MANUAL DE OPERACIONES

De interoperabilidad IHCE

Elaborado por: OTIC (Ministerio de Salud y Protección Social)
Oficina de OTIC
Versión: 01

MINISTERIO DE SALUD Y PROTECCIÒN SOCIAL
Bogotá-Octubre 2025

Salud

Contenido

1. OBJETIVO

Establecer las directrices técnicas y operativas para la integración de los prestadores de servicios de salud con el mecanismo de Interoperabilidad de la Historia Clínica Electrónica (IHCE) del Ministerio de Salud y Protección Social, con el propósito de garantizar el intercambio seguro de los Resúmenes Digitales de Atención (RDA) de conformidad con la Guía de Implementación HL7 FHIR.

2. ALCANCE

Este documento aplica a los prestadores de servicios de salud que requieran implementar procesos de envío y consulta de los Resúmenes Digitales de Atención (RDA) a través del mecanismo de Interoperabilidad de la Historia Clínica Electrónica (IHCE).

El alcance abarca desde los procedimientos de autenticación y obtención de credenciales, hasta el envío, consulta, validación y monitoreo de la información intercambiada. Asimismo, incluye los lineamientos de seguridad operativa y las directrices para la gestión del soporte técnico asociado a la interoperabilidad.

3. AMBITO DE APLICACION

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:** Resumen 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 (IHCE), que permita el intercambio seguro, oportuno y estandarizado de datos clínicos entre los diferentes actores del Sistema de Salud colombiano, garantizando la continuidad asistencial, la calidad de la información y el fortalecimiento de la gestión en salud.

5.1 Resumen Operativo

Propósito del mecanismo: El Mecanismo de Interoperabilidad tiene como propósito facilitar el intercambio de los Resúmenes Digitales de Atención (RDA), entre los prestadores de servicios de salud y el Ministerio de Salud y Protección Social, conforme a la Guía de Implementación HL7 FHIR —específicamente *Bundles* de tipo *document*, recursos *Composition* y sus *resources* referenciados—.

El mecanismo de IHCE provee un punto de integración basado en el marco del estándar HL7 FHIR y conforme a los lineamientos descritos en la Guía de Implementación https://vulcano.ihcecol.gov.co/guia/) para:

- **Enviar** Resúmenes Digitales de Atención (RDA) — *Bundles* de tipo *document* con un recurso *Composition* en la primera entrada.
- **Consultar** Resúmenes Digitales de Atención (RDA) y documentos clínicos (epicrisis/pdf) de pacientes atendidos por otros prestadores de

servicios de salud, así como un resumen longitudinal con información asociada al mismo.

- **Consultar** y validar pacientes, profesionales, organizaciones y sedes (Location) previo al envío de los Resúmenes Digitales de Atención (RDA).

Cada prestador de servicios de salud recibirá credenciales de acceso —compuestas por un client_id, un client_secret y las llaves del API—, las cuales permitirán obtener tokens de autenticación OAuth2 para el consumo seguro de los servicios expuestos por la API de IHCE.

5.2 Autenticación y Seguridad

Para realizar el consumo de los diferentes servicios expuestos por la API de IHCE, el acceso deberá gestionarse a través del portal habilitado para la solicitud de credenciales, procedimiento que deberá ser adelantado por el responsable designado de cada prestador de servicios de salud. (manual de gestión de credenciales).

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

Con las credenciales otorgadas.

- **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 prestador de servicios de salud obtiene un access_token como respuesta al proceso de autenticación, el cual debe incluirse en el encabezado de cada petición authorization: Bearer <token>.

- **Buenas prácticas:**

  ✓ **Rotación de credenciales:** las credenciales o llaves asignadas a cada prestador de servicios de salud estará sujeto a una rotación periódica definida por el Ministerio de Salud y Protección Social, con el fin de fortalecer la seguridad en el acceso a la API de IHCE.

  Para realizar la solicitud de nuevas credenciales, el administrador designado del prestador de servicios de salud deberá seguir el procedimiento establecido en el manual de gestión de credenciales.

5.3 Convenciones de recursos y referencias

Estas convenciones aplican para los métodos expuestos como Envío de Resumen Digital de Atención (RDA).

- **Bundle**: resourceType: Bundle, type: "document".

- **Composition**: Debe ser la primera entrada del recurso *Bundle*. Solo un recurso *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 hace referencia a un recurso externo (ya existente en IHCE), esta debe realizarse conforme al siguiente esquema para los tipos de recursos que se detallan a continuación.

a) Patient

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

Ejemplo de referencia: #CC-1234567890

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

Ejemplo de ID del recurso: CC-1234567890

b) Practitioner

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

Ejemplo de referencia: #CC-1234567890

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

Ejemplo de ID del recurso: CC-1234567890

c) Organization (Prestador)

Usar el patrón #NumeroDeHabilitacion para agregar la referencia de cada recurso *Organization* correspondiente al prestador.

Ejemplo de referencia: #0987654321

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

Ejemplo de ID del recurso: 0987654321

d) Location (Sede del Prestador)

Usar el patrón #CodigoSedePrestador-NumeroSede para agregar la referencia de cada recurso *Location* correspondiente a la sede del presatdor.

Ejemplo de referencia: #0987654321-00

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

Ejemplo de ID del recurso:0987654321-00

e) Organization (EAPBS)

Usar el patrón #CodigoEAPBS para agregar la referencia de cada recurso *Organization* correspondiente a la EAPB.

Ejemplo de referencia: #EPS000

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

Ejemplo de ID del recurso: EPS000

5.4 Reglas de validación (obligatorias)

Estas reglas aplican para los métodos expuestos en la operación para el envío de resúmenes Digitales de Atención (RDA) y son ejecutadas por el mecanismo de IHCE al recibir un recurso de tipo *Bundle*. El prestador de servicios de salud deberá validar estas reglas localmente antes del envío, con el fin de reducir rechazos por parte del mecanismo.

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 las definiciones establecidas en la Guía de Implementación, todas las secciones del recurso *Composition* deben ser enviadas. En los casos que no se genere entradas para una sección específica, se enviará un campo/objeto *emptyReason* acompañado de un text estándar y valores predefinidos. Ejemplo sección de alergias en el 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

Paciente:

a. El recurso *Patient* referenciado debe existir en el Registro Nacional EVOL, y cumplir con las siguientes condiciones:

   - **Tipo y número de identificación:** deben coincidir exactamente con los registrados en EVOL.
   - **Primer apellido:** debe coincidir, sin diferenciar mayúsculas o minúsculas (*case-insensitive*).
   - **Primer nombre:** debe coincidir, sin diferenciar mayúsculas o minúsculas (*case-insensitive*).
   - **Sexo biológico:** debe coincidir exactamente con el registrado en EVOL.

b. En el caso de un paciente extranjero, el recurso *Patient* referenciado no se valida contra el Registro Nacional EVOL. Se validará únicamente si la referencia ya existe dentro del sistema; de no existir, el paciente será creado como nuevo registro.
c. En el caso de un paciente sin identificación, el recurso *Patient* referenciado no se valida contra el Registro Nacional EVOL. Se validará únicamente si la referencia ya existe dentro del sistema; de no existir, el paciente será creado como nuevo registro.

Resúmenes Digitales de Atención (RDA) duplicados: El mecanismo considerará un RDA duplicado cuando, en el recurso *Encounter*, los siguientes atributos coinciden exactamente con un registro existente:

- *subject*
- *period*
- *serviceProvider*
- *participant*

Si todos los atributos coinciden, el mecanismo rechazará la transacción con el código HTTP 409 (*Conflict*). Si alguno de los atributos difiere, el registro será aceptado.

Identificadores de recursos (IDs): Cuando se utilicen referencias con el patrón #Tipo-Num dentro del recurso *Bundle*, debe existir una entrada correspondiente en el mismo recurso *Bundle* que contenga un recurso con el ID Tipo-Num. De no existir la entrada asociada, el servidor rechazará el envío por inconsistencia de referencias.

DocumentReference / Attachments: En caso de incluir documentos adjuntos (por ejemplo, epicrisis (PDF)):

- El atributo *content.contentType* debe especificar el tipo MIME correcto (application/pdf).
- El contenido del archivo (data o attachment) debe estar correctamente codificado en Base64.
- Se aplicará un límite de tamaño configurable, por ejemplo, 5 MB por archivo adjunto.
- En caso de error de formato o tamaño excedido, el mecanismo rechazará el Resumen Digital de Atención (RDA)**.**

Validación de los recursos Practitioner, Organization y Location: Los recursos *Practitioner, Organization y Location* referenciados deben encontrarse habilitados y/o activos en los registros nacionales correspondientes (RETHUS y REPS) para permitir el envío y procesamiento de los Resúmenes Digitales de Atención (RDA).

5.5 Operaciones principales (resumen técnico)

A continuación, se documentan las operaciones que debe implementar/integrar en el sistema de información hospitalario (HIS *por sus siglas en inglés*) del prestador.

Nota: La URL base será la publicada en el momento de la asignación de credenciales, conforme al procedimiento descrito en el Manual de Gestión de Credenciales.

Para el consumo es necesario generar el token de autenticación con el scope correspondiente como se encuentra 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 Digital de Atención (RDA) 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: Esta operación permite el envío del Resumen Digital de Atención (RDA) correspondiente a un evento de hospitalización.

- **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/ Patient/ $consultar-paciente-similar-Búsqueda por similaridad

Uso: Retornar 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.

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

Uso: Permite listar todos los Resúmenes Digitales de Atención (RDA) asociados a un paciente, identificados por su número de documento de identidad, con el fin de obtener el historial de atenciones registradas por los diferentes prestadores de servicios de salud.

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).

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

Uso: Cuando el *Bundle.entry* contiene más recursos de los establecidos como límite máximo de paginación, el mecanismo retornará un elemento link.url con la relación next, que servirá como punto de consulta para obtener la página siguiente.

El cliente deberá invocar la URL proporcionada en **link.url** para continuar recuperando los recursos restantes.

- **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.

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

Uso: Esta operación se utiliza para recuperar el Resumen Digital de Atención (RDA) y devuelve un recurso *Bundle* de tipo *document*, que incluye el recurso *Composition* solicitado y todos los recursos referenciados en primer nivel (por ejemplo: *Patient, Encounter, Practitioner, Organization, Condition, Procedure,* entre otros).

- **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.

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

Uso: Esta operación permite verificar que el profesional autor de un Resumen Digital de Atención (RDA) esté debidamente registrado y activo en el Registro Único Nacional del Talento Humano en Salud (RETHUS)

- **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: Esta operación permite obtener el resumen longitudinal del paciente, consolidando de forma transversal toda la información clínica registrada en el Mecanismo de Interoperabilidad IHCE. El resumen longitudinal permite identificar la evolución del paciente a lo largo del tiempo, los procedimientos realizados, diagnósticos formulados, medicamentos prescritos y otra información relevante para la continuidad asistencial.

- **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 Manejo de errores y Operation Outcome

- **Estructura:** La API de IHCE retorna errores estructurados utilizando el recurso *OperationOutcome* conforme al estándar HL7 FHIR.

  Este recurso se emplea para comunicar los resultados de validaciones o errores producidos durante el procesamiento de una solicitud, tanto a nivel estructural como de negocio.

  Cada mensaje de error incluye un conjunto de elementos dentro del arreglo *issue[]*, donde cada entrada describe un problema identificado.

  Estructura general de *OperationOutcome.issue*[]:

  - **severity**: nivel de severidad del error (por ejemplo: error, warning, information).
  - **code**: tipo o categoría del error, de acuerdo con los códigos definidos por HL7 FHIR (por ejemplo, structure, value, processing, invalid).
  - **diagnostics**: descripción detallada del error o mensaje explicativo generado por el servidor.

- **location**: referencia al elemento o campo específico del recurso donde se produjo el error.

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

5.7 Buenas prácticas para integración (orientado a prestadores).

A continuación, recomendaciones prácticas y específicas para los prestadores de servicios de salud

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).
- Confirmar que todas las referencias internas (#) existan dentro del mismo recurso *Bundle*.

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

B. Encolamiento

Se recomienda implementar un mecanismo de envío asincrónico para los Resúmenes Digitales de Atención (RDA), de modo que el proceso no interfiera con la continuidad de la operación del prestador de servicios de salud.

Buenas prácticas:

- Implementar una política de reintentos con backoff exponencial, registrando cada intento y su respuesta.
- Mantener trazabilidad completa de los envíos, respuestas del mecanismo de IHCE y errores recibidos.

C. Representación del profesional de la salud

El profesional de la salud autor del Resumen Digital de Atención (RDA) debe estar representado por un recurso *Practitioner* válido.

Verificar que el profesional de la salud esté habilitado y activo en los registros oficiales (RETHUS) y confirmar que la organización asociada en el envío corresponda a la institución a la cual pertenece el profesional.

D. Visualización en el contexto de atención de un evento

- Integrar resultado de Patient/$consultar-rda-paciente y Patient/{{id-paciente}}/$consultar-resumen-longitudinal en un visor de historia clínica del Sistema de Información Hospitalario (HIS *por sus siglas en inglés*) y mostrar únicamente los Resumenes Digitales de Atención (RDA), cuando este exista.

- Mostrar un historial mínimo de los últimos 12 meses, permitiendo filtrar por fecha o tipo de Resumen Digital de Atención (RDA).

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

- Los enlaces de paginación (link.url con relación "next") tienen una vigencia temporal limitada. Si expiran, el prestador de servicios de

salud deberá reanudar la consulta original para obtener un nuevo identificador de página. Se recomienda implementar una carga dinámica (scroll infinito) en lugar de una paginación tradicional (1, 2, 3…).

E. Manejo de attachments / documentos

- Evitar el envío de archivos de gran tamaño dentro del recurso *Bundle*.
- Preferir el uso del recurso DocumentReference, con archivos adjuntos codificados en Base64 o mediante enlaces seguros.
- En el visor clínico, permitir una vista previa del documento y habilitar la descarga únicamente si el profesional de la salud cuenta con los permisos adecuados.

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

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

Para garantizar una correcta integración con el Mecanismo de Interoperabilidad (IHCE), los prestadores de servicios de salud deberán cumplir con las siguientes acciones técnicas y operativas:

- **Obtener credenciales:** gestionar y registrar las credenciales de acceso (client_id, client_secret y/o certificado digital) e inicializar pruebas con el endpoint de generación de tokens.

- **Implementar validaciones locales del Bundle:** verificar estructura, referencias internas, tipo de documento y datos mínimos requeridos antes de su envío de los Resúmenes Digitales de Atención (RDA) al mecanismo IHCE.

- **Configurar encolamiento con persistencia de intentos:** implementar un mecanismo de envío asincrónico que registre cada intento, respuesta y posible error, con política de reintentos y backoff exponencial.

- **Integrar consultas de pacientes:** habilitar las operaciones: POST /Patient/$consultar-paciente, y POST/Patient/$consultar-paciente-similar, para realizar la validación o búsqueda por similaridad antes del registro o envío del RDA.

- **Configurar el visor clínico:** permitir la visualización de los Resúmenes Digitales de Atención (RDA) asociados al paciente, integrando las operaciones de consulta definidas.

- **Asegurar transmisión de adjuntos:** garantizar el streaming controlado de archivos y aplicar límites de tamaño para los attachments, conforme a las especificaciones del mecanismo.

- **Configurar auditoría y alertas:** implementar registros controlados (logs) y alertas automáticas de error, que permitan la trazabilidad y el seguimiento de los eventos de interoperabilidad.

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

En el micrositio del proyecto de Interoperabilidad de la Historia Clínica Electrónica (IHCE) en la sección Recursos se encuentra disponible una colección Postman de libre descarga, que contiene ejemplos prácticos de las principales operaciones del mecanismo.

Esta colección puede ser utilizada por los equipos técnicos de los prestadores de servicios de salud para probar, validar y familiarizarse con la API de IHCE antes de su implementación en los entornos de integración.

Para soporte técnico, los prestadores deberán contactar al equipo de técnico del Ministerio de Salud y Protección Social, con el fin de solicitar:

- Los endpoints correspondientes a los ambientes de QA, Preproducción y Producción.
- Las credenciales de acceso (client_id, client_secret o certificados).
- El listado de límites de tamaño y configuración de attachments por ambiente.

Toda comunicación de soporte deberá canalizarse a través de los medios oficiales establecidos en la sección Mesa de Servicios del micrositio del proyecto de Interoperabilidad de la Historia Clínica Electrónica (IHCE).