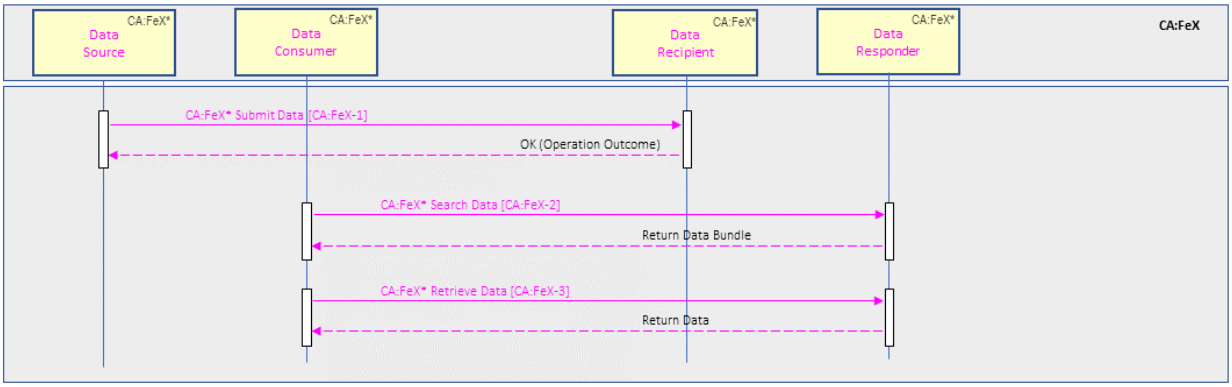
Additional information on handling responses is provided in the Response Handling section under Exchanging Documents in FHIR.

Security Considerations

Data Responder SHALL reject any unauthorized requests by returning an HTTP 401 unauthorized response code. This transaction should not return information that the Data Consumer is not authorized to access.

1.10 CA:FeX Actors and Transactions

The following diagram illustrates the actors and transactions in scope for the CA:FeX Interoperability Specification.



There are three primary transactions for the CA:FeX Interoperability Specification, along with additional sub-transactions listed below for specific circumstances. Please refer to the Exchanging Documents in FHIR section for more details.

Transaction ID	Description	Notes
CA:FeX-1	Submit Data	
CA:FeX-2	CA:FeX-2A: Search Against FHIR Assembled Documents Repository	
	CA:FeX-2B: Search Against Hybrid Documents Repository	Future consideration

Transaction ID	Description	Notes
CA:FeX-3	CA:FeX-3A: Retrieve Document From FHIR Assembled Documents Repository	
	CA:FeX-3B: Retrieve Document from Hybrid Documents Repository	Future consideration

1.11 CA:FeX Sequence Diagrams

The CA:FeX sequence diagrams provide guidance on how to apply CA:FeX implementation patterns along with other IHE profiles to address interoperability needs pertaining to FHIR Health Information Exchange (HIE) implementation patterns. They group together actors and transactions from multiple profiles including CA:FeX to address the scope of the use cases.

1.11.1 Sequence Diagram for UC-01: Create and Submit Document

Scenario: Clinical Solution A Retrieves Document from a Central Clinical Data Repository

Assumption: Document is stored in a Clinical Data Repository

This sequence diagram provides the option of using the CA:FeX Interoperability Specifications that provide support for saving and retrieving data (e.g., documents) to and from a central Clinical Data Repository. This specification includes a Data Source and a Data Recipient actor. Additionally, this sequence diagram uses the 'Submit Data' FHIR operation.

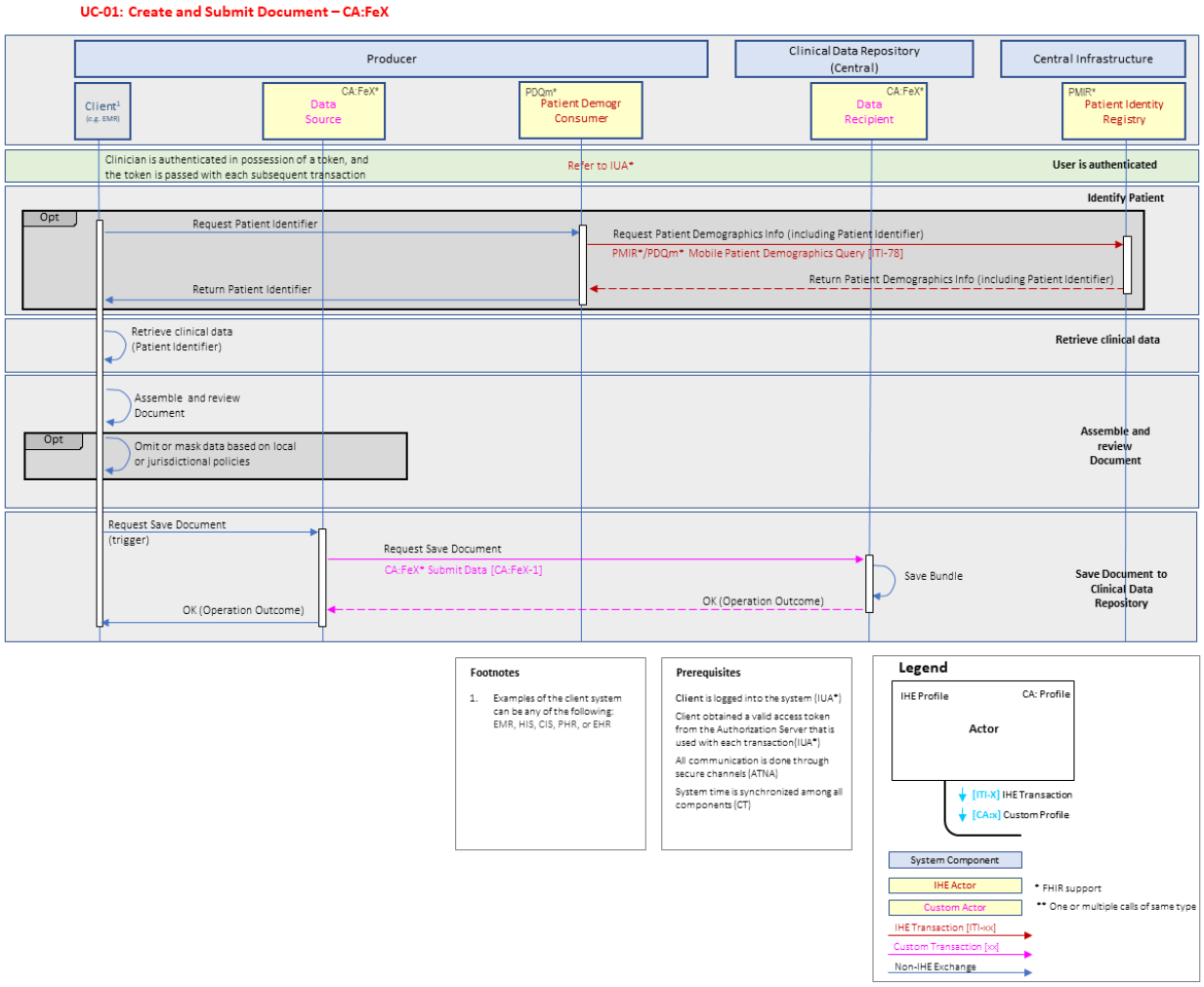
Sequence Diagram Overview:

Below provides guidance on how to read the sequence diagram:

- This sequence diagram illustrates how the different standardized actors of a system should interact with each other to carry out specific standardized transactions, and the order in which the transactions and interactions occur when UC-01 of the CA:FeX Specification is executed.
- The legend on the bottom right corner describes the different system components, actors and transactions that are necessary to carry out this use case.
- The green swim lane is a simplified view of the actors and transactions required by the Foundational Profiles, defined here, in addition to the other ones that are not explicitly illustrated on the diagram (e.g., ATNA, CT, etc.) but included as a white note. These are pre-requisite conditions for this use case and it is assumed that these will be satisfied.
- The blue swim lanes group a sequence of processes (along with their required actors and transactions) that are needed to occur to satisfy this use case. These are to be read from left to right and top to bottom.
- The red note boxes describe important information and notes that provide more context for the sequence diagram.
- For more information on core IHE Profiles and specific Canadian implementation guidance, refer to the Reference Architecture available here: RA v0.1.0 DFT.

Additional Considerations

The sequence diagrams included in this section do not showcase all of the possible combinations of IHE profiles and transactions that can be used for a particular implementation pattern. For example, ITI-83 transaction can be used in place of ITI-78 if the preferred implementation pattern is PIXm/PMIR.



1.11.2 Sequence Diagram for UC:02: Query and Retrieve Document

Scenario: Clinical Solution A Retrieves Clinical Data from a Clinical Data Repository.

Assumption: Clinical Data is stored in a Central Clinical Data Repository

This sequence diagram provides the option of using the CA:FeX Interoperability Specifications that provide support for saving and retrieving data (e.g. documents) to and from a central Clinical Data Repository. This specification includes a Data Consumer and a Data Responder actor. Additionally, this sequence diagram uses the 'Search Data' and 'Retrieve Data' FHIR operations.

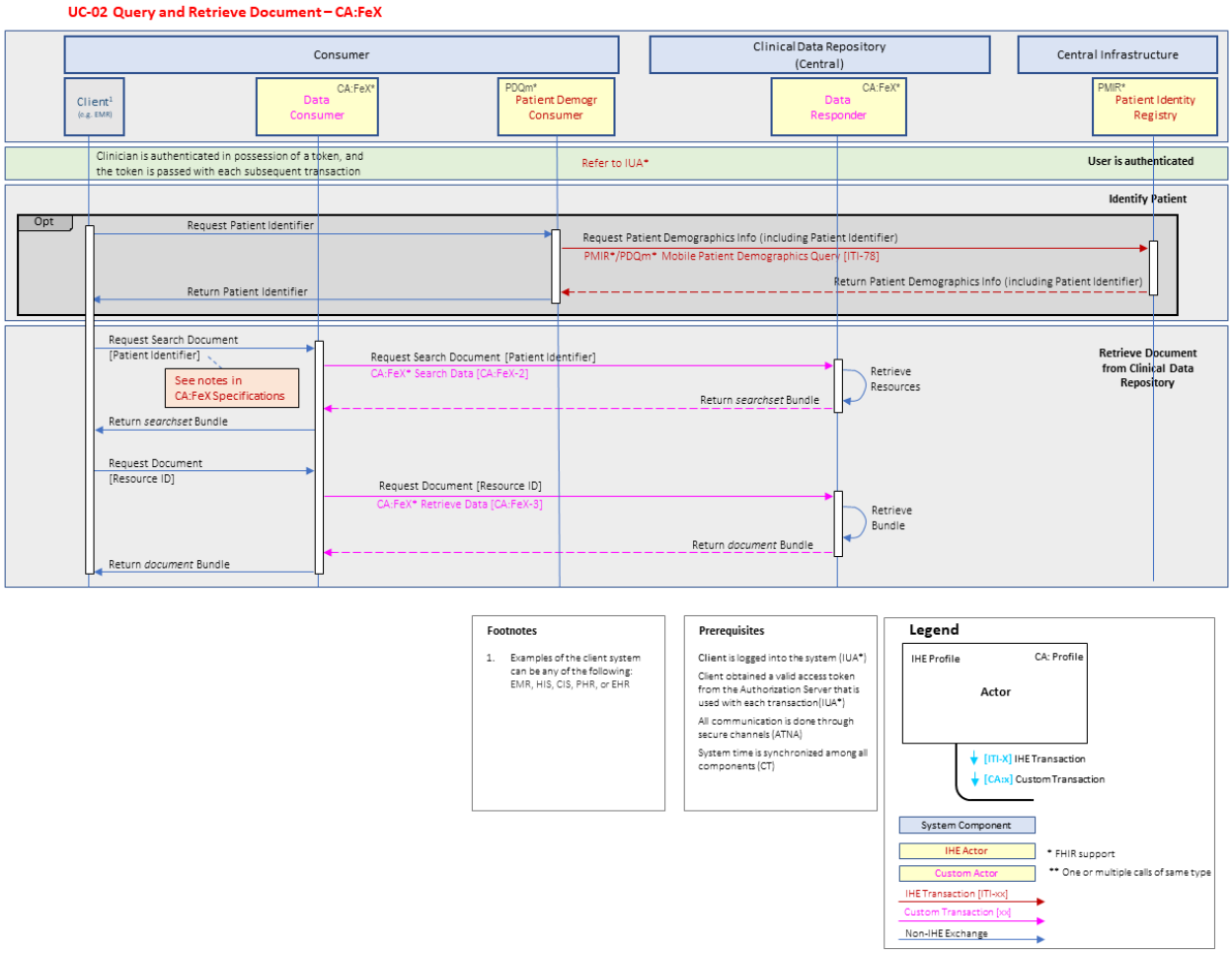
Sequence Diagram Overview:

Below provides guidance on how to read the sequence diagram:

- This sequence diagram illustrates how the different standardized actors of a system should interact with each other to carry out specific standardized transactions, and the order in which the transactions and interactions occur when Use Case 2 of the CA:FeX Specification is executed.
- Data Consumer role varies by client type:
    - HCP: Clinical Solution, e.g., EMR used by the Health Care Provider to request & retrieve access to clinical document(s) from the Clinical Data Repository
    - Patient: Patient Portal used by the Patient / Subject of Care to request & retrieve access to their clinical document(s) from the Clinical Data Repository
- The legend on the bottom right corner describes the different system components, actors and transactions that are necessary to carry out this particular use case.
- The green swim lane is a simplified view of the actors and transactions required by the Foundational Profiles, defined here, in addition to the other ones that are not explicitly illustrated on the diagram (e.g. ATNA, CT) but included as a white note. These are pre-requisite conditions for this particular use case and it is assumed that these will be satisfied.
- The blue swim lanes group sequence of processes (along with their required actors and transactions) that are needed to occur to satisfy this particular use case. These are to be read from left to right and top to bottom.
- The red note boxes describe important call outs, information and notes that provide more context for the sequence diagram.
- For more information on core IHE Profiles and specific Canadian implementation guidance, refer to the Reference Architecture available here: RA v0.1.0 DFT.

Additional Considerations

The sequence diagrams included in this section do not showcase all of the possible combinations of IHE profiles and transactions that can be used for a particular implementation pattern. For example, ITI-83 transaction can be used in place of ITI-78 if the preferred implementation pattern is PIXm/PMIR.



1.12 CA:FeX Cross Profile Considerations

This section provides guidance on groupings between the CA:FeX actors with other IHE profiles to achieve additional functionality such as Network Security, Authentication, Authorization, Auditing and more.

1.12.1 Consistent Time (CT) Grouping

The Consistent Time (CT) Profile provides a means to ensure that the system clocks and time stamps of the computers in a network are synchronized. To allow for these features, CA:FeX actors can be grouped with CT actors.

For the specific Canadian implementation guidance for the CT profile, refer to the RA v0.1.0 DFT, section **CT - Canadian Implementation Guidance**.

If the grouping is in place, an actor from CA:FeX shall implement the required transactions and/or content modules in CA:FeX in addition to all the transactions required for the grouped actor (Column 2).

CA:FeX Actor	**Actor(s) to be grouped with**
Data Source	CT / Time Client

Data Recipient	CT / Time Client
Data Consumer	CT / Time Client
Data Responder	CT / Time Client

1.12.2 Internet User Authorization (IUA) Grouping

The Internet User Authorization (IUA) Profile provides support for user authentication, app authentication, and authorization decisions. To allow for these features, CA:FeX actors can be grouped with IUA actors.

For the specific Canadian implementation guidance for the IUA profile, refer to the RA v0.1.0 DFT, section **IUA - Canadian Implementation Guidance**.

If the grouping is in place, an actor from CA:FeX shall implement the required transactions and/or content modules in CA:FeX ***in addition to all*** the transactions required for the grouped actor (Column 2).

CA:FeX Actor	**Actor(s) to be grouped with**
Data Source	IUA / Authorization Client
Data Recipient	IUA / Resource Server
Data Consumer	IUA / Authorization Client
Data Responder	IUA / Resource Server

The CA:FeX Data Source and Data Consumer actors, when grouped with IUA Authorization Client, shall use Get Access Token [ITI-71] to request the corresponding scope from the IUA Authorization Server.

This enables the CA:FeX actor to submit the corresponding CA:FeX transaction with the combined transaction Incorporate Access Token [ITI-72].

The CA:FeX Data Recipient and Data Responder actors. When grouped with IUA Resource Server, shall require Incorporate Access Token [ITI-72] in all CA:FeX transaction requests, shall enforce the authorization decision in the token, and may further enforce policies beyond those made by the Authorization Server such as consent or business rules.

There are additional security and privacy functionalities enabled by this grouping.

- Transactions are combined with IUA transactions requiring access tokens
- There are additional requirements and functionality enabled through scope definitions that are transaction specific.

Actors	**Transactions**	**IUA/OIDC Scopes**
Data Source	Submit Data [CA:FeX-1]	CAFEX-1
Data Recipient	Submit Data [CA:FeX-1]	CAFEX-1

Data Consumer	Search Data [CA:FeX-2]	CAFEX-2
	Retrieve Data [CA:FeX-3]	CAFEX-3
Data Responder	Search Data [CA:FeX-2]	CAFEX-2
	Retrieve Data [CA:FeX-3]	CAFEX-3

Each scope authorizes the full CA:FeX transaction. This scope implicitly allows for patient-specific CRUD/S operations in line with and supported by the corresponding CA:FeX transaction.

Further scope refinement is allowed in realm or project-specific situations; these scopes would be in addition to the scopes defined here.

1.12.3 Canadian Network Security (CA:Sec) Grouping

The Reference Architecture provides specific Canadian implementation guidance for the implementation of the network security aspect of the ATNA profile in Canada. For details, refer to the RA v0.1.0 DFT, section **Canadian Network Security (CA:Sec) Implementation Guidance.**

CA:Sec provides support for secure network communication. To allow for these features, CA:FeX actors can be grouped with CA:Sec actors.

If the grouping is in place, an actor from CA:FeX shall implement the required transactions and/or content modules in CA:FeX ***in addition to all*** the transactions required for the grouped actor (Column 2).

CA:FeX Actor	**Actor(s) to be grouped with**
Data Source	CA:Sec / Secure Application
Data Recipient	CA:Sec / Secure Application
Data Consumer	CA:Sec / Secure Application
Data Responder	CA:Sec / Secure Application

The CA:FeX actors, when grouped with CA:Sec Secure Application, shall use the Authenticate Node [ITI-19] transaction to ensure secure communication between actors.

1.12.4 Canadian Audit Trail (CA:Aud) Grouping

The Reference Architecture provides specific Canadian implementation guidance for the implementation of the auditing aspect of the ATNA profile in Canada. For details, refer to the RA v0.1.0 DFT, section **Canadian Audit Trail (CA:Aud) Implementation Guidance.**

CA:Aud provides support for Event Logging for Auditing. To allow for these features, CA:FeX actors can be grouped with CA:Aud actors.

If the grouping is in place, an actor from CA:FeX shall implement the required transactions and/or content modules in CA:FeX ***in addition to all*** the transactions required for the grouped actor (Column 2).

CA:FeX Actor	Actor(s) to be grouped with
Data Source	CA:Aud / Audit Creator
Data Recipient	CA:Aud / Audit Creator
Data Consumer	CA:Aud / Audit Creator
Data Responder	CA:Aud / Audit Creator

CA:FeX actors, when grouped with CA:Aud Audit Creator, shall use the Record Audit Event [ITI-20] transaction to send audit event log messages to an Audit Record Repository.

1.13 CA:FeX Audit Considerations

To add support for audit, CA:FeX actors are recommended to be grouped with CA:Aud actors (see Cross Profile Considerations / Canadian Audit Trail (CA:Aud) Grouping).

Alternatively, other non-IHE methods can be used to record audit messages, that do not require grouping with CA:Aud actors.

The audit criteria are defined for each actor that participates in a CA:FeX transaction.

1.13.1 Submit Data [CA:FeX-1] Audit

The audit criteria are similar to other IHE transactions that export a document, such as MHD Provide Document Bundle[ITI-65] transaction).

Data Source Audit

The Data Source when grouped with CA:Aud Secure Node or Secure Application actor shall be able to record a Submit Data Source Audit Event Log.

Terminology Bindings

Path	Conformance	ValueSet / Code
AuditEvent.language	preferred	CommonLanguages **Max Binding**: AllLanguages
AuditEvent.type	extensible	Pattern: 110106("Export")
AuditEvent.subtype	extensible	Pattern: CA:FeX-1("Submit Data")
AuditEvent.action	required	Pattern: R
AuditEvent.outcome	required	AuditEventOutcome

AuditEvent.purposeOfEvent	extensible	PurposeOfUse
AuditEvent.agent.type	extensible	ParticipationRoleType
AuditEvent.agent.role	example	SecurityRoleType
AuditEvent.agent.media	extensible	MediaTypeCode
AuditEvent.agent.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataSource.type	extensible	Pattern: 110153("Source Role ID")
AuditEvent.agent:dataSource.role	example	SecurityRoleType
AuditEvent.agent:dataSource.media	extensible	MediaTypeCode
AuditEvent.agent:dataSource.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataSource.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataRecipient.type	extensible	Pattern: 110152("Destination Role ID")
AuditEvent.agent:dataRecipient.role	example	SecurityRoleType
AuditEvent.agent:dataRecipient.media	extensible	MediaTypeCode
AuditEvent.agent:dataRecipient.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataRecipient.purposeOfUse	extensible	PurposeOfUse
AuditEvent.source.type	extensible	AuditEventSourceType
AuditEvent.entity.type	extensible	AuditEventEntityType
AuditEvent.entity.role	extensible	AuditEventEntityRole

AuditEvent.entity.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity.securityLabel	extensible	All Security Labels
AuditEvent.entity:patient.type	extensible	Pattern: 1("Person")
AuditEvent.entity:patient.role	extensible	Pattern: 1("Patient")
AuditEvent.entity:patient.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:patient.securityLabel	extensible	All Security Labels
AuditEvent.entity:submissionSet.type	extensible	Pattern: 2("System Object")
AuditEvent.entity:submissionSet.role	extensible	Pattern: 20("Job")
AuditEvent.entity:submissionSet.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:submissionSet.security Label	extensible	All Security Labels

Data Recipient Audit

The Data Recipient when grouped with CA:Aud Secure Node or Secure Application actor shall be able to record a Submit Data Recipient Audit Event Log.

Terminology Bindings

Path	Conformance	ValueSet / Code
AuditEvent.language	preferred	CommonLanguages **Max Binding**: AllLanguages
AuditEvent.type	extensible	Pattern: 110107("Import")
AuditEvent.subtype	extensible	Pattern: CA:FeX-1("Submit Data")
AuditEvent.action	required	Pattern: C
AuditEvent.outcome	required	AuditEventOutcome
AuditEvent.purposeOfEvent	extensible	PurposeOfUse

AuditEvent.agent.type	extensible	ParticipationRoleType
AuditEvent.agent.role	example	SecurityRoleType
AuditEvent.agent.media	extensible	MediaTypeCode
AuditEvent.agent.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataSource.type	extensible	Pattern: 110153("Source Role ID")
AuditEvent.agent:dataSource.role	example	SecurityRoleType
AuditEvent.agent:dataSource.media	extensible	MediaTypeCode
AuditEvent.agent:dataSource.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataSource.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataRecipient.type	extensible	Pattern: 110152("Destination Role ID")
AuditEvent.agent:dataRecipient.role	example	SecurityRoleType
AuditEvent.agent:dataRecipient.media	extensible	MediaTypeCode
AuditEvent.agent:dataRecipient.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataRecipient.purposeOfUse	extensible	PurposeOfUse
AuditEvent.source.type	extensible	AuditEventSourceType
AuditEvent.entity.type	extensible	AuditEventEntityType
AuditEvent.entity.role	extensible	AuditEventEntityRole
AuditEvent.entity.lifecycle	extensible	ObjectLifecycleEvents

AuditEvent.entity.securityLabel	extensible	All Security Labels
AuditEvent.entity:patient.type	extensible	Pattern: 1("Person")
AuditEvent.entity:patient.role	extensible	Pattern: 1("Patient")
AuditEvent.entity:patient.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:patient.securityLabel	extensible	All Security Labels
AuditEvent.entity:submissionSet.type	extensible	Pattern: 2("System Object")
AuditEvent.entity:submissionSet.role	extensible	Pattern: 20("Job")
AuditEvent.entity:submissionSet.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:submissionSet.security Label	extensible	All Security Labels

1.13.2 Search Data [CA:FeX-2] Audit

The audit criteria are similar to those for the MHD Find Document References [ITI-67] transaction.

Data Consumer Audit

The Data Consumer when grouped with CA:Aud Secure Node or Secure Application actor shall be able to record a Search Data Consumer Audit Event Log.

Terminology Bindings

Path	**Conformance**	**ValueSet / Code**
AuditEvent.language	preferred	CommonLanguages **Max Binding**: AllLanguages
AuditEvent.type	extensible	Pattern: 110112("Query")
AuditEvent.subtype	extensible	Pattern: CA:FeX-2("Search Data")
AuditEvent.action	required	Pattern: E
AuditEvent.outcome	required	AuditEventOutcome

AuditEvent.purposeOfEvent	extensible	PurposeOfUse
AuditEvent.agent.type	extensible	ParticipationRoleType
AuditEvent.agent.role	example	SecurityRoleType
AuditEvent.agent.media	extensible	MediaTypeCode
AuditEvent.agent.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataConsumer.type	extensible	Pattern: 110153("Source Role ID")
AuditEvent.agent:dataConsumer.role	example	SecurityRoleType
AuditEvent.agent:dataConsumer.media	extensible	MediaTypeCode
AuditEvent.agent:dataConsumer.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataConsumer.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataResponder.type	extensible	Pattern: 110152("Destination Role ID")
AuditEvent.agent:dataResponder.role	example	SecurityRoleType
AuditEvent.agent:dataResponder.media	extensible	MediaTypeCode
AuditEvent.agent:dataResponder.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataResponder.purposeOfUse	extensible	PurposeOfUse
AuditEvent.source.type	extensible	AuditEventSourceType
AuditEvent.entity.type	extensible	AuditEventEntityType
AuditEvent.entity.role	extensible	AuditEventEntityRole

AuditEvent.entity.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity.securityLabel	extensible	All Security Labels
AuditEvent.entity:patient.type	extensible	Pattern: 1("Person")
AuditEvent.entity:patient.role	extensible	Pattern: 1("Patient")
AuditEvent.entity:patient.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:patient.securityLabel	extensible	All Security Labels
AuditEvent.entity:queryParameters.type	extensible	Pattern: 2("System Object")
AuditEvent.entity:queryParameters.role	extensible	Pattern: 24("Query")
AuditEvent.entity:queryParameters.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:queryParameters.securityLabel	extensible	All Security Labels

Data Responder Audit

The Data Responder when grouped with CA:Aud Secure Node or Secure Application actor shall be able to record a Search Data Consumer Audit Event Log.

Terminology Bindings

Path	Conformance	ValueSet / Code
AuditEvent.language	preferred	CommonLanguages **Max Binding**: AllLanguages
AuditEvent.type	extensible	Pattern: 110112("Query")
AuditEvent.subtype	extensible	Pattern: CA:FeX-2("Search Data")
AuditEvent.action	required	Pattern: E
AuditEvent.outcome	required	AuditEventOutcome

AuditEvent.purposeOfEvent	extensible	PurposeOfUse
AuditEvent.agent.type	extensible	ParticipationRoleType
AuditEvent.agent.role	example	SecurityRoleType
AuditEvent.agent.media	extensible	MediaTypeCode
AuditEvent.agent.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataConsumer.type	extensible	Pattern: 110153("Source Role ID")
AuditEvent.agent:dataConsumer.role	example	SecurityRoleType
AuditEvent.agent:dataConsumer.media	extensible	MediaTypeCode
AuditEvent.agent:dataConsumer.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataConsumer.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataResponder.type	extensible	Pattern: 110152("Destination Role ID")
AuditEvent.agent:dataResponder.role	example	SecurityRoleType
AuditEvent.agent:dataResponder.media	extensible	MediaTypeCode
AuditEvent.agent:dataResponder.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataResponder.purposeOfUse	extensible	PurposeOfUse
AuditEvent.source.type	extensible	AuditEventSourceType
AuditEvent.entity.type	extensible	AuditEventEntityType
AuditEvent.entity.role	extensible	AuditEventEntityRole

AuditEvent.entity.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity.securityLabel	extensible	All Security Labels
AuditEvent.entity:patient.type	extensible	Pattern: 1("Person")
AuditEvent.entity:patient.role	extensible	Pattern: 1("Patient")
AuditEvent.entity:patient.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:patient.securityLabel	extensible	All Security Labels
AuditEvent.entity:queryParameters.type	extensible	Pattern: 2("System Object")
AuditEvent.entity:queryParameters.role	extensible	Pattern: 24("Query")
AuditEvent.entity:queryParameters.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:queryParameters.securityLabel	extensible	All Security Labels

1.13.3 Retrieve Data [CA:FeX-3] Audit

The audit criteria are similar to those for the MHD Retrieve Document [ITI-68] transaction.

Data Consumer Audit

The Data Consumer when grouped with CA:Aud Secure Node or Secure Application actor shall be able to record a Retrieve Data Consumer Audit Event Log.

Terminology Bindings

Path	**Conformance**	**ValueSet / Code**
AuditEvent.language	preferred	CommonLanguages **Max Binding**: AllLanguages
AuditEvent.type	extensible	Pattern: 110107("Import")
AuditEvent.subtype	extensible	Pattern: CA:FeX-3("Retrieve Data")
AuditEvent.action	required	Pattern: C

AuditEvent.outcome	required	AuditEventOutcome
AuditEvent.purposeOfEvent	extensible	PurposeOfUse
AuditEvent.agent.type	extensible	ParticipationRoleType
AuditEvent.agent.role	example	SecurityRoleType
AuditEvent.agent.media	extensible	MediaTypeCode
AuditEvent.agent.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataConsumer.type	extensible	Pattern: 110153("Source Role ID")
AuditEvent.agent:dataConsumer.role	example	SecurityRoleType
AuditEvent.agent:dataConsumer.media	extensible	MediaTypeCode
AuditEvent.agent:dataConsumer.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataConsumer.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataResponder.type	extensible	Pattern: 110152("Destination Role ID")
AuditEvent.agent:dataResponder.role	example	SecurityRoleType
AuditEvent.agent:dataResponder.media	extensible	MediaTypeCode
AuditEvent.agent:dataResponder.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataResponder.purposeOfUse	extensible	PurposeOfUse
AuditEvent.source.type	extensible	AuditEventSourceType
AuditEvent.entity.type	extensible	AuditEventEntityType

AuditEvent.entity.role	extensible	AuditEventEntityRole
AuditEvent.entity.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity.securityLabel	extensible	All Security Labels
AuditEvent.entity:patient.type	extensible	Pattern: 1("Person")
AuditEvent.entity:patient.role	extensible	Pattern: 1("Patient")
AuditEvent.entity:patient.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:patient.securityLabel	extensible	All Security Labels
AuditEvent.entity:documentUniqueId.what.type	extensible	ResourceType
AuditEvent.entity:documentUniqueId.type	extensible	Pattern: 2("System Object")
AuditEvent.entity:documentUniqueId.role	extensible	Pattern: 3("Report")
AuditEvent.entity:documentUniqueId.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:documentUniqueId.securityLabel	extensible	All Security Labels

Data Responder Audit

The Data Responder when grouped with CA:Aud Secure Node or Secure Application actor shall be able to record a Retrieve Data Responder Audit Event Log.

Terminology Bindings

Path	**Conformance**	**ValueSet / Code**
AuditEvent.language	preferred	CommonLanguages **Max Binding**: AllLanguages
AuditEvent.type	extensible	Pattern: 110106("Export")
AuditEvent.subtype	extensible	Pattern: CA:FeX-3("Retrieve Data")

AuditEvent.action	required	Pattern: R
AuditEvent.outcome	required	AuditEventOutcome
AuditEvent.purposeOfEvent	extensible	PurposeOfUse
AuditEvent.agent.type	extensible	ParticipationRoleType
AuditEvent.agent.role	example	SecurityRoleType
AuditEvent.agent.media	extensible	MediaTypeCode
AuditEvent.agent.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataConsumer.type	extensible	Pattern: 110153("Source Role ID")
AuditEvent.agent:dataConsumer.role	example	SecurityRoleType
AuditEvent.agent:dataConsumer.media	extensible	MediaTypeCode
AuditEvent.agent:dataConsumer.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataConsumer.purposeOfUse	extensible	PurposeOfUse
AuditEvent.agent:dataResponder.type	extensible	Pattern: 110152("Destination Role ID")
AuditEvent.agent:dataResponder.role	example	SecurityRoleType
AuditEvent.agent:dataResponder.media	extensible	MediaTypeCode
AuditEvent.agent:dataResponder.network.type	required	AuditEventAgentNetworkType
AuditEvent.agent:dataResponder.purposeOfUse	extensible	PurposeOfUse
AuditEvent.source.type	extensible	AuditEventSourceType

AuditEvent.entity.type	extensible	AuditEventEntityType
AuditEvent.entity.role	extensible	AuditEventEntityRole
AuditEvent.entity.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity.securityLabel	extensible	All Security Labels
AuditEvent.entity:patient.type	extensible	Pattern: 1("Person")
AuditEvent.entity:patient.role	extensible	Pattern: 1("Patient")
AuditEvent.entity:patient.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:patient.securityLabel	extensible	All Security Labels
AuditEvent.entity:documentUniqueId.what.type	extensible	ResourceType
AuditEvent.entity:documentUniqueId.type	extensible	Pattern: 2("System Object")
AuditEvent.entity:documentUniqueId.role	extensible	Pattern: 3("Report")
AuditEvent.entity:documentUniqueId.lifecycle	extensible	ObjectLifecycleEvents
AuditEvent.entity:documentUniqueId.securityLabel	extensible	All Security Labels

2 Use Cases and Definitions

The purpose is to describe the use cases and workflow scenarios for sharing clinical documents across solutions. Each jurisdiction may have implementation variances within the use cases. Therefore, these use cases do not represent required implementation choices, nor are they representative of all possible implementation choices. These uses cases are to be considered as examples. The use cases provide high-level interactions between a Health Care Provider or Patient using a Clinical Solution (e.g., EMR, Patient Portal, etc.) and the HIE. Use cases provide the business description or "conversation" between the system(s) and its user(s), known as Participants. Participants can be people (e.g., health care providers, patients, etc.) using a Clinical Solution (e.g., EMR, Patient Portal) or systems (e.g., HIE, etc.). Please note that detailed interactions are defined in the CA:FeX Interoperability Specifications Sequence Diagrams section of this document.

Each use case will include:

- use case scenario,
- examples of use case triggers, pre- and post-conditions,
- who the participants are (i.e., people and systems),
- a use case diagram to provide a visual representation of the interactions between participants,
- use case steps corresponding to the diagram and potential alternate flows, and
- requirements.

2.1 Use Case Index

This section includes a proposed list of use cases which were identified as being priority use cases in the pan-Canadian environmental scan. Additional use cases will be defined in future releases.

The scope for this release of the CA:FeX Specifications has been defined to include use cases UC-01 and UC-02.

The list below includes the use cases a Use Case ID, name and description of the use case.

Use Case ID	Use Case Name	Use Case Description
UC-01	Create and Submit Document	A Health Care Provider, in any care setting, adds Patient clinical information for use at point of care, which is made available to other authorized HCPs.
UC-02	Query and Retrieve Document	Query and retrieval of clinical documentation performed by a Health Care Provider for use at the point of care or by the Patient themselves to obtain a copy of their own personal health information.

2.2 Requirement Priority Definitions

Priority	Definition
SHALL	• used to indicate a **required** requirement.

Priority	Definition
SHOULD	• used to indicate that a requirement is **recommended** and **should** be considered as best practice for implementation, but not required (i.e., it is optional) for implementation.

2.3 UC-01 Create and Submit Document

Description

A Health Care Provider, in any care setting, adds Patient clinical information for use at point of care, which is made available to other authorized HCPs.

Scenario

A patient schedules a visit with their regular health care provider, within their Medical Home, with symptoms including dizziness and an earache. The patient mentions that since they last visited, another clinic noted that they have high blood pressure (hypertension) which is being monitored at home for now. The patient also mentions a suspected penicillin allergy. The health care provider determines that the patient has an external ear infection (otitis externa) and prescribes antibiotics. The health care provider creates a clinical note in their EMR, which may trigger automatic updates, such as updates to the prescription information. The health care provider decides to submit this new information to the network (i.e., Clinical Data Repository) so that it is available for other health care providers who may be providing care for this patient.

Triggers, Pre-conditions, Post-Conditions

This section describes example triggers, pre-conditions & post-conditions related to uploading new clinical information to the Clinical Data Repository. It is not inclusive of all potential workflow scenarios which may be implemented within Canadian jurisdictions.

Triggers

- Health Care Provider provides care to a patient and adds clinical information to the Patient's record.
- Health Care Provider receives additional information for a patient that they wish to share with other HCPs. For example, HCP receives test results for a Patient and adds the clinical information to the Patient's problem list.

Pre-conditions

- Clinical documentation shall uniquely identify the Patient so that it can be uploaded to the Clinical Data Repository and available to other HCPs (e.g., uniquely identified by a Client Registry ID)
- In jurisdictions where explicit consent is required to share Patient clinical information:
    - Patient provides, or has previously provided, consent to share their data to the Clinical Data Repository.

Post-conditions

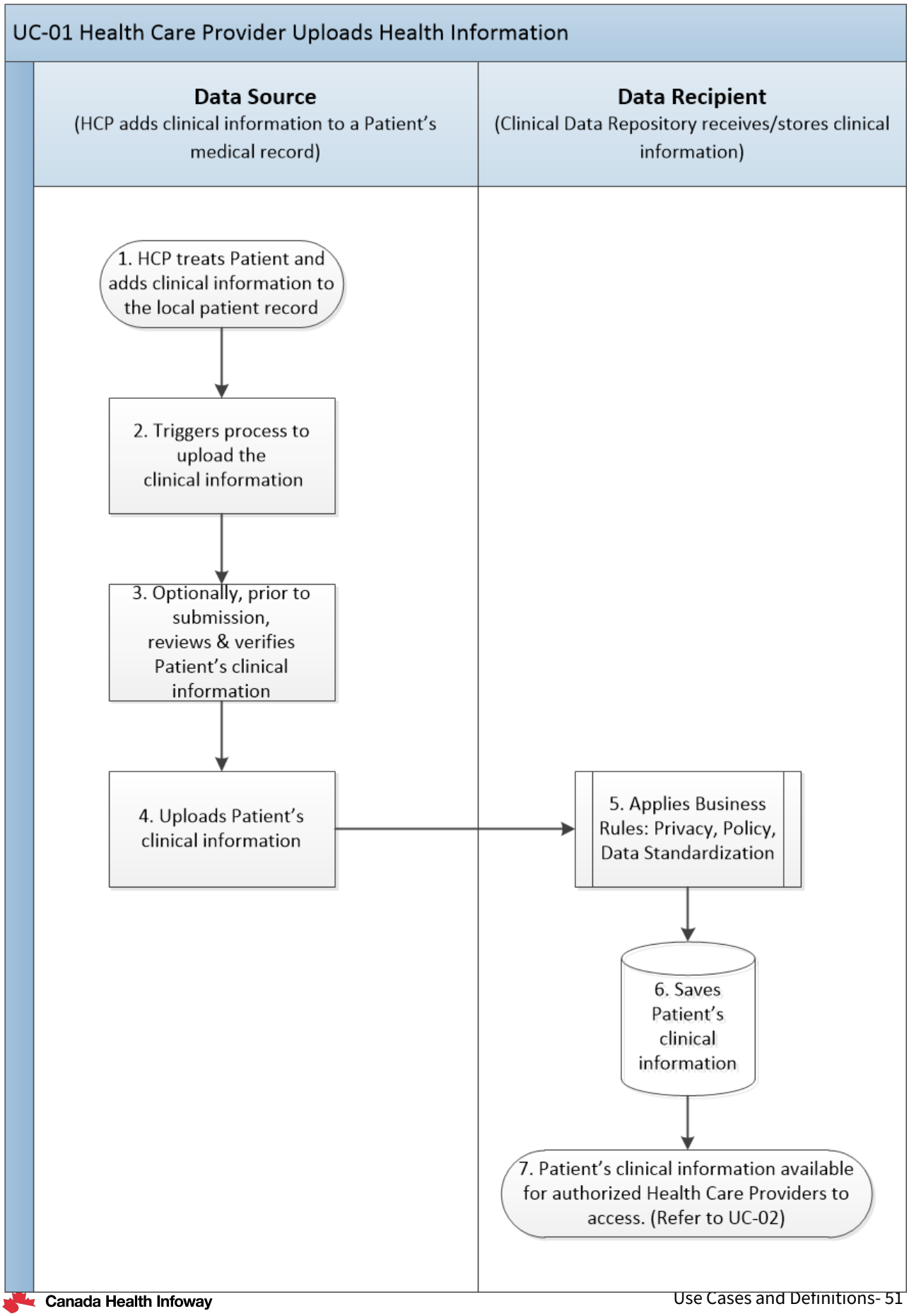
- New Patient clinical information recorded/registered in the Clinical Data Repository.
- Authorized health care providers have access to view the Patient's clinical information or may receive a notification that new clinical information about the patient is available.

Use Case Participants & Diagram

The participants involved in this use case are:

- Data Source (Health Care Provider adding patient clinical information via their local Clinical Solution (e.g., EMR))
- Data Recipient (Clinical Data Repository receiving/storing the Patient's clinical information)

This use case diagram represents the participants and their role in the use case with a high-level view of the flow of information.


UC-01 Health Care Provider Uploads Health Information
Data Source
(HCP adds clinical information to a Patient's medical record)
Data Recipient
(Clinical Data Repository receives/stores clinical information)
1. HCP treats Patient and adds clinical information to the local patient record
2. Triggers process to upload the clinical information
3. Optionally, prior to submission, reviews & verifies Patient's clinical information
4. Uploads Patient's clinical information
5. Applies Business Rules: Privacy, Policy, Data Standardization
6. Saves Patient's clinical information
7. Patient's clinical information available for authorized Health Care Providers to access. (Refer to UC-02)

Use Case - Primary Flow

The following provides a textual description corresponding to the use case diagram.

1. Health Care Provider treats Patient and adds clinical information to the Patient's health record in their local Clinical Solution (e.g., EMR, HIS).
2. Health Care Provider decides to share the new clinical information collected and triggers the process to upload the information to the Clinical Data Repository.
3. Health Care Provider, optionally, reviews and validates the Patient's clinical information prior to sharing/ uploading it to the Clinical Data Repository.
4. Health Care Provider sends / uploads the Patient's clinical information to the Clinical Data Repository.
5. Clinical Data Repository applies business rules (e.g. data standardization, privacy, policy, etc.).
   For example:
   a. Validation of Patient Summary data (e.g. Provider identified and eligible to submit clinical information, Patient identified, etc.)
   b. Checks for existing clinical information for same patient/same provider - apply replacement / archiving rules
6. Clinical Data Repository saves the Patient's clinical information.
   a. Clinical Data Repository responds to the submitting system to indicate that the submission was accepted (i.e., recorded/registered) or it was a bad request.
7. Patient's clinical information is available for access by authorized Health Care Providers. (Refer to UC-02 Query and Retrieve Document)

Use Case - Alternate Flow

The following list provides possible alternate flows that may occur within this use case.

- Step 3: Health Care Provider has the option to bypass an additional review of the clinical information, allowing the Clinical Solution to automatically share/upload the Clinical Information to the Clinical Data Repository.
- Step 3: Health Care Provider, upon review of the clinical information, chooses to make changes within the local Patient's health record prior to uploading it to the Clinical Data Repository.
- Step 4: Health Care Provider, after submitting the Patient's clinical information, identifies that there is incorrect or missing information. The HCP will have the option to modify and upload the corrected clinical information to the Clinical Data Repository.
- Step 4: Health Care Provider, after submitting the Patient's clinical information, identifies that incorrect information has been uploaded (e.g., information is for the wrong patient). The HCP will have the option to retract / delete the information from the Clinical Data Repository.

Use Case - Requirements

The following is a list of key requirements that will be addressed as part of this use case.

#	Category	Requirement Description
1	Write	FHIR API SHALL be capable of accepting write operations to allow creation of new clinical document in the central Clinical Data Repository
2	Response	FHIR API SHALL be capable of returning a response that a new clinical information has been successfully recorded/registered in the central Clinical Data Repository

#	Category	Requirement Description
3	Response	FHIR API SHALL be capable of returning a response that a Patient clinical information could not be recorded/registered in the central Clinical Data Repository (HTTP 400 - Bad Request)

2.4 UC-02 Query and Retrieve Document

Description

Query and retrieval of clinical documentation performed by a Health Care Provider for use at the point of care or by the Patient themselves to obtain a copy of their own personal health information.

Scenario

The following are example scenarios. It is not inclusive of all potential scenarios which may be implemented within Canadian jurisdictions.

1) A Health Care Provider, in any care setting, queries and retrieves a clinical document for use at the point of care

A patient schedules a visit with a health care provider, outside of their Medical Home, with symptoms including dizziness and an earache. The patient mentions that they have a regular health care provider, within their Medical Home, and experiences high blood pressure (hypertension) which is being monitored at home for now. The health care provider collects information from the patient and, using their Clinical Solution (e.g., EMR), searches for clinical information (e.g., searches the network to locate clinical documentation created and shared by another Health Care Provider). Upon finding a clinical document(s) for their patient, the health care provider views and uses the information in support of providing care for this patient.

2) A Patient or Subject of Care accesses/views and can obtain a copy of their own personal health information.

A patient, or their designated caregiver, would like to access their personal health information (PHI) to stay up to date with their medical health information, empowering them to play an active role in their own care.

Triggers, Pre-conditions, Post-conditions

This section describes example triggers, pre-conditions & post-conditions related to the query and retrieval of clinical document(s) from the Clinical Data Repository. It is not inclusive of all potential workflow scenarios which may be implemented within Canadian jurisdictions.

Triggers

Scenario 1:

- Patient visits Health Care Provider for care.
- Where applicable, HCP received a notification that new clinical information is available for the Patient to which they have subscribed to receive notifications.

Scenario 2:

- Patient, or their designated caregiver, chooses to view personal health information to stay informed of their medical information.
- Patient wants to obtain a copy of their personal health information to have on their person while travelling.

- Patient wants to obtain a copy of their personal health information to share with another care provider.

Pre-conditions

Scenario 1:

- Health Care Provider is logged in to their Clinical Solution (e.g., EMR).
- Health Care Provider's Clinical Solution is connected / part of the Clinical Data Repository network.

Scenario 2:

- In jurisdictions where a patient may have applied consent directives to their clinical information, HCP complies with local/jurisdictional privacy policies.
- A jurisdictional clinical system with patient access is available.
- If applicable, patient has designated and authorized a designated caregiver to access their personal health record on their behalf.

Post-conditions

Scenario 1:

- Health Care Provider views and uses the clinical document(s) in support of Patient care.

Scenario 2:

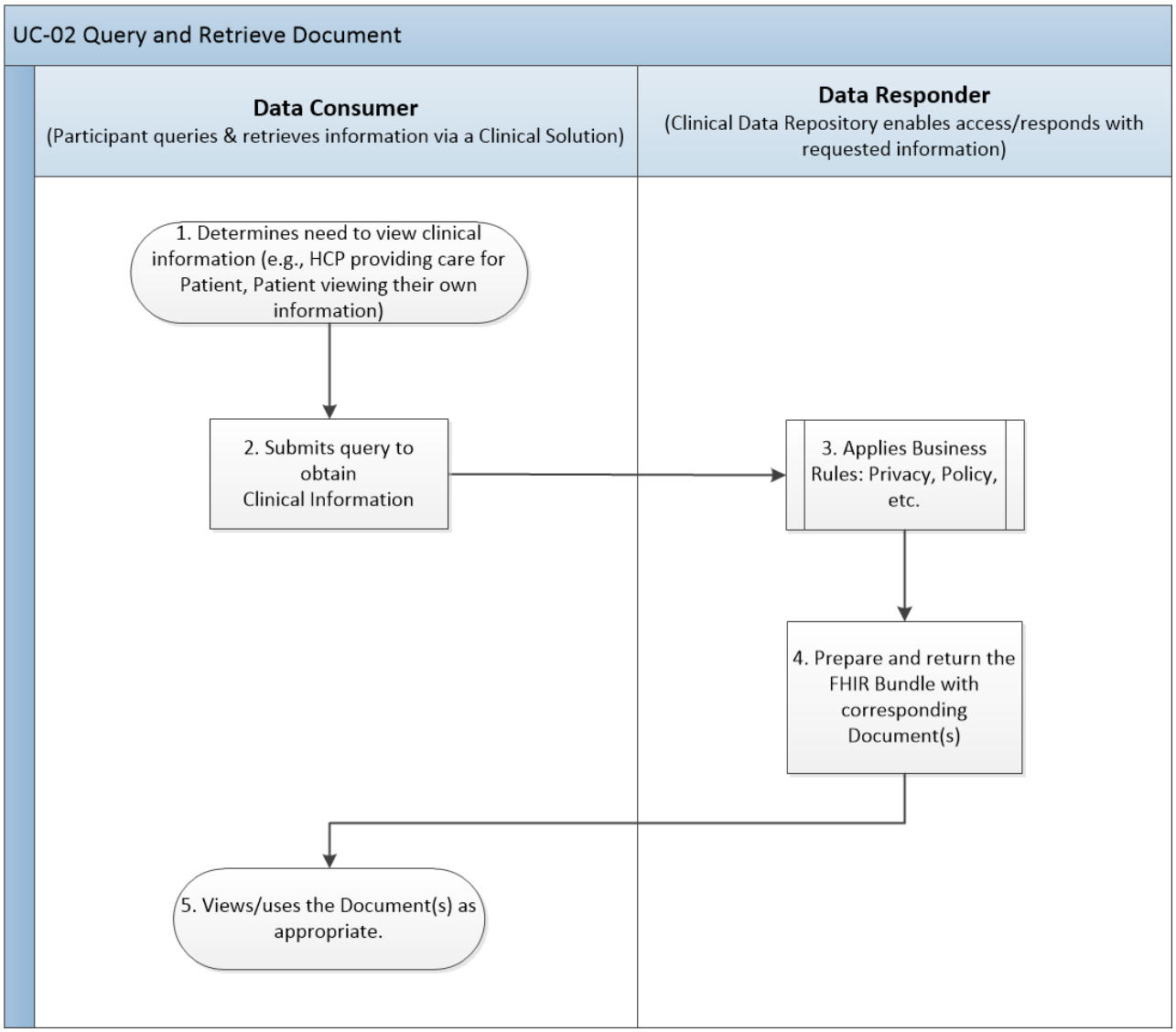
- Patient, or their designated caregiver, accessed/viewed, and optionally printed a copy of, their personal health information.
- Patient, or their designated caregiver, presents their personal health information to another health care provider to support continuity of care.

Use Case Participants & Diagram

The participants involved in this use case are:

- Data Consumer (Clinical Solution, e.g., EMR used by the Health Care Provider to request & retrieve access to clinical document(s) from the Clinical Data Repository; Patient Portal used by the Patient / Subject of Care to request & retrieve access to their clinical document(s) from the Clinical Data Repository)
- Data Responder (Health Records System acting as the Clinical Data Repository enabling access and responding with the requested clinical document(s))

This use case diagram represents the participants and their role in the use case with a high-level view of the flow of information.



Use Case - Primary Flow

The following provides a textual description corresponding to the use case diagram.

1. Participant (i.e., Health Care Provider or Patient / Subject of Care) determines need to view clinical information.
2. Participant requests access (i.e., queries) for clinical information via the clinical solution.
3. Clinical Data Repository applies applicable business/policy rules (e.g. validates requestors credentials).
4. Clinical Data Repository prepares and returns the FHIR bundle with corresponding clinical document(s).
5. Participant views/uses the clinical document(s) in support of care for the Patient or themselves.

Use Case - Alternate Flow

The following list provides possible alternate flows that may occur within this use case.

- Step 3: Patient Consent Services are not currently supported in the CA:FeX specifications. However, Patient consent is considered as a roadmap item and would be represented in a separate use case at that time where a Patient has identified consent directives requiring the Health Care Provider to address prior to

accessing the Patient's clinical information. It is recognized that some jurisdictions may have existing Patient Consent Services implemented and should be considered when implementing in that jurisdiction.

Use Case - Requirements

The following is a list of key requirements that will be addressed as part of this use case.

#	Category	Requirement Description
1	Query	FHIR API SHALL be capable of executing searches based on a Patient Identifier
2	Query	FHIR API SHALL be capable of executing searches based on a specified date range
3	Query	FHIR API SHOULD be capable of executing searches based on specific Document Type that the health care provider is interested in retrieving
4	Query	FHIR API SHALL be capable of accepting requests originating from a patient portal or any other system that allows a patient to initiate a request to access their personal health information (PHI)
5	Response	FHIR API SHALL be capable of responding to requests for retrieval of clinical information for requests initiated by patient to access their PHI

3 Exchanging Documents in FHIR

The transactions presented below represent an initial solution to the identified use cases and are expected to evolve, particularly as we hear from the implementer community and use cases are refined and added. We encourage the community to provide feedback on these emerging specifications.

3.1 Overview

HL7 characterizes a document by the following properties:

- Persistence – Documents are persistent over time. The content of the document does not change from one moment to another. A document represents information stored at a single instance in time.
- Wholeness - A document is a whole unit of information. Parts of the document may be created or edited separately, or may also be authenticated or legally authenticated, but the entire document is still to be treated as a whole unit.
- Stewardship - A document is maintained over its lifetime by a custodian, either an organization or a person entrusted with its care.
- Context - A clinical document establishes the default context for its contents.
- Potential for authentication - A clinical document is an assemblage of information that is intended to be legally authenticated.

This specification defines a document as a record (written, printed or electronic) that compiles information about a patient's care for a particular purpose or workflow. Documents are distinct from the medical data that may be included in the document as they provide an additional layer of context and metadata around how and why the pieces of medical data were compiled.

Examples of documents include discharge summaries, history & physical notes, medical imaging reports, patient summaries, and more.

Scope

This specification is starting with the exchange of documents (and their respective resources) in FHIR. As the CA:FeX Interoperability Specifications evolve, it will be expanded to tackle the exchange of individual FHIR resources that can be exchanged independent of a document workflow (e.g., retrieval of last 3 years of dispensed medications).

While HL7 FHIR defines a format for documents that are authored and assembled in FHIR (See FHIR Composition Resource), it is important to acknowledge that FHIR can be used to exchange documents that are constructed in other formats (e.g., FHIR Binary).

This specification has been developed and refined to support an initial round of implementers who will use its transactions to exchange the pan-Canadian Patient Summary (PS-CA) in the form of a FHIR Document. In choosing PS-CA as initial proving ground, this specification has been able to identify and address requirements that are expected to be extrapolated to other types of FHIR Documents.

Note: Prior versions of this specification included additional transactions (CA:FeX 2B, CA:FeX 3B) that were intended to cover interactions with Hybrid Repositories (e.g., repositories that support both native FHIR Documents and legacy Binary documents). However, these transactions have been migrated to a future release of CA:FeX as they require additional rounds of exposure and testing with implementers before being considered Trial Implementation.

The CA:FeX Interoperability Specifications will provide detailed information for the following transactions.

Transaction ID	Description
CA:FeX-1	Submit Data
CA:FeX-2	CA:FeX-2A: Search Against FHIR Assembled Documents Repository
CA:FeX-3	CA:FeX-3A: Retrieve Document From FHIR Assembled Documents Repository

3.2 FHIR Version

FHIR content in this specification is based on on FHIR Release 4 (v4.0.1).

3.3 Submit a Document

Scope

This capability is currently scoped to the ability to submit new FHIR Documents.

While there are a variety of ways documents can be modeled and exchanged in FHIR, the initial release of this specification is focused on the submission patterns used by early implementers that are expecting the PS-CA (pan-Canadian Patient Summary) to be delivered in FHIR Document form. Patient Summaries are a relatively new document type (e.g., legacy implementations not expected) and have been modeled as FHIR Documents.

FHIR Documents are Bundle resources with the `type` of `"document"` and which contain a Composition resource as the first entry, and key referenced resources as additional Bundle entries. For more on FHIR Documents, see Documents.

3.3.1 Out of Scope

As this specification evolves, and new document types and architectures are included, this scope will also evolve in subsequent releases to supply guidance for those business cases.

Global, pan-Canadian, and jurisdictional practices for document lifecycle management of patient summaries are still in development. For this reason, the management, verification, replacement and deprecation of documents, are out of scope of the guidance included in this release but have been included in the roadmap for future releases.

Note: This does not preclude or prevent early implementers from defining their document management practices and beginning to exercise them in their own specifications.

> **Info**
>
> Implementers expecting to support use cases involving multiple patient summaries over time are still expected to familiarize themselves with the boundaries the FHIR standard applies to document immutability. Once assembled into a document bundle, the document is immutable - its content can never be changed, and the document id can never be reused. Note that the document may be represented in either XML or JSON and interconverted between these or have its character encoding changed, all the while remaining the same document. However, the directly referenced content within the document and

> the presentation of the document cannot change substantially (such that it changes the clinical meaning of the content). Any additional documents derived from the same composition SHALL have a different document id. See https://www.hl7.org/fhir/documents.html#content for more details.

3.3.2 Use Cases

The following CA:FeX use case leverages this capability:

- UC-01 Create and Submit Document

3.3.3 CA:FeX Transactions

This capability describes the FHIR implementation of the CA:FeX Submit Data (CA:FeX-1) transaction found in the Sequence Diagram for UC-01: Create and Submit Document.

3.3.4 HTTP Operations

This capability can be leveraged using HTTP POST requests. Implementers are expected to familiarize themselves with how create interactions are executed using the FHIR RESTful API framework.

For more information on the supported HTTP operations, refer to the section CA:FeX Actors and Transactions.

HTTP POST

A create is executed by performing a `POST` operation in the RESTful framework:

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

Content Types and Encodings:

Either `application/fhir+json` or `application/fhir+xml` content types are permitted

3.3.5 Document Submit Patterns

The optimal document submission pattern for any given implementation is determined by a number of factors. These factors include (but are not limited to): presence/absence of XDS and XCA architecture, organizational short-term and long-term goals for FHIR, current assets and prioritized capabilities, role in the health exchange ecosystem, readiness of contributing actors to adopt FHIR, etc.

These factors will be discussed in more detail in a forthcoming FHIR Document Exchange Companion Whitepaper.

The patterns discussed below only apply to Data Recipients that are expecting Data Sources to submit documents using FHIR endpoints.

Some implementers may choose to use the data received through existing workflows and transform it into FHIR, particularly if their electronic medical record systems are not ready to exchange data in FHIR. Other implementations may allow for a FHIR Document to be created "on-demand" in response to a query - both are perfectly legitimate practices that do not require a submission endpoint. *These creation patterns will be surfaced as a separate capability in a later release.*

Direct Submissions of FHIR Document Bundle

Data Recipients that want to receive FHIR Documents from Data Sources need to at a minimum support the submission of the FHIR Document Bundle to a HTTP POST request to a `[base]/Bundle` endpoint.

This will create the new Bundle resource in a server-assigned location with a server assigned id for the Bundle resource. (*Note: this transaction pattern does not support conditional create which allows the resource to be created only if it does not already exist on the server).*

Per the FHIR standard on HTTP create interaction:

- The request body SHALL be a valid FHIR Resource *(in this case, a FHIR Release 4 Bundle resource).*
- The resource does not need to have an `id` element (this is one of the few cases where a resource exists without an `id` element). If an `id` is provided, the server SHALL ignore it.
- If the request body includes a meta, the server SHALL ignore the existing `versionId` and `lastUpdated` values. The server SHALL populate the `id`, `meta.versionId` and `meta.lastUpdated` with the new correct values.
- Servers are allowed to review and alter the other metadata values, but SHOULD refrain from doing so (see metadata description for further information).
- A server SHOULD otherwise accept the resource as submitted when it accepts the create, and return the same content when it is subsequently read. However, some systems might not be able to do this; see the note on transactional integrity for discussion.
- The server returns a `201` Created HTTP status code, and SHALL also return a `Location` header which contains the new Logical Id and Version Id of the created resource version. See Response Handling for more details.

Considerations for Document Submission Using Bundle Endpoints

Two key attributes of FHIR Documents submitted to the Bundle endpoint are (with limited exceptions):

- Self-contained—All of the primary resources used in the document must be included in the document (see Composition in the FHIR standard); other resources used in the document should also be included.
- Point-in-time—The entire document is stored under the /Bundle endpoint, and the content is not (generally) updated. If the Data Receiver actor, which supports the /Patient endpoint outside of this transaction, updates an address in a Patient resource under /Patient, a Patient resource inside a Document would not be expected to reflect that.

Submission of a FHIR Document to a Bundle endpoint is not enough on its own for this pattern to be effectively used for document lifecycle management. This pattern is seen as a "building block" that can be further augmented either through a) API interactions and operations, or through b) implementation of significant internal business logic to make determinations on document currency for example.

Note: Despite the fact that a FHIR Document may contain Composition, Patient, Practitioner or other resources, posting a FHIR Document Bundle to a Bundle Endpoint does not make those resources automatically available at their equivalent endpoints (e.g., /Composition, /Patient, /Practitioner, etc.).

> Outside of the scope of this specification's guidance, an implementation may choose to decompose a received FHIR Document, and manage the included resources individually. An implementation that does this should consider several issues, including:
>
> - Resource deduplication (e.g., when the Patient or Composition resource in a document is actually the same as an already known Patient or Composition resource, perhaps obtained from another document)

- Sources of truth for various resources and document currency (e.g., whether to update an existing patient address based on a 10-year old document)
- Whether and how updates to the extracted resources feed back into the submitted document
- Document lifecycle compared to resource lifecycle (i.e., if a Practitioner resource is removed from the system 5 years after the Practitioner retires, consider whether a FHIR Document or the Composition extracted from it is still useable, etc.)
- Whether to persist the submitted document as well as the extracted resources

3.3.6 Document Submit Patterns: Augmenting Base Capabilities & Cutting Edge Capabilities

This specification previously surfaced cutting edge capabilities (e.g., $document Operation) for the purpose of acquiring early feedback on patterns that are being considered for inclusion and testing in later releases. These capabilities have been migrated to a future release of the CA:FeX to ensure the content of the existing specification fully encapsulates the patterns and capabilities with a maturity level of Trial Implementation.

3.4 Search for a Document

3.4.1 Scope

This capability supports the ability to find documents using parameterized queries.

This capability supports the following query behavior:

- Searches that are intended to return a payload that includes any FHIR Documents that match the parameters provided. These types of queries combine search and retrieval but put more strain on the requesting system to manage and filter the volume of content in the response in a way that is more manageable to the user.

***Note**: Details on what the responder supports can be found within the CapabilityStatement that the requester retrieves as a separate step from this search. Querying for a CapabilityStatement is an expected pre-requisite for being able to query a source. However, it is not required to be conducted at the beginning of every session to avoid forcing performance costs on clients that interact with known servers that do not update their security services and/or supported capabilities frequently.*

3.4.2 Use Cases

The following CA:FeX use cases leverage this capability:

- UC-02 Query and Retrieve Document

3.4.3 CA:FeX Transactions

This capability describes the FHIR implementation of the CA:FeX Search Data (CA:FeX-2) transaction found in the Sequence Diagram for UC-02: Query and Retrieve Document.

3.4.4 HTTP Operations

This capability can be leveraged using HTTP GET requests and/or HTTP POST. Implementers are expected to familiarize themselves with how searches are executed using the FHIR RESTful API framework.

See CA:FeX Actors and Transactions for more information on the supported HTTP operations.

HTTP GET

In the simplest case, a search is executed by performing a `GET` operation in the RESTful framework:

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

HTTP POST

For this RESTful search (see definition in RESTful API), the parameters are a series of name=[value] pairs encoded in the URL or as an application/x-www-form-urlencoded submission for a POST:

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

3.4.5 Considerations for Document Search Patterns

While there is more space for variability of document submission patterns based on a number of factors (that will be discussed in more detail in a future FHIR Document Exchange Companion Whitepaper), variations in supported document search patterns incur a higher cost towards Data Consumers.

A primary driver of this specification is to fill the gap that "FHIR-first" implementers are experiencing with existing document exchange standards like MHD and XDS. See *pan-Canadian FHIR Exchange (CA:FeX) Interoperability Specifications: Preface*. One of these particular challenges, is the need to balance efficacious and consistent search patterns against the additional effort incurred to supply supplementary metadata/resources (e.g., DocumentReference) that include more potent attributes to aid in targeted searches.

Clinical systems in US markets are more familiar with using MHD-like patterns to exchange C-CDAs using FHIR - largely due to the proliferation of XDS implementations in the US Market. Many organizations that had already invested in XDS infrastructure opted to support a FHIR façade for retrieving C-CDAs and utilized MHD (and related IHE profiles) as the mechanism for doing so. Naturally, these systems are considering how to retrofit their existing configurations to support search and retrieval of other types of documents in a similar manner.

Systems that serve non-US markets (or new solutions built entirely in FHIR for document exchange) may not have the same historical context to immediately catalyze investment of effort to supply additional resources for more desirable search behaviors. Recently, new operations have been developed that are more lightweight and may ease the burden of supporting these more potent search attributes. However, these patterns are evolving and their place in the Canadian market is yet to be fully evaluated.

Note: The pattern intended for the search against FHIR Document Repositories (CA:FeX 2A) has received significantly more rounds of feedback and projectathon testing than the pattern that was socialized for implementers of Hybrid Repositories (CA:FeX 2B). CA:FeX 2B and advanced capabilities that require further implementer feedback have been migrated to a future release of the CA:FeX.

3.4.6 Document Search Patterns: CA:FeX-2A (Search Against FHIR Assembled Documents Repository)

This pattern is intended to represent the most straightforward method of searching for FHIR Documents from a repository that does not have an existing XDS/MHD architecture and has not further augmented their search capabilities.

Implementers who are trialing this pattern will either play the role of a Data Consumer or a Data Responder in an interaction where a query is constructed (using the parameters identified below) and then submitted to a `[base]/Bundle` endpoint using a HTTP `GET` or `POST` command.

This will execute a search which will return the results in the HTTP response as a searchset Bundle containing any document Bundle resources that match the criteria of the search. While the endpoint is anchored around Bundle, the expectation is that searches will use chaining on a handful of parameters under bundle.composition, to narrow the search to FHIR Documents.

Per the FHIR standard on HTTP search interaction:

- Because of the way that some user agents and proxies treat `GET` and `POST` requests, in addition to the get based search method, servers that support *search* SHALL also support a `POST` based search
- Supporting `GET` means that PHI (Personal health information) might appear in search parameters, and therefore in HTTP logs. For this reason logs should be regarded as being as sensitive as the resources themselves. This is a general requirement irrespective of the use of `GET` - see the FHIR security page for further commentary.
- If the search succeeds, the server SHALL return a 200 OK HTTP status code and the return content SHALL be a Bundle with type = `searchset` containing the results of the search as a collection of zero or more resources in a defined order.
- If the search fails (cannot be executed, not that there are no matches), the return value SHALL be a status code 4xx or 5xx with an OperationOutcome. See Response Handling.

Implementers are encouraged to review the Base FHIR Specification for further details on the HTTP search interaction.

Considerations for Document Search Using Bundle Endpoints

Anchoring searches around Bundle in this search pattern is recommended for implementers that want to retrieve all the FHIR Documents that meet their search criteria.

- Implementers that use this approach should consider using a combination of search parameters to reduce the processing load on responders and requesters.
- The result collection can be long, so servers may use paging. If they do, they SHALL use the method described here for breaking the collection into pages if appropriate.

This search pattern does not separate the act of search from retrieval. Clients that want to provide their users the ability to review high level information (lists, summaries, etc.) for matching documents to support selective retrieval of the desired FHIR Document bundles will need to utilize different search patterns or manage this behavior in the client's user interface.

> **Note**: Due to limitations in querying for discrete resources when the document is loaded as a FHIR Document bundle, performing searches against endpoints for Composition or other contained resources (e.g., using Patient resource id) will only work for repositories that a) decompose the resources within the submitted bundles, or b) enable the submission of the contents of the document at their individual endpoints or through a transaction bundle so that they might be retrievable. This approach requires significant caution - implementers should be well versed in the Document Handling Obligations before considering either approach. Guidance on both mechanisms is outside the scope of this specification.

Supported Search Parameters for Document Search Using Bundle Endpoints

The following search parameters are used generically to support document retrieval anchored around the Bundle endpoint. *These will continue to evolve as new use cases and requirements are identified.*

Additional search parameters that are specific to the requirements for a particular use case or IGuide may be further defined by those implementations. See *Option 2 - FHIR Health Information Exchange (HIE) Pattern Using CA:FeX* in the pan-Canadian Patient Summary (PS-CA) Specification for details and examples of which of the parameters below are used to retrieve patient summaries.

Query Search Parameters	Applied to	Description
timestamp	bundle.timestamp	This parameter, of type date, specifies the timestamp when the FHIR bundle was created. See FHIR http://hl7.org/fhir/R4/search.html#date for use of the date search type.
patient.identifier	bundle.composition.patient.identifier	This parameter, of type token, specifies an identifier associated with the patient to which the document is assigned. This use of patient.identifier follows the FHIR Chaining Parameters search methodology.
type	bundle.composition.type	This parameter, of type token, specifies the kind of document (LOINC if possible). The use of bundle.composition.type follows the FHIR Chaining Parameters search methodology.
status	bundle.composition.status	This parameter, of type token, specifies the status of the composition. The use of bundle.composition.status follows the FHIR Chaining Parameters search methodology.
author	bundle.composition.author	This parameter, of type reference, specifies who and/or what authored the document. The use of bundle.composition.author follows the FHIR Chaining Parameters search methodology.
date	bundle.composition.date	This parameter, of type date, specifies when this document reference was created. The use of bundle.composition.date follows the FHIR Chaining Parameters search methodology.

There are additional parameters that can be provided in the request that help further order and organize the resources that are returned. These types of parameters are identified in the base specification as standard parameters and result parameters.

CA:FeX does not currently require the support of certain result parameters, since conformance expectations for these types of parameters are implementation-specific and/or conditionally useful (e.g., _count parameter when an implementation expects a high volume of documents could be returned).

3.5 Retrieve a Document

Scope

This capability supports the ability to retrieve known documents using the document's resource id.

3.5.1 Use Cases

The following CA:FeX use cases leverage this capability:

- UC-02 Query and Retrieve Document

3.5.2 CA:FeX Transactions

This capability describes the FHIR implementation of the CA:FeX Retrieve Data (CA:FeX-3) transaction found in the Sequence Diagram for UC:02: Query and Retrieve Document.

3.5.3 HTTP Operations

This capability can be leveraged using HTTP GET requests. Implementers are expected to familiarize themselves with how searches are executed using the FHIR RESTful API framework.

See CA:FeX Actors and Transactions for more information on the supported HTTP operations.

HTTP GET

In the simplest case, a retrieve is executed by performing a `GET` operation in the RESTful framework:

```
GET [base]/[resourcetype]/id
```

3.5.4 Considerations for Document Retrieve Patterns

This pattern is predicated on the requestor knowing the id of the resource they are attempting to retrieve.

Depending on the maturity and scope of the repository, the endpoints supported may be isolated to `[base]/Bundle` but the repository could potentially support additional document formats which would be retrieved from different endpoints.

Guidance is provided below for early adopters of CA:FeX that will support the ability to retrieve FHIR Documents directly from a FHIR Assembled Documents Repository.

Note: The pattern intended for the retrieve from a FHIR Document Repository (CA:FeX 3A) has received significantly more rounds of feedback and projectathon testing than the pattern that was socialized for implementers retrieving documents from Hybrid Repositories (CA:FeX 3B). CA:FeX 3B has been migrated to a future release of the CA:FeX.

3.5.5 Document Retrieve Patterns

CA:FeX-3A (Retrieve Document From FHIR Assembled Documents Repository)

The most straightforward method to retrieve a FHIR Document is to perform a read interaction using HTTP `GET` [base]/[type]/[resource id] against a `[base]/Bundle` endpoint.

Per the FHIR Standard on the HTTP read interaction:

- This returns a single instance with the content specified for the resource type.
- This URL may be accessed by a browser.
- The possible values for the Logical Id ("id") itself are described in the id type.
- The returned resource SHALL have an `id` element with a value that is the `[id]`.

Considerations for Document Retrieve Using Bundle Endpoints

Anchoring retrievals around a Bundle endpoint in this retrieval pattern is recommended for implementers that want to retrieve the FHIR Document using the known id for the Bundle. This retrieval pattern is expected to be used by implementers re-retrieving a Bundle that was previously identified in a search/or prior retrieval.

3.5.6 Document Retrieve Patterns: Supported Retrieval Parameters

The following examples are used to retrieve documents based on a known resource ID.

GET [base]/Bundle/[id]

3.6 Response Handling

3.6.1 HTTP Status Codes

The HTTP status codes returned in the response aid applications in understanding whether a search was successful, and if not successful, provides some context as to why the search did not return the expected response.

These status codes are considered the base status codes that should be present in any implementing API. Implementations and guides may include additional status codes that their service supports and may supply further details on the circumstances or expected client behavior.

Error

If the search fails (cannot be executed, not that there are no matches), the return value return value SHALL be a status code 4xx (client error) or 5xx (API/service error). An OperationOutcome SHOULD be returned detailing the error.

Scenario	HTTP Status Code	Outcome
The request is performed with incorrect syntax or against a resource or search parameter that the API does not currently support.	HTTP 400 Bad Request	Error code is returned in the response with an OperationOutcome detailing the error
The request is performed by an application that has not properly authenticated.	HTTP 401 Unauthorized	Error code is returned in the response with an OperationOutcome detailing the error

Scenario	HTTP Status Code	Outcome
The request is performed by an authenticated user, but the authenticated user is not permitted to perform the requested operation.	HTTP 403 Forbidden	Error code is returned in the response with an OperationOutcome detailing the error
The request is performed on a resource type that is not supported	HTTP 404 Not Found	Error code is returned in the response with an OperationOutcome detailing the error
The request is performed using an HTTP method that the server does not support for the resource.	HTTP 405 Method Not Allowed	Error code is returned in the response with an OperationOutcome detailing the error
The request includes a media type which is not supported. For example, the client uploads an image as image/svg+xml, but the server requires that images use a different format.	415 Unsupported Media Type	Error code is returned in the response with an OperationOutcome detailing the error
The request is performed but the server encountered an internal error during the process of the response message.	500 Internal Server Error	Error code is returned in the response with an OperationOutcome detailing the error
The request is made when the service is temporarily unavailable.	503 Service Unavailable	Error code is returned in the response with an OperationOutcome detailing the error
The request is performed but the server, while acting as a gateway or proxy, does not get a response in time from an upstream server in order to complete the request.	504 Gateway Timeout	Error code is returned in the response with an OperationOutcome detailing the error

Success

If the search is properly formatted and succeeds, the API SHALL return an `HTTP 200 OK` status code and the return content SHALL be a Bundle with type = searchset containing the results of the search as a collection of zero* or more resources in a defined order.

NOTE: Searches that are properly performed but have no PHI to return will still result in a `HTTP 200 OK` *status code*

Scenario	HTTP Status Code	Outcome
The request is performed with correct syntax and there are FHIR resources available that match those search parameters	HTTP 200 OK	Success code is returned in the response, Bundle returned in the response contains entries with requested FHIR resources

Scenario	HTTP Status Code	Outcome
The request is successful and a FHIR resource has been created on the server	HTTP 201 Created	Success code is returned in the response, the location of the resource is returned in the location header of the response

3.6.2 Operation Outcome

OperationOutcome is used to provide more detailed description of any issues that occurred during execution of an operation. The general conventions for OperationOutcome are:

- OperationOutcome can either be the sole response to an operation (generally accompanying an HTTP code that indicates a failure) or it can be part of a Bundle indicating potential warnings associated with the generation of the search response.
- If an OperationOutcome is returned with anything other than a success (200), the issues it contains will be of type 'error' or 'fatal'. Fatal is used for issues that occur before the query can be exercised, 'error' is used for issues that occur during query execution.
- OperationOutcomes returned as part of a Bundle will only contain 'warning' and 'information' messages. The user should always be made aware of the existence of these messages and the user should have the opportunity to review all such messages.
- The OperationOutcome.issue.code provides a standardized description of the issue. Systems MAY create logic based on the specific code returned.
- The details of the issue or warning will be found in issue.details.text. This content should always be displayed to the user.
- The issue.details.coding values, issue.diagnostics and issue.location are intended for diagnostic purposes and will generally only be relevant to help-desk personnel. It may be appropriate to make access to this information available only by clicking on a button rather than displaying information to the user that may be confusing.
- issue.location will only occur if the problem is with a submitted FHIR instance (i.e. it will not be present if the issue is for query parameters, HTTP headers, etc.). It will be expressed as an XPath regardless of whether the submitted content is XML or JSON.