*An **InterSystems** Cloud Offering Guide*

InterSystems HealthShare

One Memorial Drive, Cambridge, MA 02142, USA
Tel: +1.617.621.0600 | Fax: +1.617.494.1631
http://www.intersystems.com

FHIR Transformation Service

Offering Specification

February 2022

Table of Contents

Introduction to FHIR Transformation Service

What is FHIR Transformation Service (FTS)?

FHIR Transformation Service (FTS) is a cloud service to translate HL7 v2 and CCDA to FHIR. It is a "solution as a service" offering delivered and managed by InterSystems. We built this system for customers who have HL7 v2 messages and/or CCDA documents and want to transform them into FHIR Bundles. These FHIR bundles can be transmitted to other systems or stored in a FHIR Server. You can efficiently operate on data from different sources and disparate data exchange standards by using FTS. The services are built on the core capabilities of InterSystems IRIS for Health for seamless conversion and delivery of healthcare data and cloud services. Current cloud providers include Amazon Web Services (AWS).

What is included in FHIR Transformation Service?

FHIR Transformation Service is a complete package that includes:

- Access to FTS input and output configuration
- All cloud resources needed to run FTS in a dedicated Virtual Private Cloud (VPC)
- Ongoing maintenance of FTS
- Customer-specific configuration and implementation services to bring the solution to live operations, if required
- 24/7 monitoring of FTS, including real-time monitoring
- Sophisticated security and data protection controls
- Error reporting
- Auto-scaling

Who is the InterSystems Cloud Delivery team?

FHIR Transformation Service is delivered by the InterSystems Cloud Delivery team, which is staffed with experienced technical professionals with extensive backgrounds in the design, configuration, and management of:

- InterSystems IRIS for Health Operations
- Cloud Networking
- Cloud Platforms
- Cloud Storage
- Cloud System Security
- Cloud Operations
- Service Desk Operation
- Monitoring and Alerting
- Business Continuity
- Containerization

Who does configuration / implementation?

FTS implementation is fast and simple. Customers are able to implement and configure this service in a few minutes. InterSystems built implementation automation to assist customers to configure the input and output resources. InterSystems recommends one interface per message/document source as every source usually have slight differences that influence the final results. InterSystems Professional Services can be separately leveraged to help perform data profiling/mapping to fine tune the results of the FHIR bundle as part of a separate Statement of Work or Contract Change Request.

How does InterSystems deliver FHIR Transformation Service?

FHIR Transformation service is implemented in each cloud provider as a container-based solution with automatic failover between availability zones within a given region. Currently, FTS supports transformations of HL7 v2 messages and CCDA documents (detailed information in the table below) with three types of FHIR Bundles: Transaction, Message, and Document. Additionally, extensive monitoring and alerting are configured to permit the customer to ensure that services for the offering are available and performing at the level required for efficient operation, and that any incidents are detected and addressed. Data availability, integrity, and data security are achieved using redundant infrastructure, data encryption, dual availability zone deployment, vulnerability scanning, regular updates to the FTS, and ongoing auditing. Data only exists during the processing time. No PHI is stored to guarantee confidentiality.

HL7 v2 to FHIR transformation

FHIR Transformation Services currently supports most of the HL7 v2 message types relevant to FHIR resources. We are continuously expanding our support. The table below presents the current supported message types.

Message Type	Message Type Description
A01	Admit/Visit notification
A02	Patient transfer
A03	Discharge
A04	Register patient
A05	Pre-Admit patient
A06	Change Outpatient to Inpatient
A07	Change Inpatient to Outpatient
A08	Update Patient Info
A09	Patient Departing
A10	Patient Arriving

A11	Cancel Admit
A12	Cancel Transfer
A13	Cancel Discharge
A16	Pending Discharge
A17	Swap Patients (Beds)
A23	Delete Patient
A25	Cancel Pending Discharge
A27	Cancel Pending Admit
A28	Add Person or Pt Info
A31	Update Person Info

CCDA to FHIR Transformation

CCDA Sections Supported

Admission Diagnosis	Functional Status	Plan Of Treatment
Allergies	Goals	Problems
Assessment	Health Concerns	Procedures
Care Teams	Immunizations	Reason For Visit
Discharge Diagnosis	Insurances	Resolved Problems
Discharge Medications	Medical Equipment	Results
Encounters	Medications	Social History
Family History	Medications Administered	Vital Signs

Cloud Service Provider and Resources

Customers can deploy FHIR Transformation Service on supported cloud provider environments. Currently, FTS is available on AWS.

For AWS, FTS is deployed across availability zones in the region of your choice. Each customer is allocated a dedicated VPC for complete isolation from other customers. Multiple regions are available to support the closest proximity to your organization for the lowest possible network latency.

Highly Available and Secure Network Connectivity

- Automatically recover unhealthy containers to ensure that you have the desired amount of processing power supporting your workload.
- Customers define the security policy of their S3 buckets and have complete control of the inbound and outbound access. InterSystems provides sample security polices to expedite implementation.
- Network-based separation via VPCs to ensure isolation
- Security and networking monitoring and management of all access consistent with the solutions available in the cloud provider environment

Data Encryption

Data is encrypted in transit to/from FHIR Transformation Service. This is accomplished using combinations of standard encryption methods and may include the following:

- SSL/TLS encrypted communication
- InterSystems product encryption technologies
- SFTP File Transfers
- S3 object transfer

Data is encrypted in transit from participant sites to the VPC, as well as in communication between availability zones when appropriate.

Cloud Resource Provisioning Consistency and Security

Compatible cloud resource types (e.g., networking, ECS services) and any required supporting third-party software are deployed in all instances to ensure reliable service delivery in primary operation.

Software Deployed

- InterSystems FHIR Transformation Service
- Customer systems deployed on Linux -based containers
- Enterprise-grade management tools, such as Splunk
- Monitoring via cloud provider monitoring tools, such as AWS CloudWatch, CloudTrail, Splunk alerting, , custom scripts, and InterSystems built-in product monitoring capabilities
- Web servers: Apache HTTPD
- Version control: Monitored and maintained primarily through the use of cloud provider monitoring tools, such as CloudWatch, CloudTrail, and internally written scripts
- Configuration maintained using CloudFormation, as well as custom applications and scripts

Decommissioning

When the customer wants to decommission a FHIR Transformation Service environment, the relevant cloud resources that InterSystems deployed for the environment will be deleted and destroyed when the customer selects the option to delete the identified environment. The processes used by the cloud delivery system ensure that all the resources deployed are removed, and any encryption keys for deployed instances of the environment are destroyed. Because all cloud deployment obligatorily uses encrypted storage, the destruction of the relevant encryption keys for the environment is consistent with the processes for Cryptographic Erase under NIST SP 800-88, Guideline for Media Sanitation.

InterSystems may retain non-PHI aggregated data (such as the count of processed messages by type) for the billing purposes.

Change Control

For FHIR Transformation Service, all changes to the offering are tracked to allow failback to any prior state. The InterSystems Cloud Delivery team uses tested change procedures, coupled with Git based workflow. A separate Git based workflow project can be made available to the customer to assist with change control for interface development and operations by the customer.

At the time of any FHIR Transformation Service upgrade, the update is tested by InterSystems in a different environment, limited to operational tasks related to FTS. Customers will get notice of a change that may affect a transformation.

Monitoring and Alerting

The FTS environment is extensively and constantly monitored by the InterSystems Cloud Delivery team. Monitoring tools, such as CloudWatch, CloudTrial and Splunk (depending on cloud providers and region) are employed to monitor:

- Availability
- Environment consistency
- Incident occurrences
- Abnormal activity
- Vulnerabilities
- Message volume

The InterSystems Cloud Delivery team is alerted to any issues and any critical alerts result in an immediate notification. The monitoring information is tracked and used to troubleshoot issues, as well as for information to be used for capacity planning. Any incident that results in a service interruption to the client is reported to the client.

Customers are responsible for monitoring their message errors, message volume, and their S3 buckets.

Message Volume is used for the billing process. We count the inbound messages for each deployment available in the customer’s tenant. A report is available for customers to verify their message volume at any time on the InterSystems Cloud Service Portal under Deployment>Metrics. The count is separated by deployment and is updated every hour.

Incident Management/Change Management/Configuration Management/Support

The Incident Management, Change Management, and Configuration Management processes are all focused on communication via the InterSystems iService internal tracking system. This application is used to initiate and track all aspects of customer communication with the InterSystems Cloud Delivery team. Incident management, change management, and service requests from the customer will all be tracked in the iService application. All Support requests are also entered and tracked in the iService application.

General Operations

The InterSystems Cloud Delivery team provides all the standard tasks expected with the operation of a cloud-based platform offering. The following table shows some specific items that may be of interest.

Task	Schedule	Notes
Software Maintenance	As needed	Dictated by security or operational stability
Container Log Audit Review	Daily/Weekly	Automated reviews daily, weekly manual
Account audits to validate ongoing access requirement	Quarterly	List of active users on InterSystems Cloud Delivery Portal with access accounts sent to client for review/audit
Vulnerability Scanning	Weekly	Credentialed internal and non-credentialed external
Monitoring	Ongoing	CloudWatch, CloudTrial and Splunk are used to monitor network, CPU, server memory, various error log conditions, participant feed statistics, existence of expected participant file uploads, various other services, devices, and states.
Incident Reporting	As needed	Clients are informed of any incident that results in an outage of a production service. A formal incident report is sent to the client within 5 business days of resolution, including root cause analysis.
Regular Maintenance	Weekly	All Maintenance tasks are scheduled every Tuesday from 8:00 pm to 10:00 pm Eastern Time (US).

What are the customer responsibilities?

While FHIR Transformation Service is extremely comprehensive, there are some customer responsibilities:

- Establishing connectivity from the customer’s S3 bucket to the FTS is a self-service model.
- Configuration of deployments
- Maintenance, monitoring, and management of the S3 bucket
- Integration testing following patches or upgrades

Standard InterSystems Cloud Components

Behind the scenes, FHIR Transformation Service makes use of a wide variety of InterSystems Cloud components, including:

Availability Management	Event Management
Capacity Management	Incident Management
Change Management	Operations Management
Configuration Management	Service Desk
Security Management	

The following sections detail these standard components.

Availability Management

- SLA commitment of 99.9% availability for cloud infrastructure and customer Deployment Environment.
- Use of multiple containers in parallel on demand to guarantee performance and high availability
- Provisioning infrastructure for customers' environments.
- Continuous monitoring of infrastructure to detect and proactively correct potential problems.
- Continuous monitoring of customer's deployments and Environment to detect and deliver alerts of potential incidents.
- Continuous monitoring of customer environments and systems to deliver alerts about sufficient capacity and performance to meet expected workloads.
- Standard delivery of customer environments with dedicated VPC and dedicated container cluster.
- Maintenance to the customer environments in the form of patches or FHIR Transformation Service updates will be delivered with the least disruption to the delivery of customer services during a weekly maintenance window. Some maintenance will require downtime and will be performed on a standard schedule – customers will receive notification of an adequate window of time during which to perform testing in each environment before upgrades are promoted to the next environment.

Capacity Management

- Regular review of resource usage and trends
- Allocation of additional resources if deemed necessary by the InterSystems Cloud Delivery team
- Continuous monitoring of InterSystems Cloud performance indicators to proactively identify and correct potential shortfalls

Change Management

- Application of standard change process for FTS that ensures appropriate authorization, review, testing, and failback in place
- Application of automation tools to ensure consistent delivery and tracking of changes

- Version control for operational scripts and configurations

Configuration Management

- Cloud resource provisioning using configuration management tools to limit the risk of user errors
- Peer review of configuration changes prior to deployment
- Continuous monitoring to ensure that tracked components are configured as deployed
- Customer environments delivered by the InterSystems Cloud Delivery team standardized deployments
- Customer environments monitored to provide alerting to ensure ongoing compliance with installation standards

Security Management

Security requirements for deployment and operation of FTS are provided in the InterSystems Cloud Privacy & Security Requirements addendum at https://www.intersystems.com/ICPSS. As part of FHIR Transformation Service, InterSystems will:

- Configure and maintain administrative access to the cloud environments and resources
- Configure and maintain firewalls to provide only required services and communications
- Provide access to the customer portal on an as-required basis
- Encrypt using at a minimum of 256 bits keys all customer data in flight between cloud boundaries and external connections

Event Management

- Continuous monitoring of infrastructure and customer deployments.
- Collection of monitoring data to assist with operational activities (CPU utilization, data throughput, network utilization.)
- Configuration of alerts appropriate to the monitored system or service (health of containers, number of containers running, number of tasks running, etc.)
- Incident detection via monitoring of infrastructure and customer non--production environments that generates a business hour service desk ticket for the InterSystems Cloud Delivery team response
- Incident detection via monitoring of infrastructure or customer Production Environment that generates an urgent service desk ticket for the InterSystems Cloud Delivery team response within 30 minutes
- Detection of hardware or other operational problems that do not impact the delivery of customer services and are not considered customer incidents
- Alert generation via email for detected non-incident events to inform the InterSystems Cloud staff

Incident Management

- Restoration of service to infrastructure and customer Production Environment incidents as quickly as possible after detection
- Delivery of Incident report with root cause analysis to customer within five business days of incident resolution
- Creation of a Problem ticket in service desk application if problem identified during incident root cause analysis
- Maintenance and application of standard incident management policy
- Communication and documentation of incidents in service desk application
- Calculation of incident-related outages for reporting

Operations Management

- Provide segregated customer VPC to ensure that no customer has ability to access another customer environment
- Perform weekly automated vulnerability scans using tools that are regularly updated with vulnerability signatures
- Engage an independent party to perform a vulnerability assessment at least once annually
- Respond to all security-related incidents with highest urgency

Service Desk

- Availability 24/7/365 for customer access via phone, email, and web
- Availability of a single point of contact 24/7/365 to the Worldwide Response Center (WRC) through iService
- Monitoring of phone, email, and web contacts by WRC staff
- Entry into iService of all customer contacts that will be communicating with InterSystems
- Designating customer contacts with special roles (Administrative Contact, Maintenance Contact, Report Contact, etc.) in the support application
- Managing escalation with the WRC as single point of contact
- Responding to service desk requests within 30 minutes of contact during standard business hours for routine requests and incidents in non-production environments