

Health Claims Data Exchange - Domain Specifications

Domain data specifications and business policies to implement health claims data exchange

Objectives of the document

This document builds further from [Health Claims Data Exchange - Open Specifications](#) and focuses on **business specifications** needed to realise the health claims data exchange - Domain Data specifications and domain policies.

Details of Open Protocol and TechOps policies are covered in a separate document [here](#).

Domain Data Specifications

The most significant aspect of domain specification would be agreement on formats of data being exchanged and terminologies (taxonomies) being used in those data models. These would mainly include:

1. **Domain data model** - Schema definition of domain entities like Claims, Providers, Payors, Policies etc. Please note that based on available DSLs some of these data models may be flexible, e.g. policy schema if Policy Markup Language (PML) is available.
2. **Metadata specifications** - Metadata is data about data, data associated with an object, a document, or a dataset for purposes of description, administration, technical functionality and preservation. For the context of claims, this would mainly involve coding systems and suggested values for key claim attributes like disease codes, procedure codes, diagnostic codes, billing related codes (e.g. room rent, ICU charges etc.) etc.
3. **Domain Specific Language(s)** - Usually known as DSL, these may be developed When the attributes of the entity are variable from use case to use case but need to adhere to some common constraints/characteristics like types of data element it can contain, the relationship between two data elements, number of occurrences of data elements, etc. Examples of such entities within a claims data exchange would be policies, bills, contracts. In such cases, defining a markup language (DSL) rather than the entity itself allows needed flexibility to the ecosystem to innovate on such entities. These can be thought of like HTML, where multiple flavours of web pages can be defined using the markup elements.

In order to achieve this, in line with the key design principles detailed in [Health Claims Data Exchange - Open Specifications](#), following key design guidelines are proposed:

Key design considerations

1. Data specifications should be broken down to simpler fundamental units as far as possible.
2. In order to leverage existing knowledge and resources and provide wider interoperability, data specifications should extend/ reuse/ adopt international/ national models wherever available/applicable. In order to follow this in claims context, data specification should leverage resources as follows:
 - Leverage HL7/FHIR R4 specifications wherever possible
 - Leverage NRCES FHIR specifications where base FHIR specs need contextualisation to the Indian context
 - Create minimal extensions needed in case both base FHIR and NRCES specs are not enough to support the use case
 - FHIR Document profiles appropriate for the protocol should be created composed of base FHIR resources
3. Data specifications should be created with the principle of minimalism and inclusivity. In order to achieve this:
 - Specs should permissive cardinalities as much as possible. E.g. they should require minimal mandatory fields to enable maximal inclusion. As a thumb rule, wherever unsure of the cardinality of an attribute, the most permissible one should be used.
 - Specs should use permissive terminologies/code binding strength as much as possible. E.g. in the [FHIR terminology construct](#) (Section 4.1.5), if there's a conflict in choosing between "extensible" and "preferred" strengths for a coding system, "preferred" should be chosen.
4. Data specifications should be extensible i.e. they should allow a way to capture extra information that was not initially included during the model design. To achieve this:
 - It may provide a simple map of key-value pairs. Future versions of the data model may choose to create mandatory/optional names attributes in the data models after researching the wider applicability of such fields.
 - Data specifications should allow for namespacing in field names to indicate the source/reason/category of the extended fields.
5. It is recommended that all timestamps be captured in ISO-8601 format e.g. 2020-08-15T17:02:53.495+05:30. APIs may define display format property to indicate the human readable format most suitable for display.

Based on the above priorities and design considerations, key domain specifications included in phase 1 are:

Domain Data Models

The domain data model comprises the electronic claim (eclaim) objects (eObjects, in short) that are designed to capture the required information essential for processing a health claim transaction. The eclaim objects, being machine readable, facilitate the flow of data exchange between different systems and data processing in health claim transactions without the need for human intervention.

This version of the document defines the domain model specifications required for the following eclaim objects:

- Coverage Eligibility Request and Coverage Eligibility Response
- Claim Request and Claim Response: These objects will be used for both Pre-Authorization and Claim use cases (and for Pre-Determination also in future).
- Payment Notice and Payment Reconciliation

As mentioned in the design considerations above, the eclaim objects leverage HL7/FHIR4 specification and extend it, wherever required.

Guidelines for eObjects

1. Bundle Structure

- All eclaim objects will be modelled as FHIR bundles of type "document", with "bundle.composition.type" specifying the type of bundle.
- The first resource in the bundle shall be a "Composition" resource followed by a series of other resources referenced from the "Composition" resource. The elements "type", "category" and "section" in the "Composition" shall be used to define the purpose and set the context of the document.
- Example: the data packet for a coverage eligibility check request will be a bundle with "bundle.composition.type" as "Coverage Eligibility Check" and the bundle will have a "CoverageEligibilityRequest" FHIR resource embedded in it.

- CoverageEligibilityRequest Document
 - type = "document"
 - composition
 - type = "Coverage Eligibility Check Bundle"
 - section : cardinality (1..1)
 - code = "Coverage Eligibility Request"
 - entry : cardinality (1..1)
 - reference : "CoverageEligibilityRequest"
 - CoverageEligibilityRequest FHIR resource
 - Patient FHIR resource
 - Coverage FHIR resource
 - Any other resources referenced in the CoverageEligibilityRequest resource

2. Identifiers:

- For any resources requiring identifiers (e.g. Patient.identifier), naming systems have to be defined and agreed upon within the affinity domain to be specified in the "identifier.system" element to namespace the identifier value. This can allow an entity or resource to be referenced against system specific identifiers. For example, a patient may be referenced as:

```
{  
  "resourceType": "Patient",  
}
```

```

"identifier": [
  {
    "system": "https://ndhm.gov.in/patients",
    "value": "hinapatel@ndhm"
  },
  {
    "system": "https://pmjay.gov.in/beneficiaries",
    "value": "QWRT23456"
  }
]
}

```

- b. For some identifiers, “identifier.type” can be used to provide additional information.
- c. “identifier.use” can be used to indicate what/where/how a particular identifier might be used for.
- d. Example:

```

{
  "type": { // type of identifier
    "coding": [
      {
        "system": "http://terminology.hl7.org/CodeSystem/v2-0203",
        "code": "EI",
        "display": "Employee Number"
      }
    ]
  },
  "system": "https://esi.karnataka.org/employees", // naming system
  "value": "BEN-ID-1001"
}

```

3. Resources

- a. For external entities like patients, organisations, practitioners, etc, a reference alone is enough unless additional information is required to be passed. For example, patient address & other demographics.

4. Domain Header

- a. All eObjects shall be encrypted and sent in the API request body and cannot be accessed by the HCX gateways. However, there is a provision in the API request body for providers and payers to share certain information about the eObjects with the HCX gateway. This information can be sent in the domain_header part of the request body (as key-value pairs) which can be accessed and stored by HCX gateways for auditing and reporting purposes. Each eObject shall define the domain header values that are to be sent in the API request body.

5. Search Object

- a. In addition to the workflow APIs for claim processing workflows, HCX also defines APIs for searching eObjects. To support the search APIs, all eObjects should define the search request objects.

eObjects

The definitions for the current scope of objects are present in this [document](#). The structure of this document is as follows:

- **General Comments:** List of comments/guidelines applicable to all eObjects.
- **Description of eObjects:** Human readable description of eObjects. There is one sheet for each eObject and the sheet contains comments/questions from the domain and tech groups.
- **FHIR Profile definition of objects:** Differential view of HCX specific FHIR profiles.
- **ValueSets:** List of terminology bindings that need to be created or extended by HCX. HCX can extend this by creating custom value sets or mapping to an already existing value set published by others.
- **Naming Systems:** List of suggested naming systems to namespace the identifiers of different entities. This list has to be made extensive and institutionalised

The eObjects document shall be used for sharing thoughts and discussing the eObject definitions by the domain working group and the technology group. After a consensus is reached on the definitions, HCX will publish an integration guide that the ecosystem can use to create, manage and use the eObjects.

Coverage Eligibility Request

As per the design considerations and guidelines listed above, the coverage eligibility request payload has to be created as an FHIR document bundle. The bundle should have the following resources:

Resource	Description
Composition	type: should be a code representing Coverage Eligibility Request document type. section: The document shall have one section with a single entry having reference to CoverageEligibilityRequest resource.
	Structure Definition of Coverage Eligibility Request document
CoverageEligibility Request	The document must contain a CoverageEligibilityRequest resource
	FHIR Profile details: " CoverageEligibilityRequest FHIR Profile " sheet. Structure Definition of CoverageEligibilityRequest
Patient	The document should contain a Patient resource with minimal required information about the patient (refer to rows #38-42 in the " Coverage eligibility check " sheet).
	FHIR Profile details: 1. Patient resources should mandatorily have an NDHM identifier.

	2. Patient resources can also have a hospital Id (Medical record number). 3. Patient resources can also have an insurance id (PMJAY ID). 4. Patient resources can also have employee IDs and other business identifiers.
	Structure Definition of Patient
Coverage	The document should contain one or more Coverage resources with minimal information of the policy about which the information is requested (refer to row#30 in the " Coverage eligibility check " sheet).
	FHIR Profile details: <ul style="list-style-type: none"> Coverage resources should mandatorily have an identifier for the policy ID issued by the insurer.
	Structure Definition of Coverage

Domain Headers:

Key	Description

Coverage Eligibility Response

Resource	Description
Composition	type: should be a code representing Coverage Eligibility Response document type. section: The document shall have one section with a single entry having reference to CoverageEligibilityResponse resource.
	Structure Definition of Coverage Eligibility Response document
CoverageEligibility Response	The document must contain a CoverageEligibilityResponse resource
	FHIR Profile details: " CoverageEligibilityResponse FHIR Profile " sheet.
	Structure Definition of CoverageEligibilityResponse
Coverage	The document should contain one or more Coverage resources with minimal information of the policy about which the information is being returned.

	FHIR Profile details: <ul style="list-style-type: none"> Coverage resources should mandatorily have an identifier for the policy ID issued by the insurer.
	Structure Definition of Coverage

Domain Headers:

Key	Description

Claim Request

Claim object is used by providers to submit pre-authorization and claim requests to the payers. The same eObject can be used for both these use cases and the usage can be differentiated by the value of “claim.use” element. The value of this element should be set as “**preauthorization**” for Pre-Authorization requests and as “**claim**” for Claim requests.

Resource	Description
Composition	type: should be a code representing Claim Request document type. section: The document shall have one section with multiple entries having references to Claim and Signature resources.
	Structure Definition of Claim Request document
Claim	The document must contain a Claim resource
	FHIR Profile details: “ Claim FHIR Profile ” sheet.
	Structure Definition of Claim
Coverage	The document should contain one or more Coverage resources with minimal information on the policy about which the information is being returned.
	FHIR Profile details: <ul style="list-style-type: none"> Coverage resources should mandatorily have an identifier for the policy ID issued by the insurer.
	Structure Definition of Coverage
Encounter	Details of the Encounters during which this Claim was created or to which the creation of this Claim is associated.
Condition	Details of the health conditions relevant to this Claim request.

Signature resources	List of signatures by Hospital, Doctor and Patient associated with this Claim request.
---------------------	--

Domain Headers:

Key	Description
usage	“preauthorization” or “claim”, to indicate the use case this eObject is being used for.

Claim Response

ClaimResponse object is used by payers to send the response for pre-authorization and claim requests to the providers. The same eObject can be used for both these use cases and the usage can be differentiated by the value of “ClaimResponse.use” element. The value of this element should be set as “**preauthorization**” for Pre-Authorization responses and as “**claim**” for Claim responses.

Resource	Description
Composition	type: should be a code representing Claim Response document type. section: The document shall have one section with a single entry having reference to ClaimResponse resource.
	Structure Definition of Claim Response document
ClaimResponse	The document must contain a ClaimResponse resource
	FHIR Profile details: “ ClaimResponse FHIR Profile ” sheet.
	Structure Definition of ClaimResponse

Domain Headers:

Key	Description
usage	“preauthorization” or “claim”, to indicate the use case this eObject is being used for.

Payment Notice

Resource	Description
Composition	type: should be a code representing Payment Notice document type. section: The document shall have one section with a single entry having reference to PaymentNotice resource.
	TODO: Structure Definition of Coverage Eligibility Response document
PaymentNotice	The document must contain a PaymentNotice resource
	FHIR Profile details: " PaymentNotice FHIR Profile " sheet.
	Structure Definition of PaymentNotice
PaymentReconciliation	The document should contain a PaymentReconciliation resource with information about the payment related to this payment notice.
	FHIR Profile details: " PaymentReconciliation FHIR Profile " sheet.
	TODO: Structure Definition of PaymentReconciliation

Domain Headers:

Key	Description

Implementation Guide (IG)

To assist implementers in the ecosystem to create flow specific payload defined in FHIR spec applicable in HCX, an implementation guide (IG) defining a set of rules about how FHIR resources are used (or should be used), with associated documentation to support and clarify the usage will be created.

Such a publication can be used to validate content against the implementation guide as a whole.

The extended profiles and structures of the FHIR bundles and resources to be used in HCX are available <here>

Terminologies (Code sets or Metadata standards)

To achieve semantic interoperability, it is recommended that HCX data standards incorporate well established and suitable terminology and coding systems.

In various HL7 standards (including FHIR), these are expressed as Concepts and codes and forms essential vocabulary, ontological binding for resources used to describe document types/categories, element codes and clinical coding like procedure codes, diagnosis codes etc. The data standards defined using FHIR resources and types usually will require agreement on references and usages, through agreed Code Systems and codes, typically manifested through ValueSets.

Guidelines

- For Clinical resources (e.g. Condition, Procedure, Observations) - please refer to the guidance issued by NCRoS.
 - In India, SNOMED-CT is free for use by all as Clinical Terminology, while ICD codes are used for classifications.
 - Labs typically use LOINC codes
- For other code/concepts in the FHIR based data standards, we would recommend guidelines
 - If any attributes are marked as “required” - then, use of the codes defined in the value sets
 - If it is marked as “preferred” or “extensible” - then, users are encouraged to draw from the specified codes for interoperability purposes, unless deemed appropriate within the affinity domain.
 - If marked as “example” - then the domain must agree and define a value set for usage.
 - ValueSet may be created derived from existing sets, either composed/included from the base or expanded.
- For insurance claim domain specific element attributes (e.g. Claim.type) - the domain may define and establish value sets, as suitable in India’s context.

For the broader NDHM interoperability and conformance, HCX would align/inherit domain specific guidelines.

The table below lists the code systems/value sets proposed by current domain working groups. Based on the above guidelines, we are proposing them to be “preferred” or “example” binding strengths as per [FHIR Terminology binding strength definitions \(Section 4.1.5\)](#).

Terminology name	Working Group Link/ Suggestion	FHIR Value Set link	Proposed Binding Strength
Insurance Company Owners (coverageeligibilityrequest.insurer)	 Standard Valu...	TODO	Preferred
Procedure Type (claim.procedure.type)	 Standard Valu...	TODO	Example

Procedure Code (claim.procedure.procedureCode)	ICD-10 Procedure codes	TODO	Example
Denial Codes (claimresponse.item.adjudication.reason)	 E-objects - Tec...	valueset-denial-codes.json	Preferred
Procedure Modifiers (claim.item.modifier)	 Modifiers _proc...	TODO	Example
Service Categories (claim.item.category)	 Suggested _Co...	valueset-service-categories.json	Example
Service Codes (claim.item.productOrService)	 Suggested _Co...	TODO	Preferred
Medical Speciality Type (practitionerRole.speciality)	 Standard Valu...		Preferred
Health Service Provider role (claim.careTeam.role)	 Standard Valu...		Example

HCX or a neutral protocol supporting organisation will host domain specific FHIR Terminology Services which the ecosystem can leverage to retrieve information and use, and validate resources as defined by the IG.

Domain Specific languages (DSLs)

There are two key DSLs being considered for the Health Claims Exchange - Policy Markup Language (PML) and Bill Markup Language (BML). These are currently work in progress and are expected to be released in the later version of HCX specifications after substantial proof of concept development with various members of domain working groups.

Policy Markup Language (PML)

The purpose of policy markup language is to provide a DSL to payers such that the policies can be encoded in machine readable format, thereby helping with the automation of eligibility check and adjudication processes.

Bill Markup Language (BML)

The purpose of bill markup language is to provide a DSL to payers such that the supporting bills can be parsed as machine readable structured data, thereby helping with the automation of adjudication processes.

Healthcare Operations Policies

A thriving data exchange requires clear rules of engagement on various activities in the data exchange to ensure trust from all actors. The key list of policy candidates to be addressed is:

1. Onboarding
2. Defaulting/Deboarding policies
3. Dispute resolution policies
4. Access control (Data sharing) policies - which actor plays what role and gets to see which parts of data. These policies will then affect the visibility and access to domain specific attributes that will typically travel in the body of the data structures defined by the data exchange.
5. Business SLAs
6. Charges and fees - These would be policies around charges various data exchange entities will be allowed to levy on others depending on the role they play
7. Service rating policies - What would be the parameters and mechanisms to rate each type of actor on the data exchange.

The success of the data exchange will depend on trust and willing participation from its ecosystem players. Therefore, to ensure the success of the claims data exchange, its governing policies need to focus on enabling the ecosystem and gaining its trust. To ensure this, the following key policy design guidelines are recommended:

Key design considerations

1. Policies should focus on enabling the ecosystem rather than monitoring or controlling it
2. Policy formulation should be done as an open consultative process to foster trust in policies
3. Rules of participation and disqualification should be transparently laid out
4. They should follow the principle of minimalism and be evolved over a period of time

Keeping these guidelines in mind, the following key policies guidelines are provided for the purpose of wider consultation as part of version 1:

1. Access control (Roles)
2. Participant onboarding/deboarding
3. Grievance redressal
4. Event Audit

Access Control (Roles)

Participating systems in the Claims information exchange ecosystem may possess one or more of the following roles. These roles are based on the base set of organisation roles defined in hl7 specifications [here](#). Namespaced coding is used to further qualify the role in the context of the claims exchange process.

1. **provider**: Health Service Provider
2. **payer**: Insurance service provider
3. **agency.tpa**: Third party administrator acting on behalf of the payer. In the current version, this role is expected to behave like a payer from the data exchange perspective.
4. **agency.regulator**: IRDAI and IIB like regulatory bodies.
5. **research**: Research groups, etc.
6. **member.isnp**: eCommerce platforms facilitating insurance adoption
7. **agency.sponsor**: Scheme owners of specific programs, e.g. NHA for Ayushman Bharat
8. **HIE/HIO.HCX**: Other HCXs

The following table further describes these roles for their corresponding access rights and scenarios for version 1 of the claims exchange process:

Role	Allowed actions	Comments
provider	<ol style="list-style-type: none">1. Eligibility check<ol style="list-style-type: none">a. Send requestb. Receive response2. Pre Auth<ol style="list-style-type: none">a. Send requestb. Receive response3. Claims request<ol style="list-style-type: none">a. Send requestb. Receive response4. Payment<ol style="list-style-type: none">a. Receive noticeb. Send Acknowledgement5. Search/Status<ol style="list-style-type: none">a. Pre authb. Claims status	Providers can make search/status requests for multiple requests that originated from them.
payer/ agency.tpa	<ol style="list-style-type: none">1. Eligibility check<ol style="list-style-type: none">a. Receive requestb. Send response2. Pre Auth<ol style="list-style-type: none">a. Receive requestb. Send response3. Claims request<ol style="list-style-type: none">a. Receive requestb. Send response4. Payment<ol style="list-style-type: none">a. Send noticeb. Receive Acknowledgement	Payers can make search/status requests for multiple payment notices that originated from them.

	5. Search/Status a. Payment confirmation	
agency.regulator	1. Search a. Claims	Data exchange switch will forward the search request to all payers who are expected to return the claims data in the proposed FHIR structure as per regulator's policies.
research	1. Eligibility check a. Receive request b. Send response 2. Search a. Pre Auths - aggregate and/or anonymised b. Claims - aggregate and/or anonymised	All data exhausts for these roles would only have aggregate and anonymised data. Key aggregations for eligibility requests, preauthentication, claims and payments information will need to be further defined.
member.isnp	3. Eligibility check a. Receive request b. Send response 4. Search a. Pre Auths - aggregate and/or anonymised b. Claims - aggregate and/or anonymised c. Claims - Individual claims data as per beneficiary consent	As facilitators of insurance eCommerce, it is proposed to provide ISNPs access to the data available to research role as well as individual beneficiary queries (preauth, claims) based on beneficiary consent. This consent flow is expected to work with existing consent management infrastructure and ISNPs are expected to submit the acquired consent as part of the domain header.
agency.sponsor		As planners of the insurance schemes, sponsors are proposed to be given access equivalent to payer role.
HIE/HIO.HCX		As an HCX this participant is expected to play different roles as per the need of the use case. However, due to

		the data privacy and security measures prescribed in the Open Protocol, it will not be able to view the actual payload.
--	--	---

Participant onboarding

While the actual onboarding/deboarding process for an HCX ecosystem would be drafted by its operator and agreed upon by its participants, this section outlines key design guidelines and an overall approach to arrive at such a policy.

A list of different kinds of participants who would need onboarding into an HCX registry is provided in the Access Control section above. Onboarding onto the HCX is envisioned as a two step process:

1. Sandbox - for compliance testing and certification
2. Go Live on live instances

Sections below provide high level guidelines for each of these steps.

Sandbox Process

The key goal of the sandbox is to help the ecosystem test its specific components against the communication standards, and get certified to become a part of the system. Once a participant successfully completes the sandbox process, they can use the certification to get onboarded to the HCX production environment with the necessary access.

HCX operator(s) may nominate or list Sandbox operators whose certification will be considered valid for onboarding to their platforms.

The following are the steps to integrate, test and launch with the help of sandbox.

Step 1: Registration

The participants submit an online application to express their interest to access the HCX sandbox. The requests from different participants are verified to see if the participant is eligible to participate in the sandbox environment by doing basic checks against the details provided in the application form. Details of the model application form for various roles will be developed in the upcoming phase of the specifications.

There may be requests that would not satisfy the conditions required for the sandbox access such as multiple requests from the same participant, participants not registered with any registry, TSPs without a valid website, spam applications, etc., which would prove to be redundant and may have to be filtered. This process would be semi-manual.

On successful verification, the approved participants are added to the HCX sandbox and provisioned with the necessary credentials to access the sandbox environment.

Step 2: API integration and testing

In this step, the participants integrate their respective claim processing applications with the sandbox HCX. This is to aid the developments as well as ensure that their applications are compliant with the HCX standards and build all the missing pieces on their side to use the set of HCX APIs necessary for their planned workflows.

Sandbox website would also include documentation and suggestions regarding the software libraries, tools and example implementations for encryption, FHIR resource generation, code generation and other new/complex parts of the HCX protocol. The sandbox portal would ensure that the participants are provided with all the necessary help to get started and complete the API integration.

Step 3: Sandbox certification

All participants are expected to fulfil a set of functional and security tests/flows applicable to them.

Based on affiliate HCX policies, the sandbox may necessitate additional security testing and reviews like STQC or CERT-IN. Suggestive pointers on infrastructural requirements for security testing clearance can be found in this [document](#).

Once the system is ready and tested against the applicable test cases, the participant will be required to submit their test results including the application's usage of and interaction with HCX APIs to the Sandbox Operator for review and approval.

On successful review, the sandbox will issue a successful completion certificate valid for a configured period of time. This certificate can be used by the participant to get onboarded to the production environments of the HCX operators.

Go Live process

After obtaining the affiliated sandbox certification, the participant would have to apply for onboarding into the HCX production environment. This process will consist of following key steps:

Step 1: Registration on HCX

In this step, interested participants will be required to go through the onboarding process with the HCX. HCX operators are expected to provide a choice of registration flows with the following high level guidelines:

1. If the participants are registered in the NDHM Health Facility registry, then they should be allowed to use HFR authentication as a means to register in the HCX registry, if they choose to do so.
2. If the participants are not registered in the NDHM Health facility registry then the participant should be allowed to use alternate means of verification like
 - a. Option to complete the NDHM HFR process and use the resultant credentials.

- b. Authentication/Certificates/documents from IRDA or equivalent such agency identified and clearly stated in HCX's onboarding policy.
3. Summary details of the HCX application duly filled. This application form will be more detailed, requiring more details of the participant including contact numbers, company registration details, and other details as needed in the HCX registry.

Step 2: Review of Sandbox certification

A final round of approval for application go-live will be sought from the internal team at HCX. Applicants will be required to share Functional and security testing certificates issued by the affiliate sandbox environment.

Step 3: Provisioning of production credentials

Once these requirements are met, the participant id along with the production access secret credentials will be provided. Participants are expected to keep the secret credentials safe and report any compromises at the earliest to the HCX operators.

Step 4: Go-Live

The application is now expected to be prepared for go-live in respective participant ends. All the participants are advised to plan the change management at their end and conduct necessary training for their staff before going live in production HCX, preferably after piloting with a small set of clients.

Deboarding scenarios

This section lists some of the deboarding scenarios that may be considered as part of the final deboarding policies by the HCX operators:

1. Involuntary deboarding of a participant initiated by Regulator/Legal Authority. Few examples:
 - Suspension/Deactivation of a provider by a regulator for fraudulent activity.
 - Suspension/Deactivation of a TPA or a Payer by IRDA
2. Involuntary deboarding of a participant (mostly TSPs) initiated by HCX. Some examples:
 - Serious violation of HCX policies (e.g. grave SLA violation repeatedly)
 - Hacking attempts made by participants for unauthorized access, after an investigation by HCX
 - Bad or irresponsible behaviour from participants if it significantly impacts the stability and performance of the HCX (like frequent bursts of requests beyond authorised rate limits).
3. Voluntary deboarding of participants. Some examples:
 - A provider or payer shifting to another HCX
 - A provider or payer shuts down their business
 - A provider or payer merges with another entity listed on the exchange

Please note that while the above list suggests a few of the scenarios for potential deboarding of a participant, this process should be treated with utmost care and an elaborate warning mechanism should be kept in place whenever the deboarding is not voluntary.

In addition, to provide a fair chance of appeal, the grievance redressal process on HCX is expected to provide grievance mechanisms to handle appeal against deboarding of a participant.

Guidelines for Grievance Redressal

While the actual grievance redressal policy for an HCX ecosystem would be drafted by its operator and agreed upon by its participants, this section outlines key design guidelines and an overall approach to arrive at such a policy. These guidelines and approach are aligned with earlier thinking from IRDAI in its publication [Re: GUIDELINES FOR GRIEVANCE REDRESSAL BY INSURANCE COMPANIES](#), however these are now envisioned to cover grievance from any actor of the ecosystem with respect to other actors.

Key policy design guidelines

Final operational policies for grievance redressal are expected to be drafted by the HCX operators as these may change over time based on the need of the ecosystem and use cases under consideration. However, to make the policies consistent and effective, the following key grievance policy design guidelines are proposed:

1. Each HCX operator must publish a dispute/grievance resolution policy to allow digital initiation, routing and tracking of the grievances of any of the participants.
2. Policy should clearly list out all the grievances that would be addressed under it and mechanism to resolve grievances that are not covered under it.
3. The policy should require all participating actors to set up nodal governance bodies contactable at the digital and physical communication mechanisms provided as part of onboarding. These communication details are made available to all participants using the read access to the registry.
4. As part of the participant registry, the HCX instance also publishes the details of its governance body.
5. The policy should publish the types and priority of the grievances handled by each type/role of the participant including any required as per prevailing regulations.
6. The policy should publish SLA for each grievance type including any required as per prevailing regulations.
7. The policy should be versioned, required to be signed by new members at the time of onboarding and any change has to be proactively informed to all existing network participants.
8. The policy should require ample due diligence cycle to address the grievance and review the redressal before responding back to the requester
9. The policy should allow for the reopening of the grievances
10. The policy should allow for escalation to the network operator in case the requestor does not feel satisfied with the resolution. Escalated grievances should follow accelerated timelines for resolution.
11. The policy should clearly lay out review and resolution criteria for a grievance to be escalated and the approach the operator would take to reach a resolution.
12. The policy should include ways of keeping requesters informed about the latest status and any additional requirements to help address the grievance.

Proposed Approach for policy formulation

Drafting and evolving an efficient and truly implementable policy for grievance resolution would need an active participation from the HCX ecosystem. Keeping this in mind, following high level approach is proposed in line with overall Approach for Open Specifications described in [HCX - Cover note](#):

1. Like with the specifications so far, constitute a new working group for Dispute Resolution policies.
2. The working group contextualises and adopts the open specifications **design principles** and **high level approach** as detailed in [HCX - Cover note](#) for the dispute resolution context.
3. The working group drafts a model policy in accordance with above principles and in line with detailed approach from step 2 above.
4. The principles, detailed approach and model dispute resolution policy draft is versioned and released for public consultation.
5. The domain working group deliberates the feedback and enhances principles/model policy as needed.
6. HCX Operators adopt the model policy according to the needs of their network
7. Further enhancements, e.g. for new use cases, changes in approach, improvements in model policy due to on ground observations undergo steps 3-6 and result in a newer version of the artefacts (principles, approach or model policy).

Guidelines for event Audits

All events (claim request created, claim forwarded, data requested, authorisation, payment, etc) in the claims flow and corresponding system requests and responses between Provider TMS/Beneficiary apps, HCPs, and Payer TMS must be digitally signed and logged to ensure immutability, non-tamperability, and non-repudiability.

The HCX needs to persist the logs for a configurable (as prescribed by the law of the land) period of time so that they can be retrieved when necessary and this audit trail must be made transparently available to the customer. To ensure integrity, logs should be append-only and should not be allowed to be edited.

Guidelines for Beneficiary Authentication by Providers/Payers

Aadhar Digital eKYC API

Authentication of beneficiaries by providers on provider TMS/beneficiary APP.

The Provider TMS system will support Aadhar eKYC open API integration for beneficiary authentication using Aadhar. All the govt schemes and most of the private providers may use Aadhar based KYC process for verification of the beneficiary in their TMS system.

Optional Aadhar Authentication (mobile OTP/biometric)

Authentication of beneficiaries by providers on provider TMS/beneficiary APP

The Provider TMS system will use Aadhaar based authentication (Aadhar integrated Mobile OTP based authentication, biometric based authentication) for authentication of a beneficiary to initiate the claim transaction in provider TMS system. All provider systems that are enrolled with NDHM will have biometric devices for validation and creation of the health ID.

The payer TMS system and HCP will integrate the Aadhar authentication open API for verification of the beneficiary ID during the claim validation stage.

Verifiable Govt ID based verification (DL/PAN/Voter ID)

Authentication of beneficiaries by providers on provider TMS/beneficiary APP

The providers and payers may choose to integrate different open APIs in their TMS systems to validate the beneficiary ID based on verifiable Government identity database lookup (e.g. PAN, Ration Card, Passport etc.) as well as any other mechanism to verify the beneficiary credentials during enrollment of beneficiary in their systems and validate the beneficiary ID during claim processing

Token based authentication by Payer

In this case, the payer issues a token (e.g., an OTP) to the customer, which the customer then supplies to the provider for subsequent forwarding back to the payer. This provides a confirmation to the payer that the customer has approved the claim request.

Direct Authentication by Payer

The payer authenticates the customer by directly interacting with him. For example, the payer sends a message with an OTP and a URL to the beneficiary's phone. The beneficiary clicks on the URL. The payer displays the beneficiary's photo and some basic details of the claim (e.g. diagnosis, treatment planned and sum claimed). The beneficiary either rejects the claim, or approves it.

Appendix

A - Scenarios for Cross gateway exchange

The cross gateway communication will be required in the following scenarios –

1. When a provider is onboarded in a gateway instance but the payer for that health policy scheme is registered in another gateway instance.
2. If a beneficiary enrolled in health policy took treatment in a network hospital in another state and that hospital is onboarded in a different gateway instance than the payer.

3. For top-up cases, the providers and payers are registered in different gateway instances and in such scenarios primary insurance is handled by one payer in one gateway instance but the secondary insurance is handled by another payer registered in a different gateway instance.