MANUAL DE OPERACIONES

De interoperabilidad IHCE

Elaborado por: OTIC (Ministerio de Salud y Protección Social)
Oficina de OTIC
Versión: 01.1

MINISTERIO DE SALUD Y PROTECCIÒN SOCIAL
Bogotá-Noviembre 2025

Salud

Contenido

1. OBJETIVO

Establecer las directrices técnicas y operativas para la integración de prestadores de salud con la API de Interoperabilidad **IHCE**, con el fin de garantizar el intercambio seguro de Registros Digitales de Atención (RDA), documentos clínicos y resúmenes longitudinales, utilizando el estándar HL7 FHIR.

2. ALCANCE

Este documento aplica a prestadores de servicios de salud (hospitales, clínicas, IPS, centros de urgencias y sistemas HIS) que requieran implementar el envío y consulta de registros clínicos digitales mediante la API IHCE. Cubre desde la autenticación y obtención de credenciales, hasta el envío, consulta, validación y monitoreo de la información intercambiada y finaliza con lineamientos de seguridad operativa y soporte técnico.

3. AMBITO DE APLICACIÒN

Iniciativa: Interoperabilidad de Historia Clínica Electrónica (IHCE).

Responsables: Equipos técnicos de TI de los prestadores de servicios de salud, con acompañamiento del Ministerio de Salud y Protección Social.

Aplicación: Integración de sistemas HIS y plataformas institucionales para el envío y consulta de datos clínicos en el marco de la estrategia nacional de interoperabilidad.

4. DEFINICIONES

- **IHCE:** Interoperabilidad de Historia clínica Electrónica**.**
- **REPS:** Registro Especial de Prestadores de Servicios de Salud.
- **RETHUS:** Registro Único Nacional del Talento Humano en Salud.
- **RDA:** Registro digital de atención.
- **FHIR:** Recursos Rápidos de Interoperabilidad en Salud.
- **HIS:** Sistema de Información Hospitalaria.

5. MANUAL OPERATIVO IHCE

Diseñar e implementar un mecanismo nacional de interoperabilidad para la Historia Clínica Electrónica que permita el intercambio seguro, oportuno y estandarizado de datos clínicos entre los actores del Sistema de Salud colombiano.

5.1 Resumen Operativo

Propósito del mecanismo: Intercambio de Registros Digitales de Atención (RDA) y Resúmenes/Documentos clínicos entre los prestadores y el Ministerio de Salud y Protección Social utilizando el estandar HL7 FHIR (Bundles tipo document, Composition, resources referenciados). El servicio IHCE provee un punto de integración estándar (basado en FHIR y teniendo en cuenta lo expuesto en la guía ***https://vulcano.ihcecol.gov.co/guia/***) para:

- **Enviar** Registros Digitales de Atención (RDA) — Bundles de tipo document con una Composition en la primera entrada.
- **Consultar** RDAs y documentos clínicos (epicrisis/pdf) de pacientes atendidos por otros prestadores, así como un resumen longitudinal con información asociada al mismo.
- **Consultar** y validar pacientes, profesionales, organizaciones y sedes (Location) antes de enviar RDAs.

Cada prestador recibirá credenciales (client_id, client_secret y llaves del API) para obtener tokens OAuth2 y consumir la API.

5.2 Autenticación y Seguridad

Para realizar el consumo de los diferentes servicios expuestos por el mecanismo de interoperabilidad IHCE tendrá que ser gestionado por medio del portal definido para lo solicitud de credenciales por el administrador de cada prestador (Ver manual de gestión de credenciales).

→ **Obtener token (OAuth2 Client Credentials)**

Con las credenciales entregadas.

- **URL:** POST https://login.microsoftonline.com/<tenantid>/oauth2/v2.0/token
- **Transporte**: TLS 1.2+ obligatorio.
- **Headers**

Elemento	Descripción	Valor
Content-Type	Tipo de contenido del body	application/x-www-form-urlencoded

Tabla 1

- **Body**

Elemento	Descripción	Valor
grant_type	Tipo de flujo OAuth2	client_credentials
client_id	ID de la aplicación registrada	<clientid>
client_secret	Secreto de la aplicación	<clientsecret>
scope	Alcance solicitado	<scope>

Tabla 2

- **Response**

Elemento	Descripción	Valor
code	Código HTTP	200 OK

body	Token de acceso	{
		"access_token": "...",
		"token_type": "Bearer",
		"expires_in": 3599
		}

Tabla 3

El cliente obtiene un access_token como respuesta y usarlo como authorization: Bearer <token> en cada petición.

- **Buenas prácticas:**

  ✓ **Rotación de secretos**: El secreto implementado tendrá una rotación periódica definida por el Ministerio de Salud. Para realizar la solicitud del nuevo secreto (Ver manual de gestión de credenciales).

5.3 Convenciones de recursos y referencias

Estas convenciones aplican para los métodos expuestos como Envío de RDA.

- **Bundle**: resourceType: Bundle, type: "document".
- **Composition**: Debe ser la **primera** entrada del Bundle. Solo un Composition por Bundle.
- **IDs locales para recursos a crear**: usar el patrón #TipoRecurso-NumRecurso en cada referencia de cada recurso.

Ej.: ServiceRequest-0, Encounter-0, Condition-0, Condition-1.

El ID de cada recurso será el mismo patrón sin el (#).

Ej.: ServiceRequest-0, Encounter-0, Condition-0, Condition-1.

- **Identificadores persistidos / referencias externas:**

Cuando se referencia un recurso externo (ya existente en IHCE), se referencia como a continuación para los siguientes tipos de recursos.

a) Patient

Usar el patrón #TipoIdentificacion-NumIdentificacion para agregar la referencia de cada recurso paciente.

Ej.: #CC-1234567890

El ID de cada recurso será el mismo patrón sin el (#).

Ej.: CC-1234567890

b) Practitioner

Usar el patrón #TipoIdentificacion-NumIdentificacion para agregar la referencia de cada recurso paciente.

Ej.: #CC-1234567890

El ID de cada recurso será el mismo patrón sin el (#).

Ej.: CC-1234567890

c) Organization (IPS)

Usar el patrón #NumeroDeHabilitacion para agregar la referencia de cada recurso paciente.

Ej.: #0987654321

El ID de cada recurso será el mismo patrón sin el (#).

Ej.: 0987654321

d) Location (Sede de la IPS)

Usar el patrón #CodigoSedePrestador-NumeroSede para agregar la referencia de cada recurso paciente.

Ej.: #0987654321-00

El ID de cada recurso será el mismo patrón sin el (#).

Ej.: 0987654321-00

e) Organization (EAPBS)

Usar el patrón #CodigoEAPBS para agregar la referencia de cada recurso paciente.

Ej.: #EPS000

El ID de cada recurso será el mismo patrón sin el (#).

Ej.: EPS000

5.4 Reglas de validación (obligatorias)

Estas reglas aplican para los métodos expuestos como **envío de RDA** y son ejecutadas por el servidor al recibir un Bundle. El cliente debe validarlas localmente antes de enviar para reducir rechazos.

1. **Bundle.type** debe ser document.
2. **Primera entrada** del Bundle.entry[0] debe ser Composition.
3. **Composition**

a) Solo 1 composition permitidos

b) De acuerdo con la definición de la guía de implementación todas las secciones del Composition deben ser enviadas, dado el caso que no se genere entradas para una sección específica, se enviará un campo/objeto emptyReason con un text estándar y valores predefinidos. Ejemplo sección de alergias en recurso composition:

```
{
"resourceType": "Composition",
                .....
        {
                  "title": "Historial de alergias, intolerancias y reacciones
adversas",
                "code": {
                   "coding": [
                      {
                         "system": "http://loinc.org",
                         "code": "48765-2",
                         "display": "Allergies and adverse reactions
Document"
                      }
                   ]
                },
                "emptyReason":{
                   "coding": [
                      {
```

```
                        "system":
"http://terminology.hl7.org/CodeSystem/list-empty-reason",
                        "code": "nilknown",
                        "display": "Nil Known"
                     }
                  ]
               },
               "text" : {
                  "status" : "generated",
                  "div" : "<div
xmlns='http://www.w3.org/1999/xhtml'>No existen elementos conocidos
para esta lista y/o el paciente no declara información</div>"
               }
.........
            }
```

Imagen 1

4. **Paciente:**

   a. El Patient referenciado debe existir en el registro nacional EVOL, y:

      I. Tipo y número de identificación coinciden con EVOL.
      II. Primer apellido coincide (case-insensitive).
      III. Primer nombre coincide (case-insensitive).
      IV. Sexo biológico coincide.
      V. Paciente con estado: vivo y tipo de documento vigente.

b. El patient extranjero referenciado no realiza la validación contra el registro nacional EVOL y se validará segun la referencia si ya existe dentro del sistema, de lo contrario el patient será creado.

c. El patient sin identificación referenciado no realiza la validación contra el registro nacional EVOL y se validará según la referencia, será creado como un nuevo patient.

5. **RDA duplicados** (encuentro/encounter): El sistema considera duplicado si en Encounter todos estos campos coinciden exactamente con un registro existente: subject, period, service Provider, participant. Si **todos** coinciden → rechazar (409 Conflict). Si **alguno** difiere → acepta.

6. **IDs de recursos a crear**: si se usan referencias #Tipo-Num en el Bundle, debe existir la entrada correspondiente en el Bundle (el ID del recurso Tipo-Num).

7. **Document Reference / attachments**: si se envía un archivo (epicrisis/pdf) verificar content.contentType y que el data o attachment esté bien codificado (base64). Límite de tamaño configurable (ej. 5 MB por attachment).

8. **Practitioner/Organization/Location** referenciados deben estar habilitados y/o activos en REPS y RETHUS para permitir el envío de la información.

5.5 Operaciones principales (resumen técnico)

A continuación, se documentan las operaciones que debe implementar/integrar en el sistema de información hospitalario.

Nota: La URL base será la publicada en el momento de la solicitud de credenciales (Ver manual de gestión de credenciales).

Para el consumo es necesario generar el token de autenticación con el scope correspondiente como descrito en la sección "Autenticación y seguridad" así como incluir la clave de suscripción del ambiente destino.

1) POST / Composition /$enviar-rda-paciente-Enviar RDA Paciente.

USO: Enviar un resumen de información básica del paciente

- **URL:** POST /Composition/$enviar-rda-paciente

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 4

- **Body**

Elemento	Descripción	Valor
resourceType	Tipo de recurso	Bundle
type	Tipo de bundle	document
entry[0]	Primer recurso	Composition
entry[n]	Otros recursos	Patient, Encounter, Condition, etc.

Tabla 5

- **Response**

Elemento	Descripción	Valor
code	Código HTTP de éxito	200 OK
body	Resultado exitoso	Bundle con identificador del RDA
code	Error de estructura	400 Bad Request
body	Detalle del error	OperationOutcome con descripción del campo inválido
code	RDA duplicado	409 Conflict
body	Explicación de duplicado	OperationOutcome indicando Encounter repetido

Tabla 6

Validaciones principales: ver sección "Reglas de validación".

Buenas prácticas: (Ver la sección 5.3 de este manual Convenciones de recursos y referencias).

2) POST / Composition / $enviar-rda-hospitalizacion-Envio RDA hospitalización

USO: Enviar resumen de hospitalización; incluye Encounter.hospitalization, diagnosis, procedimientos.

- **URL:** POST /Composition/$enviar-rda-hospitalizacion
- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 7

- **Body**

Elemento	Descripción	Valor
resourceType	Tipo de recurso	Bundle
type	Tipo de bundle	Document

entry[0]	Primer recurso	Composition
entry[n]	Recurso de hospitalización	Encounter con hospitalization, diagnósticos, procedimientos

Tabla 8

- **Response**

Elemento	Descripción	Valor
code	Código de éxito	200 OK
body	Resultado	OperationOutcome con identificador del RDA hospitalización

Tabla 9

Validaciones principales: ver sección "Reglas de validación".

Buenas prácticas: (Ver la sección 5.3 de este manual Convenciones de recursos y referencias).

3) POST / Composition / $enviar-rda-urgencias-Envio RDA Urgencias

USO: Enviar resumen de urgencias; incluye Encounter.urgencias, diagnosis, procedimientos, entre otros.

- **URL:** POST /Composition/$enviar-rda-urgencias

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 10

- **Body**

Elemento	Descripción	Valor
resourceType	Tipo de recurso	Bundle
type	Tipo de bundle	Document
entry[0]	Primer recurso	Composition
entry[n]	Recurso de urgencias	Encounter con urgencias, diagnósticos, procedimientos

Tabla 11

- **Response**

Elemento	Descripción	Valor
code	Código de éxito	200 OK
body	Resultado	OperationOutcome con identificador del RDA urgencias

Tabla 12

Validaciones principales: ver sección "Reglas de validación".

Buenas prácticas: (Ver la sección 5.3 de este manual Convenciones de recursos y referencias).

4) POST/ Patient/ $consultar-paciente-similar-Búsqueda por similaridad

Uso: devolver pacientes con score para revisión manual con búsqueda similar, en el caso que el paciente ya tenga un primer registro dentro del mecanismo.

- **URL:** POST /Patient/$consultar-paciente-similar

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>

Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 13

- **Body**

Elemento	Descripción	Valor
resourceType	Tipo de recurso	Parameters
parameter.identifier	Identificador del paciente	{ type: CC, value: 1032473124 }
parameter.name	Nombre y apellido	{ family: "Perez", given: ["Juan"] }
parameter.gender	Sexo biológico	male

Tabla 14

- **Response**

Elemento	Descripción	Valor
code	Código éxito	200 OK
body	Resultado	Lista de pacientes similares con score/confianza

Tabla 15

Buenas Prácticas: Mostrar lista al profesional para selección manual si hay dudas.

5) POST / Composition/$consultar-rda-paciente_Listar RDAs

Uso: Realizar consulta de los RDA que han sido registrados a un paciente por número de cédula.

- **URL:** POST /Composition/$consultar-rda-paciente

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>

Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 16

- **Body**

Elemento	Descripción	Valor
resourceType	Tipo de recurso	Parameters
parameter.identifier	Identificador del paciente	{ type: CC, value: 1032473124 }

Tabla 17

- **Response**

Elemento	Descripción	Valor
code	Código éxito	200 OK
body	Respuesta	Bundle con lista de Composition (RDAs), con paginación, si hay paginación estará relacionada en la siguiente ruta Link.relation= next Link.url

Tabla 18

Buenas prácticas:

Paginación: token-based; hay endpoint de siguiente-página para traer la siguiente página.

Uso en visor: paginar y mostrar resumen (fecha, autor, tipo de RDA, organización).

6) GET/ siguiente-pagina /{id devuelto link.url} — Recuperar datos de la siguiente página.

Uso: Si el entry del bundle tiene más recursos de los establecidos como máximos, el sistema generará un Link.url que servirá como consulta para los siguientes recursos.

- **URL:** GET /siguiente-pagina/{id devuelto link.url}

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 19

- **Body**

No aplica

- **Response**

Elemento	Descripción	Valor
code	Código éxito	200 OK
body	Bundle	Bundle completo con recursos asociados a la siguiente página

Tabla 20

Observaciones:

Todos los link.url tienen un tiempo de vigencia, por lo cual solo estarán disponibles por un tiempo limitado.

7) GET/ Composition/ /{id}/$document — Recuperar recursos relacionados a un composition (RDA o PatientSummary)

Uso: descarga del documento clínico o Bundle completo con referencias a primer nivel.

- **URL:** GET /Composition/{id}/$document

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 21

- **Body**

No aplica

- **Response**

Elemento	Descripción	Valor
Code	Código éxito	200 OK
Body	Bundle	Bundle completo con composition y recursos asociados

Tabla 22

Buenas prácticas: Permisos: verificar rol del requester.

8) POST / Practitioner /$ consultar-profesional-salud-validación de profesional.

Uso: verificar que el profesional que firma/autoriza esté habilitado.

- **URL:** POST /Practitioner/$consultar-profesional-salud

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 25

- **Body**

Elemento	Descripción	Valor
resourceType	Tipo de recurso	Parameters
parameter.identifier	Identificador del profesional	{ type: CC, value: 10203040 }

Tabla 26

- **Response**

Elemento	Descripción	Valor
Code	Código éxito	200 OK
Body	Resultado	Datos del profesional o OperationOutcome

Tabla 27

8) GET/ Patient/ {id-patient}/$consultar-resumen-longitudinal

Uso: Usado para ver un resumen longitudinal del paciente, en donde se verá de manera transversal todo lo realizado y formulado en las diferentes atenciones.

- **URL:** GET /Patient/{id-patient}/$consultar-resumen-longitudinal

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 28

- **Body**

No aplica

- **Response**

Elemento	Descripción	Valor
code	Código éxito	200 OK
body	Bundle	Bundle completo con composition y recursos asociados

Tabla 29

Buenas prácticas:

Permisos: verificar rol del requester

5.6 Terminologías

A continuación, se documentan las operaciones de consulta, correspondientes a las terminologías necesarias para el uso correcto del mecanismo.

Nota: La URL base será la publicada en el momento de la solicitud de credenciales (Ver manual de gestión de credenciales).

Para el consumo es necesario generar el token de autenticación con el scope correspondiente como descrito en la sección "Autenticación y seguridad" así como incluir la clave de suscripción del ambiente destino.

OJO! Se recomienda no depender de los endpoints de terminologías a continuación para el envío de los diferentes RDAs y usar dichos endpoints para mantener al día las tablas de codificación y sus respectivos display dentro de sus sistemas.

El sistema es estricto entre el code y su respectivo display. El display debe coincidir exactamente al que se encuentran configurados dentro del mecanismo.

9) GET / CodeSystem/ {code-system} – Codificación.

USO: Permite ver todos los códigos relacionados a una codificación especifica. El nombre del code-system debe ser el que se encuentra relacionado dentro de la guía de implementación

- **URL:** GET /CodeSystem/{code-system}

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 30

- **Body**

No aplica

- **Response**

Elemento	Descripción	Valor
code	Código HTTP de éxito	200 OK
body	Resultado exitoso	CodeSystem con id y concepts de todos los códigos posibles

Tabla 31

10) GET / CodeSystem/ {code-system} /$validate-code?code={código-validar} – Validate Code.

USO: Validar existencia y display de un código para una codificación especifica

- **URL:** GET /CodeSystem/{code-system}/$validate-code?code={código-validar}

- **Headers**

Elemento	Descripción	Valor

Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 32

- **Body**

No aplica

- **Response**

Elemento	Descripción	Valor
code	Código HTTP de éxito	200 OK
body	Resultado exitoso	Parameters con result y el display si existe

Tabla 33

11) POST /CodeSystem/$lookup – Lookup

USO: Permite dar más detalle sobre una codificación.

- **URL:** POST /CodeSystem/$lookup

- **Headers**

Elemento	Descripción	Valor
Authorization	Token de autenticación	Bearer <token>
Ocp-Apim-Subscription-Key	Clave de suscripción	<subscription-key>
Content-Type	Tipo de contenido	application/fhir+json

Tabla 34

- **Body**

Elemento	Descripción	Valor

resourceType	Tipo de recurso	Parameters
parameter	Parametros de la codificación	{ "name": "system", "valueUri": "… /CodeSystem/…" }, { "name": "code", "valueCode": "000" }

Tabla 35

- **Response**

Elemento	Descripción	Valor
code	Código HTTP de éxito	200 OK
body	Resultado exitoso	Parameters con name, versión, display, entre otros, si existe

Tabla 36

5.7 MANEJO DE ERRORES Y OPERATION OUTCOME

- **Estructura:** el API retorna errores estructurados con recurso Operation Outcome (FHIR). Este recurso incluye issue[] con severity, code, diagnostics y location.

- **Mapeo HTTP sugerido:**
  - ✓ 400 Bad Request → error de formato/estructura.
  - ✓ 401 Unauthorized / 403 Forbidden → auth/permiso.
  - ✓ 409 Conflict → duplicado (RDA existente).

5.8 Buenas prácticas para integración (orientado a prestadores).

A continuación, recomendaciones prácticas y específicas para hospitales y centros de atención.

A. Validaciones en origen (HIS)

Implementar validación local *antes* de enviar:

- ✓ Bundle.type == document, Composition como primer entry.
- ✓ Patient identifier y datos demográficos coincidentes (validación mínima local antes de consultar EVOL).
- ✓ Validar que las referencias # existan en el Bundle.

Normalizar nombres (trim, remove extra spaces) y comparar case-insensitive.

B. Encolamiento

Se recomiendo encolar el envío (un envío async), una vez se realice el guardado de la atención (con el fin de no generar bloqueos entre atenciones) y aplicar backoff exponencial para reintentos. Registrar cada intento y respuesta.

C. Autorización del profesional

El profesional que firma debe estar representado por un Practitioner válido.

Antes de permitir envío, validar que el profesional esté habilitado y que la organización corresponda.

D. Visor en contexto de atención

- Integrar resultado de Patient/$consultar-rda-paciente y Patient/{{id-paciente}}/$consultar-resumen-longitudinal en un visor contextual (mostrar sólo RDAs asociados al Encounter actual si existe).

- Mostrar historial mínimo (últimos 12 meses) y proveer filtros por fecha, tipo e institución.

- Asegurar que solo se pueda ver la información del paciente en el momento en que se abra la atención, no dejar abierta la consulta por tipo de identificación y número de identificación en cualquier momento.

- Todos los links de siguiente-página tienen un tiempo de vigencia, por lo cual solo estarán disponibles por un tiempo limitado. En caso de que se venza dicho termino, es necesario realizar nuevamente la consulta original para obtener nuevamente el id de la siguiente página. Se recomienda manejarlo en el visor como suerte de carga dinámica al realizar scroll de las atenciones, no como paginación (1,2,...)

E. Manejo de attachments / documentos

- Evitar subir archivos muy grandes inline. Preferir DocumentReference con attachments codificados y/o enlaces seguros.
- Mostrar vista previa en visor; permitir descarga sólo si el profesional tiene permisos.

F. Seguridad operativa

Conforme a la Resolución 1888 de 2025, los prestadores deberán garantizar que la integración con el Mecanismo Nacional de Interoperabilidad de Historia Clínica Electrónica (IHCE) cumpla con los lineamientos de seguridad definidos por el Ministerio de Salud y Protección Social.

A continuación, se detallan las medidas que los prestadores deben implementar en sus sistemas de información y procesos de consumo del mecanismo IHCE:

En cumplimiento del artículo 6.2. Autenticación:

- Almacenamiento seguro de credenciales:
    - ✓ Los Client ID y Client Secret entregados por el Ministerio deben ser almacenados en repositorios seguros, tales como Azure Key Vault, AWS Secrets Manager o equivalentes.

- ✓ Queda prohibido el almacenamiento de credenciales en texto plano en código fuente, configuraciones no cifradas o repositorios públicos.

- ✓ En caso de que se vea comprometido su Client Secret, debe realizar la solicitud de rotación de este lo antes posible.

  - ✓ La rotación de su Client Secret será válido por un (1) año a partir de la fecha de asignación. Esta podrá ser revocada antes de cumplir dicho periodo, si el prestador deja de estar habilitado para prestar su servicio.

  - ✓ El periodo de validez del Client Secret puede variar amparar bajo la resolución 1888 de 2025.

- Autenticación de usuarios internos:

  - ✓ Deben garantizar la autenticación de sus usuarios internos (talento humano en salud), integrando sus propios mecanismos (ej. Azure AD, LDAP, B2C, etc.) que aseguren la identificación única de cada usuario que accede a la información.

En concordancia con el artículo 6.3. Control de acceso:

- Los prestadores deberán implementar controles basados en roles y permisos (RBAC) dentro de sus sistemas de información, asegurando que solo usuarios y aplicaciones autorizadas accedan a las APIs de interoperabilidad y solo a la información de los pacientes en el marco de su atención clínica.

- Los roles deben estar documentados y asociados a las funciones del talento humano en salud (ej. médico tratante, auditor clínico, administrativo).

- Se debe garantizar que una vez alguno de sus usuarios internos (talento humano en salud) no tenga ningún tipo de relacionamiento con la organización, revocar inmediatamente los permisos correspondientes a las acciones que impliquen algún uso de la solución IHCE.

Con base en el artículo 6.4. Encriptación:

- Todo el tráfico entre el prestador y las API expuesta por parte del Ministerio debe realizarse sobre TLS 1.2 o superior.
- Los datos sensibles del envío de información o respuesta de esta, deberá almacenarse cifrada en reposo, utilizando algoritmos reconocidos internacionalmente (ej. AES-256).

En cumplimiento del artículo 6.5. Monitoreo de operaciones:

- Los sistemas de los prestadores deben contar con registros de auditoría (logs) que permitan identificar:
  - Fecha y hora de cada petición hacia las APIs.
  - Usuario o sistema que realizó la acción.
  - Tipo de operación (ej. visualización de RDA, envío de RDA).
  - Estado de la transacción (éxito, error, rechazo).
- Estos registros deben almacenarse en un sistema de auditoría seguro, inmutable y con retención acorde a la normatividad vigente.
- Los prestadores deben habilitar mecanismos de monitoreo en tiempo real para detectar accesos inusuales o fallidos hacia las APIs.
- Monitorización de errores y alertas (picos de 4xx/5xx, latencia alta, tasas de duplicado).
- La retención de registros, trazas y logs con fundamento se debe amparar adicionalmente de la resolución 1888 de 2025 en (i) la Ley 1581 de 2012 (protección de datos personales) que obliga a adoptar medidas de seguridad y evidencias del tratamiento; (ii) las disposiciones sectoriales sobre manejo y conservación de la historia clínica (Resolución 839 de 2017 y normas complementarias).

En virtud de lo anterior, y atendiendo al principio de proporcionalidad y al análisis de riesgo exigido por ISO/IEC 27001, los períodos de retención aplicables recomendados son:

- Logs de seguridad, acceso, trazabilidad de historia clínica, críticos e investigaciones forenses: mínimo 2 años, ampliables hasta 5 años según riesgo contractual o requisitos regulatorios.
- Logs operacionales y de telemetría no sensibles: mínimo 1 año.
- Ante procesos judiciales, disciplinarios o investigaciones, se aplicará retención excepcional hasta la finalización del proceso.

Estos períodos serán revisados periódicamente (al menos anualmente) y ajustados cuando cambien las exigencias legales y/o definiciones establecidas por el ministerio de salud.

En línea con el artículo 6.7:

- Los prestadores deben garantizar conectividad segura hacia el Ministerio (ej. IP segura, canal TLS).
- Sus sistemas de información deben integrar de manera nativa los siguientes componentes:
  - ✓ Autenticación y autorización de usuarios.
  - ✓ Protección de datos personales en cumplimiento de la Ley 1581 de 2012.
  - ✓ Generación, transmisión y visualización de los Registros de Atención en Salud (RDA) bajo los esquemas definidos por el Ministerio

5.9 Check list de integración rápida (para el equipo técnico)

- ✓ Obtener credenciales (client_id, client_secret / certificado) y probar token endpoint.
- ✓ Realizar mapeo de terminologías
- ✓ Implementar validaciones locales del Bundle.
- ✓ Encolamiento con persistencia de intentos
- ✓ Implementar consultas de Patient/$consultar-paciente o Patient/$consultar-paciente-similar.
- ✓ Configurar visor clínico para mostrar OperationOutcome y lista de RDAs.
- ✓ Asegurar streaming y límites para attachments.
- ✓ Configurar auditoría (logs controlados) y alertas de errores.

6. Consideraciones operativas y monitoreo

- ✓ **Alertas**: tasa de rechazos 4xx elevada, aumento de duplicados (409), latencias crecientes.

- ✓ **Pruebas**: realizar integración QAS con escenarios de: envíos válidos, envíos con discrepancias en paciente, duplicados, attachments grandes.

- ✓ **Soporte**: definir canales y formatos de logs para troubleshooting (requestId obligatorio en respuesta y logs del receptor).

7. Contacto y soporte

Dentro del sitio de la guía se encontrará una colección basada en la herramienta postman de descarga libre en donde se encontrarán un ejemplo de las operaciones para ser probadas y validadas.

Para soporte técnico de integración pedir al equipo de interoperabilidad los endpoints de QAS/Preprod/Prod, las credenciales y el listado de límites de attachments por ambiente.