FACULTAD DE INGENIERÍA

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

Privacidad de Datos en la Historia Clínica Electrónica Nacional de Uruguay

Ing. Silvanna Chakeyian

Tesis de Maestría presentada al Programa de Posgrado de Maestría en Ingeniería de Software, Facultad de Ingeniería de la Universidad de la República, como parte de los requisitos necesarios para la obtención del título de Magíster en Ingeniería de Software.

Directora de Tesis:
Dra. Ing. Laura González

Montevideo – Uruguay
Octubre de 2023

Tabla de contenidos

RESUMEN

La historia clínica de un paciente es uno de los elementos esenciales dentro del proceso asistencial, siendo de vital importancia para las decisiones del profesional de la salud. En particular, la historia clínica electrónica es una herramienta fundamental para mejorar dicho proceso. En Uruguay se construyó la Plataforma Salud.uy para dar soporte al desarrollo de la Historia Clínica Electrónica Nacional (HCEN). Esta Plataforma permite y facilita el intercambio de información clínica entre los diferentes actores del área de la salud.

El intercambio de datos en este tipo de contextos introduce desafíos de privacidad que, si no se resuelven de forma adecuada, pueden ocasionar que se revele información confidencial de los pacientes sin su consentimiento. En la actualidad, la Plataforma Salud.uy aborda esta temática permitiendo a los usuarios de servicios de salud acceder a su historia clínica, consultar accesos a dicha historia y realizar una configuración básica de privacidad.

Esta tesis propone una extensión a dicha plataforma permitiendo un nivel mayor de granularidad en las configuraciones de privacidad. En particular, se realiza un relevamiento y análisis del conocimiento existe vinculado a la privacidad de datos en una HCEN, se identifican requerimientos de privacidad de datos en el contexto de la Plataforma Salud.uy, y se proponen soluciones que extienden las que actualmente se brindan en la HCEN de Uruguay.

Las soluciones propuestas comprenden el diseño tanto de interfaces gráficas como de políticas de control de acceso. El diseño de las políticas se apoya en el estándar eXtensible Access Control Markup Language (XACML), utilizando el lenguaje Formal Access Control Policy Language (FACPL).

La evaluación de estas soluciones se realizó en base a casos de prueba utilizando FACPL, una encuesta preliminar a usuarios de servicios de salud y una reunión con Salud.uy. Se concluye que es de interés y relevancia para Uruguay avanzar en las extensiones a la Plataforma Salud.uy propuestas.

Palabras claves:
privacidad, historia clínica electrónica, control de acceso.

Capítulo 1

Introducción

1.1. Contexto y motivación

La historia clínica de un paciente es uno de los elementos esenciales dentro del proceso asistencial, siendo de vital importancia para las decisiones del profesional de la salud [1].

El desarrollo de la Historia Clínica Electrónica Nacional (HCEN) en Uruguay se propuso como uno de los objetivos de la Agenda Digital 2011 - 2015 [2]. Con este fin, surgió el programa Salud.uy que tiene como objetivo proponer soluciones para una fluida y sistemática integración de servicios de salud, en particular, para el intercambio de información clínica entre las Instituciones participantes del Sistema Nacional Integrado de Salud (SNIS).

Para dar soporte al desarrollo de la HCEN, AGESIC[1] y Salud.uy construyeron la Plataforma Salud.uy [3], la cual se presenta de forma simplificada en la Figura 1.1. Esta plataforma permite y facilita el intercambio de información clínica entre los diferentes actores del área de la salud. En particular, la plataforma posibilita que profesionales de la salud consulten el listado y accedan al contenido de documentos clínicos, que fueron generados en prestadores de salud distintos al prestador en el que se está desempeñando el profesional.

[1] Agencia para el Gobierno Electrónico y la Sociedad de la Información y Conocimiento

Figura 1.1: Plataforma Salud.uy de Uruguay [4]

El intercambio de datos en este tipo de contextos introduce importantes desafíos de privacidad que, si no se resuelven de forma adecuada, pueden ocasionar que se revele información confidencial de los pacientes sin su consentimiento [5]. Esta problemática ha motivado el desarrollo de propuestas y soluciones para abordar distintos aspectos de la gestión de la privacidad de datos en el marco de una HCEN [6][7][8][9][10].

En el contexto de la HCEN de Uruguay se ha avanzado en esta temática y en agosto de 2018 se puso en producción la plataforma Accesos Salud.uy [11]. En la actualidad, esta plataforma permite a los usuarios de servicios de salud acceder a su historia clínica, consultar accesos a dicha historia (p. ej. por parte de personal de la salud) y realizar una configuración básica de privacidad. En particular, la plataforma permite que el usuario especifique si se puede o no acceder a su información clínica desde Instituciones diferentes a donde se generó y durante qué períodos de tiempo.

Si bien la Plataforma Accesos Salud.uy tiene previsto aumentar las posibilidades de configuración de políticas de privacidad por parte del usuario (p. ej. permitiendo más nivel de granularidad a la hora de compartir su información entre Instituciones) [11], en la actualidad únicamente se brindan las funcionalidades mencionadas. En este contexto, resulta de interés avanzar en alternativas de solución que brinden soporte a aspectos de privacidad más avanzados para los usuarios y que puedan ser incluidos en futuras versiones de la plataforma.

1.2. Objetivos

El objetivo general de la presente tesis es avanzar en soluciones que brinden soporte a aspectos de privacidad de datos en la HCEN de Uruguay, más avanzados de los que actualmente se ofrecen a través de la plataforma de Accesos Salud.uy. Para esto se plantean los siguientes objetivos específicos:

1. Estudiar, comprender y analizar los avances relativos a la HCEN en Uruguay, incluyendo aspectos tecnológicos y normativos, así como también desafíos a nivel de privacidad de datos.

2. Analizar y caracterizar el conocimiento existente en el área de privacidad de datos en el marco de una HCEN.

3. Identificar y analizar requerimientos relativos a la gestión de la privacidad de datos en la HCEN de Uruguay en base al estudio y análisis previo.

4. Proponer alternativas de solución más avanzadas que las actuales para la gestión de la privacidad de datos en la HCEN de Uruguay, considerando el conocimiento existente y requerimientos analizados previamente.

5. Evaluar las soluciones propuestas (p. ej. mediante casos de estudio de la realidad uruguaya, encuestas a usuarios).

1.3. Aportes

Los aportes que brinda esta tesis son:

1. Relevamiento y análisis de conocimiento existe vinculado a la privacidad de datos en una HCEN, en particular, con respecto a los avances de Uruguay, otros países cercanos y Reino Unido.

2. Análisis de requerimientos de privacidad de datos en el contexto de la plataforma Salud.uy, identificando actores y requerimientos específicos para cada uno. En particular, se identificaron requerimientos que cubren las áreas de capacitación, privacidad y auditorías.

3. Propuesta de soluciones avanzadas para la HCEN de Uruguay en base a los requerimientos identificados con foco en el área de privacidad en gestión de datos (habilitación y revocación de permisos). En particular,

estas soluciones permiten establecer políticas de acceso de granularidad más fina para partes de la HCEN (p. ej. componentes), para distintos perfiles de personal de salud (p. ej. de acuerdo a la especialidad) y para personal de salud específico (p. ej. un médico concreto).

4. Evaluación de las propuestas en base a una encuesta a usuarios y casos de prueba utilizando FACPL, que permitieron verificar funcionalmente las soluciones y validar su importancia para un conjunto de usuarios de servicios de salud de Uruguay. La evaluación también permitió tener un panorama general en relación al conocimiento actual sobre la Plataforma Accesos Salud.uy por parte de los usuarios, así como identificar funcionalidades de valor para desarrollo futuro.

1.4. Organización del documento

Este documento se organiza de la siguiente manera. El Capítulo 2 presenta conceptos generales vinculados a la tesis, describe la situación de la HCE en Uruguay y otros países, y analiza trabajo relacionado.

El Capítulo 3 presenta un análisis de la problemática planteada en el contexto de la Plataforma Salud.uy. En particular, se identifican potenciales actores y requerimientos vinculados a la privacidad de datos en dicha plataforma.

El Capítulo 4 presenta la propuesta de solución para un subconjunto de los requerimientos identificados. En particular, se desarrolla una propuesta para brindar más granularidad al paciente al momento de gestionar la privacidad de sus datos clínicos.

El Capítulo 5 presenta las actividades de evaluación y validación.

El Capítulo 6 presenta conclusiones y trabajo a futuro.

Capítulo 2

Conocimiento existente

En este capítulo se presentan conceptos generales vinculados a la presente tesis, se describe la situación de la HCE en Uruguay y otros países, y se analizan trabajos relacionados.

2.1. Marco teórico

En esta sección se presentan los siguientes conceptos generales: historia clínica electrónica, protección de datos personales en salud, control de acceso y modelos de consentimientos en el área de la salud.

2.1.1. Historia Clínica Electrónica

En esta sección se detalla la perspectiva histórica de cómo surge la historia clínica electrónica (HCE), una descripción general de la misma, qué motivación tuvo y su implementación, de forma genérica.

2.1.1.1. Perspectiva Histórica

Antes de profundizar en el estudio de soluciones propuestas sobre la privacidad en una HCE, se hará una breve introducción del nacimiento de la transformación digital en el área de la salud, para entender cómo surge y qué motivaciones existieron.

Las primeras experiencias de HCE datan de 1986, cuando la Biblioteca Nacional de los Estados Unidos comenzó a trabajar en la elaboración de un Sistema de Lenguaje Médico Unificado, cuyo propósito fue contribuir a auxiliar

a los profesionales y trabajadores de la salud y a la investigación, logrando así almacenar y acceder a los datos de forma eficiente y ágil. De esta manera, se proponía generar mayor conocimiento en el área de salud, compartiendo las prácticas y la información de cada uno de los pacientes [12].

Las HCE evolucionaron de su formato en papel acorde iba evolucionando la tecnología. En una primera instancia, se informatizó individualmente en cada centro de salud, es decir, que el uso de computadoras dio paso al almacenamiento de los datos de pacientes. Esto permitió que la información perdure a lo largo del tiempo sin necesidad de cuidar la fuente, el papel y ocupando menos espacio físico [12].

El paso siguiente fue el desarrollo de las redes internas de los centros de salud, dando la posibilidad que el almacenamiento fuera compartido por diferentes departamentos. Así, la información pasó de ser estática a ser compartida por los distintos profesionales y trabajadores de la salud [12].

Por último, la evolución de Internet permitió implantar una versión más completa de la HCE. Abrió la posibilidad de que varios centros de salud estén interconectados con información precisa de los distintos pacientes [12].

De esta manera, cada médico accede a la información histórica de sus pacientes al momento de la atención, reduciendo el margen de error al diagnosticar. Es por ello, que la evolución de la HCE permitió mejorar las condiciones de trabajo de los diferentes centros de salud, proporcionando a cada profesional la historia clínica de sus pacientes [12].

La HCE se alimenta de la colaboración de diferentes actores de la salud, que generan información y utilizan los datos precedentes para mejorar la atención, conformando así una HCE completa y eficiente [12].

2.1.1.2. Descripción General

La HCE es un compendio de información en formato electrónico que nuclea la información médica de un paciente, con el fin de conocer su estado de salud actual. Incluye informes de médicos tratantes como también un conjunto de archivos electrónicos resultantes de estudios médicos (p. ej. análisis de laboratorio, ecografías, tomografías, entre otros). Al informatizar la historia clínica pasa a ser una parte del sistema integrado de información de salud de un ciudadano [13] [14].

La HCE se conforma por un conjunto de documentos, tanto escritos como

gráficos, que hacen referencia a los episodios de salud y enfermedad de una persona, como también la identificación del médico tratante junto con su especialidad asociada y el prestador de salud al cual pertenece. Debe ser única para cada persona acumulando toda su información clínica y la información de todos sus episodios de consulta, apoyando la salud integrada, eficiente y de calidad [13] [14]. Históricamente la HCE se ha estructurado, p. ej. orientada al tiempo, problemas y fuente [14].

En la HCE orientada al tiempo, los datos se visualizan en orden cronológico. En la orientada a problemas, se registran diagnósticos para el paciente con su grado de valoración correspondiente. Por último, en la orientada a la fuente, el contenido se estructura según la información, p. ej. análisis de laboratorio, rayos X, ecografías, entre otros. Hoy en día, las HCE combinan estas tres estructuras [14].

Los principales usuarios de la HCE son los pacientes o los designados como tutores de la HCE (p. ej. padres, hermanos) y el personal de la salud (p. ej. médicos, enfermeras, técnicos de laboratorio, otros.) [14].

Dado que la HCE de un paciente se puede generar en distintos Prestadores de salud, se han desarrollado modelos de referencia para intercambiar la información clínica de los pacientes. En particular, se destaca el estándar Clinical Document Architecture (CDA) [15] que especifica la estructura y la semántica de los documentos clínicos con el fin de intercambiar y compartir datos de pacientes. El estándar es desarrollado por Health Level Seven (HL7), una organización de desarrollo de estándares centrada en el área de la atención médica. CDA facilita que los documentos sean legibles por máquina (que sean fácilmente analizados y procesados electrónicamente) y legibles por humanos (recuperarse y usarse fácilmente) [16] [17].

Por último, la obligatoriedad de la HCE representa a priori varios beneficios de índole asistencial, tanto para los usuarios del sistema de salud como para los profesionales de la salud actuantes en el acto o evento asistencial (médicos). Por otra parte, el paciente, como titular de la HCE, respecto a su privacidad se encuentra generalmente amparado por leyes de protección de datos personales, debiendo otorgar su consentimiento para el acceso a su información de salud. En este contexto, los Prestadores de salud deben garantizar la confidencialidad de la información clínica, salvo las excepciones legalmente previstas [18].

En la Figura 2.1 se observa que se pueden dar diferentes usos a la HCE,

siempre que existan protocolos de interoperabilidad entre los diferentes Prestadores de salud, potenciando su utilidad y beneficios. Entre los elementos a registrarse en una HCE se encuentran las notas que realizan los profesionales de salud (p. ej. notas hospitalarias, quirúrgicas y ambulatorias).

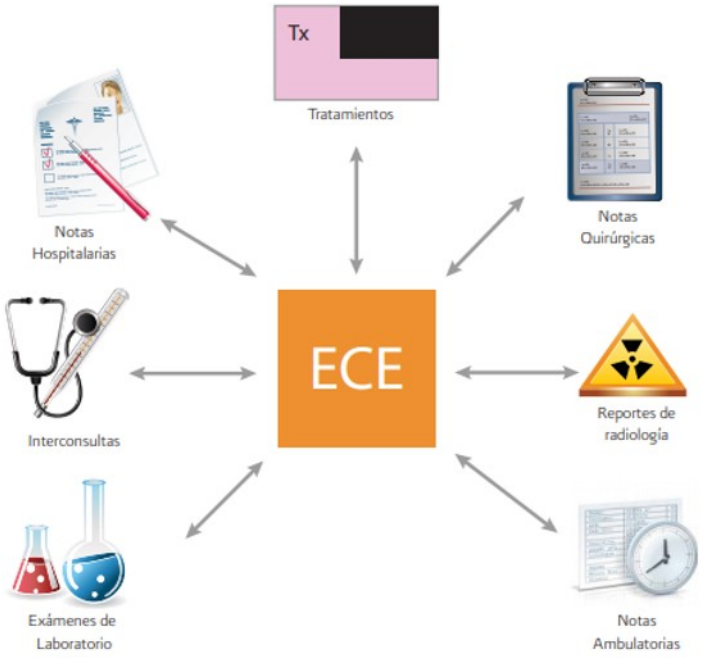

Figura 2.1: Esquema de colaboración de información de HCE [12].

A partir de que la información de una HCE se comparte, se logra mayor efectividad al momento de la atención del paciente.

2.1.1.3. Motivación para la HCE

Existen varios motivos por los cuales nace la HCE, destacándose [12]:

- Las demoras generadas al esperar que llegue la historia clínica al consultorio. Los papeles adjuntos en las carpetas pueden perderse, esto es de alta preocupación ya que, si algo se traspapela, puede ser irrecuperable.
- Problemas logísticos en las Instituciones de salud que requieren un espacio muy amplio para almacenaje de las carpetas de historias clínicas.
- Altos costos en materiales, infraestructura, personal para que sea eficiente un archivo de expedientes clínicos.

- No se puede compartir fácilmente la información de la historia clínica entre Instituciones de salud.

Asimismo, su implementación permite una mejor atención al paciente. Primeramente, lo libera de tener que transportar su historia clínica si tuviera que atenderse en otro prestador de salud. Desde el punto de vista profesional, además de acceder rápidamente a estudios y diagnósticos previos, tiene a mano material fotográfico, todo esto en un único acceso le permite realizar diagnósticos más certeros, ya que la información está almacenada y es de fácil acceso [12].

2.1.1.4. Implementación de la HCE

Para que las HCE puedan ser implantadas y tengan una evolución favorable en el sistema de salud, es necesario y requerido que la conectividad a Internet sea alcanzable en todas las regiones del país. Cada centro de salud debe tener disponible un buen servicio de banda ancha para que pueda compartir información y la propia HCE entre diferentes Prestadores de salud. Para que esto sea necesario, las políticas de estado deben apoyar esta necesidad como también presupuestos que permitan implementarlo, principalmente en los Prestadores públicos de salud [12].

Es importante también, que los Prestadores de salud públicos y privados trabajen de forma conjunta en lo que refiere a la creación de una HCE. Se trata de una medida significativa, ya que la fuerza de las HCE radica en que exista una mayor compartición de información que pueda terminar beneficiando al ciudadano [12].

Existen varios niveles de implementación de una HCE. El primer nivel es el trabajo individual entre el profesional de salud y su paciente, es decir, la consulta médica. En este nivel es requerida una base de datos clínicos del paciente como también un sistema que permita gestionarlos correctamente. Si bien este primer nivel no requiere que la estructura y contenidos del sistema estén normalizados, es preferible usar sistemas homologados con el objetivo de compatibilizar (interoperabilidad) la información con la de otros niveles. El segundo nivel abarca a un centro de salud, un consultorio médico o un servicio hospitalario. Aquí trabaja un grupo reducido de profesionales que pueden disponer de una red de terminales o de computadoras. El tercer nivel es el hospitalario, con un complejo y variado sistema de gestión clínica y adminis-

trativa. En este nivel se consideran dos tipos de arquitectura de sistemas, según la información esté concentrada en una base de datos central, o se reparta por los diversos puestos de trabajo, pudiendo acceder a la misma desde cualquier punto del sistema. El cuarto nivel es el regional o metropolitano, que permite crear una red informática entre centros médicos de una zona geográfica delimitada, urbana y/o rural, con el mismo o distinto nivel asistencial (atención primaria y hospitalaria) y sistema de financiación (público y/o privado). Este nivel facilita la coordinación entre las administraciones, aseguradoras, profesionales y usuarios, planteando objetivos de salud y desarrollando normas o acuerdos nacionales e internacionales [12].

2.1.2. Protección de Datos Personales en Salud

2.1.2.1. Conceptos Generales

Se describen algunos conceptos importantes para normalizar el conocimiento existente de la temática, tomando como base el documento de la Unión Europea [19]:

Procesamiento de datos: se define así a cualquier operación realizada sobre datos personales como ser recopilación, registro, organización, estructuración, almacenamiento, adaptación, consulta de recuperación, uso, divulgación por transmisión, puesta a disposición o difusión, borrado, destrucción [19].

Sujeto de los datos: se refiere a la persona de la cual se tratan sus datos. Por ejemplo, los pacientes son sujetos de datos cuando sus datos personales se procesan con fines de atención médica o de investigación [19].

Controlador de datos: se refiere a las personas o entidades (públicas o privadas) que recopilan y procesan datos personales. Por ejemplo, los médicos generalmente controlan los datos de sus pacientes [19].

Protección de datos: se refiere a que los datos de una persona sean utilizado para fines específicos y toda persona tiene derecho a la protección de los datos que le conciernen [19].

Datos sobre salud: datos relacionados con la salud física o mental de una persona, incluida la provisión de servicios de atención médica, que revelan información sobre su estado de salud [19].

¿Por qué las regulaciones de protección de datos son tan impor-

tantes para los pacientes?

En 2015 se realizó una encuesta de opinión pública en la Unión Europea sobre protección de datos, la misma mostró que la mayoría de la población no sentía tener el control sobre lo que sucede con sus datos. Por eso nace un reglamento, aplicado a partir del 28 de mayo de 2018, el cual busca otorgar a los ciudadanos más derechos e información. Este reglamento tiene en cuenta los cambios provocados por la tecnología, instrumento fundamental para la asistencia sanitaria y telemedicina, tanto regional como de forma transfronteriza [19].

2.1.2.2. Datos Personales en Salud

La protección de datos personales es un derecho que permite controlar la información personal que se comparte con otras personas o Instituciones de salud para prevenir cualquier problema de privacidad. Los datos personales permiten identificar a una persona física o jurídica, directa o indirectamente, y su uso debe basarse en el consentimiento de la persona [20] [21].

Los datos en salud son llamados "datos sensibles" porque su divulgación no autorizada podría tener un impacto negativo en la vida personal de un paciente. Por ello, es importante que las organizaciones conozcan y respeten los derechos de los pacientes, tanto en la atención médica, como en la investigación [20].

2.1.3. Control de Acceso

En esta sección se describe el concepto de control de acceso, así como mecanismos (p. ej. estándares, formalismos) para dar soporte al mismo.

2.1.3.1. Descripción General

El control de acceso es el proceso de mediar cada solicitud a los recursos y datos mantenidos por un sistema y determinar si la solicitud debe ser concedida o denegada. Una política define las reglas de alto nivel que se utilizan para verificar si una solicitud de acceso se concederá o denegará [22] [23] [24].

Existen distintos modelos de control de acceso: Control de Acceso Basado en Roles (RBAC), Control de Acceso Discresional (DAC), Control de Acceso Obligatorio (MAC), Control de Acceso Basado en Atributos (ABAC). En particular ABAC es un modelo lógico que controla el acceso a los objetos mediante

la evaluación de reglas que consideran los atributos de las entidades (sujeto y objeto), las operaciones y el entorno relevante para una solicitud [25].

2.1.3.2. XACML

XACML (por sus siglas en inglés eXtensible Access Control Markup Language) es un estándar que define un lenguaje de políticas de control de acceso, basado en XML y un modelo de procesamiento que describe cómo interpretar dichas políticas, para abordar protocolos de seguridad y accesos [26].

Su enfoque se basa en políticas para la gestión del control de acceso y se centra en permitir la implementación del control de acceso basado en atributos. XACML define un lenguaje de políticas para especificar políticas de control de acceso, así como el formato para solicitar y retornar decisiones de autorización [27] [26] [25].

«La idea general de XACML es que todas las solicitudes para realizar acciones (p. ej. leer, escribir) en recursos (p. ej. registros médicos) por parte de sujetos (p. ej. un usuario) son procesadas por un PEP (Punto de Aplicación de Políticas). El PEP solicita decisiones de autorización al PDP (Punto de Decisión de Políticas), el cual puede obtener información adicional de un PIP (Punto de Información de Políticas) para tomar tales decisiones. El PDP devuelve las decisiones de autorización (p. ej. permitir, denegar) al PEP, que es responsable de hacerlas cumplir. En particular, el PEP puede permitir o denegar el acceso a un solicitante, así como realizar operaciones adicionales (p. ej. obligaciones)» [27] [28].

La Figura 2.2 muestra el flujo de información descripto anteriormente.

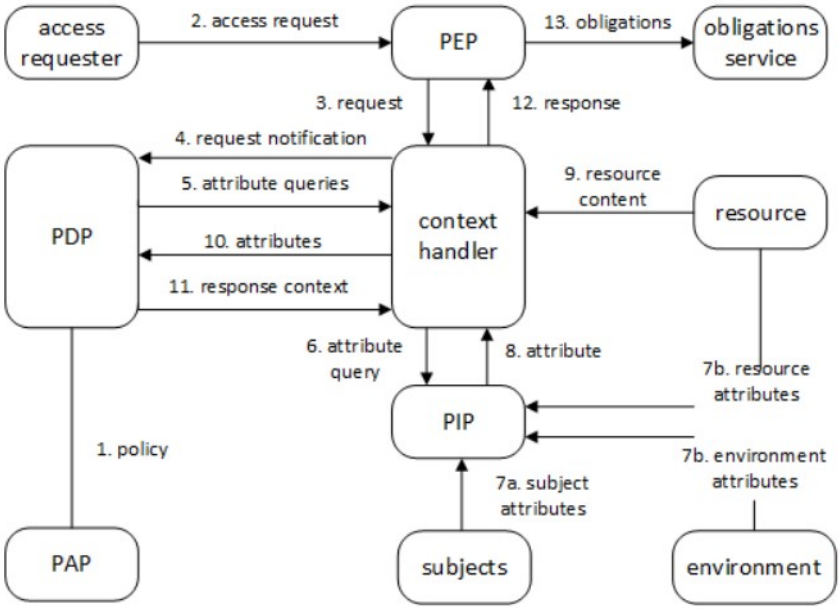

Figura 2.2: Flujo de información XACML [26]

Primero, los usuarios escriben políticas aprovechando el PAP (Punto de Administración de Políticas) y las ponen a disposición del PDP (1). Cuando el PEP recibe una solicitud para acceder a un recurso (2), envía la solicitud en su forma nativa al controlador de contexto (3). El controlador de contexto crea una solicitud XACML y la envía al PDP (4). Esta solicitud XACML puede incluir atributos del solicitante, el recurso, la acción a ejecutar y otra información relevante. El PDP puede solicitar atributos adicionales (p. ej. atributos de sujetos, recursos, acciones, entorno) al manejador de contexto (5). El manejador de contexto obtiene estos atributos de un PIP (6, 7a, 7b, 8) y los envía al PDP (10), incluyendo opcionalmente el recurso (9). El PDP toma una decisión, según las políticas y los atributos, y devuelve una respuesta XACML al controlador de contexto (11) que incluye esta decisión (p. ej., permitir, denegar). El controlador de contexto traduce la respuesta XACML al formato de respuesta nativo del PEP y lo devuelve a este componente (12). El PEP cumple con las obligaciones y recomendaciones que puedan incluirse en la respuesta (13). Además, si se permite el acceso, el PEP permite el acceso al recurso; de lo contrario, deniega el acceso [27] [28].

La Figura 2.3 presenta un ejemplo de una solicitud XACML simplificada que se puede generar cuando John Smith (sujeto) desea leer (acción) su registro médico (recurso) [27].

```
<Request>
    <Subject>John Smith</Subject>
    <Resource>JohnSmithMedicalRecord</Resource>
    <Action>read</Action>
    <Environment></Environment>
</Request>
```

Figura 2.3: Ejemplo de XACML Request [27]

Por otro lado, la Figura 2.4 presenta una respuesta XACML simplificada a la solicitud anterior en la que la decisión devuelta es *permit* y no se devuelven obligaciones ni recomendaciones [27] [28].

```
<Response>
    <Decision>permit</Decision>
    <Status>OK</Status>
    <Obligations></Obligations>
    <Advices></Advices>
</Response>
```

Figura 2.4: Ejemplo de XACML Response [27]

La Figura 2.5 presenta la política XACML simplificada que controla el acceso a la historia clínica del paciente John Smith.

```
1  <Policy>
2      <Target>
3          <Resource>JohnSmithMedicalRecord</Resource>
4          <Action>read</Action>
5      </Target>
6      <CombiningAlgorithm>
7          denyunlesspermit
8      </CombiningAlgorithm>
9      <Rules>
10         <Rule>
11             <Target>
12                 <Subject>John Smith</Subject>
13             </Target>
14             <Effect>permit</Effect>
15         </Rule>
16         <Rule>
17             <Target>
18                 <Subject>doctor</Subject>
19             </Target>
20             <Condition>
21                 subject.doctorId = resource.doctorId
22             </Condition>
23             <Effect>permit</Effect>
24         </Rule>
25     </Rules>
26     <Obligations>
27         <Obligation effect="permit">log access</Obligation>
28         <Obligation effect="deny">notify access request</Obligation>
29     </Obligations>
30 </Policy>
```

Figura 2.5: Ejemplo de política simplificada XACML [27]

El grupo de líneas 2 a 5 define al usuario John y la acción (read) para la ejecución de la política. El grupo de líneas de 6 a 8 define el tipo de acceso. El grupo de líneas de 9 a 25 define las reglas que se aplicarán en la política. El grupo de líneas de 26 a 29 define las obligaciones que deben ocurrir cuando se permite o deniega el acceso.

2.1.3.3. FACPL

El lenguaje de política de control de acceso formal (**FACPL** [29]) es un lenguaje definido formalmente para la especificación, el análisis y la aplicación de políticas de control de acceso siguiendo un modelo ABAC. FACPL tiene una sintaxis compacta e intuitiva y está equipada con herramientas basadas en Java, que incluyen un *plugin* de Eclipse [27].

La Figura 2.6 presenta una política FACPL desarrollada utilizando el *plugin* de Eclipse. La política define las mismas reglas de control de acceso que la

política XACML simplificada descrita en el punto anterior [27].

```
PolicySet MedicalRecordJohnSmith { denyunlesspermit
    target:
      equal ("JohnSmithMedicalRecord", resource/id) &&
      equal ("read", action/id)

    policies:
        Rule Rule1 (permit
            target: equal ("John Smith", subject/id)
        )
        Rule Rule2 (permit
            target: equal ("doctor", subject/rol) &&
                equal (subject/doctorId, resource/doctorId)
        )

    oblp:
         [ M log ( "Resource accessed: " , resource/id ) ]
    obld:
         [ M notify ( "Resource requested: " , resource/id )
}
```

Figura 2.6: Ejemplo de Política FACPL [27]

Proceso de evaluación FACPL[1]: Se basa en el proceso definido por el estándar XACML y descripto en la Figura 2.3. A través del *plugin* de Eclipse es posible no solo especificar políticas sino que también realizar solicitudes a recursos y obtener respuestas de control de acceso, de acuerdo a este proceso de evaluación.

2.1.4. Consentimientos en el área de la salud

En esta sección se describe el concepto de consentimiento en el área de la salud, los formatos, modelos, granularidad y principios de los mismos, de forma general y luego, brevemente aplicados en el área de la salud.

Un consentimiento es un requisito moral que compromete a un sujeto (en plena conciencia de sus actos) a garantizar la participación voluntaria e informada. Se mantiene vigente hasta nuevo aviso, otorgando el consentimiento a quien sea entregado, de acceso a sus datos clínicos sobre su HCE. Si por algún motivo el sujeto no quiere continuar con el mismo, lo revoca [30].

[1] http://facpl.sourceforge.net/guide/facpl_guide.html

2.1.4.1. Formatos de Consentimiento

Existen tres formatos principales para el consentimiento en el área de la salud [30]:

- Basic Patient Privacy Consent (BPPC)
- Advanced Patient Privacy Consent (APPC)
- Fast Healthcare Interoperability Resource (FHIR)

Consentimiento básico de privacidad del paciente (BPPC)

Es un perfil que proporciona un mecanismo para registrar el/los consentimiento/s de privacidad del paciente y un método para que los consumidores de contenido lo utilicen para hacer cumplir el consentimiento de privacidad apropiado para el uso [31].

Este perfil utiliza el término *paciente* para referirse al sujeto humano de los datos relacionados con la salud. Este perfil utiliza el término *consentimiento* para referirse al reconocimiento de una política de privacidad, también conocida como política de acceso a la información, incluyendo restricciones y obligaciones [31]. El perfil BPPC permite al paciente elegir entre un conjunto de políticas de privacidad del paciente predefinidas, sin modificaciones [32].

Los Prestadores de salud utilizan muchos conjuntos de datos diferentes para llevar a cabo tratamientos, operaciones, facturación, entre otros. Esta información puede incluir datos demográficos del paciente, información clínica general, información clínica confidencial, entre otros [31].

Los Prestadores de salud tendrán sus necesidades específicas para acceder a la información del paciente. Por ejemplo, los administradores necesitarían poder acceder a la facturación, contactos, etc., pero no necesitarían acceso a los análisis de laboratorio. Los proveedores de atención general querrán acceder a la mayoría de los documentos clínicos y los de atención directa deben tener acceso a todos los documentos clínicos. Este es un ejemplo de una política de privacidad del paciente [31]. Para profundizar en este perfil, ver Apéndice 2.

Consentimiento avanzado de privacidad del paciente (APPC)

Es un perfil que describe la semántica necesaria para permitir que el/los consentimiento/s del paciente se capturen, administren y comuniquen entre

sistemas y organizaciones. Este perfil permite capturar los consentimientos que no pueden expresarse adecuadamente usando el perfil BPPC [32].

El perfil APPC se considera específico del paciente porque incluye partes individualizadas basadas en las elecciones del paciente. Estos datos pueden incluir mucha información sensible y confidencial. Al usar estos perfiles, cada documento tiene un conjunto claramente definido de atributos de metadatos que incluyen valores codificados que denotan el tipo de documento, la especialidad médica involucrada, entre otros. Este perfil habilita la seguridad basada en atributos a nivel de documento, es decir, si un usuario está autorizado para acceder a un documento específico, mediante el uso de un conjunto de reglas que comparan atributos entre sí o contra restricciones de valor [32].

El perfil APPC permite que un dominio de política de privacidad del paciente tenga una serie de políticas de privacidad que se pueden individualizar y personalizar [32].

El perfil APPC permite que la política de privacidad del paciente brinde al momento de crear reglas de acceso, agregar restricciones a las reglas ya definidas. Es posible que un paciente no quiera dar acceso a todos los médicos a sus documentos clínicos y, por lo tanto, puede limitar las políticas de privacidad para ello [32]. Para profundizar en este perfil, ver Apéndice 2.

Especificación de consentimiento (FHIR)

El estándar HL7 FHIR (Fast Healthcare Interoperability Resources) define cómo se puede intercambiar información de atención médica entre diferentes sistemas informáticos, independientemente de cómo se almacene en esos sistemas. Permite que la información sanitaria, incluidos los datos clínicos y administrativos, estén disponible de forma segura para quienes tienen necesidad de acceder a ella y para quienes tienen derecho a hacerlo en beneficio de un paciente que recibe atención. FHIR contiene el consentimiento para los datos de un determinado paciente, como puede ser una prescripción médica [33] [30].

2.1.4.2. Modelos de Consentimiento

Esta selección de modelos fue desarrollada según investigaciones realizadas sobre las diferentes formas de intercambio electrónico en los Estados Unidos, lo que arrojó que existen cinco modelos de consentimientos básicos. A conti-

nuación, se proporciona una breve definición de cada uno. Estos modelos se presentan en orden según el grado de preferencias del consumidor, de «menor preferencia» a «mayor preferencia». Estos modelos pueden combinarse entre sí bajo el mismo tipo de intercambio [34].

Sin consentimiento

Este modelo brinda la posibilidad del intercambio de información en salud, de forma automática y electrónica, de los pacientes, disponibilizándolos a través de dicho intercambio. Este modelo se utiliza principalmente cuando no se requieren disposiciones adicionales para el intercambio electrónico de información de salud más allá del establecido por las regulaciones de privacidad (p. ej. HIPAA[1]) [34].

Un requisito posible en este enfoque, es que los pacientes sean notificados de su participación en el intercambio, sin embargo, este modelo no permite seleccionar las preferencias individuales con respecto a la participación en el intercambio electrónico (todos los datos fluyen hacia el intercambio), pero sí requiere que los pacientes tengan la oportunidad de ejercer el consentimiento para que la información esté disponible para cualquier propósito. Esto significa que, si bien los pacientes no tendrían la capacidad de restringir el flujo de su información en el intercambio, tendrían cierta autoridad para determinar cómo (p. ej. quién, en qué circunstancias) puede usarse [34].

Opt-out

En este modelo de exclusión el conjunto de datos es compartido en el intercambio, con la posibilidad que los pacientes pueden no querer compartir su información en dicho intercambio. Si aceptan, se comparte el conjunto de datos completo. En un escenario típico de exclusión voluntaria, esto podría significar que la información del paciente se recopila a través del intercambio (utilizándose sólo para fines legalmente permitidos, p. ej. salud pública), pero nunca se comparte con otros proveedores para fines clínicos, cuidando que las preferencias del paciente se acepten de manera tal que su información clínica nunca ingrese al intercambio. Este modelo no permite ninguna granularidad de

[1] https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

preferencia del paciente, lo que significa que la información del paciente está totalmente dentro o fuera del intercambio [34].

Opt-out con excepciones

Es un modelo de exclusión voluntaria con excepciones, las cuales se indican [34]:

1. Excluir selectivamente categorías de datos específicos del intercambio;
2. Limitar el intercambio de su información a organizaciones específicas; y/o
3. Limitar el intercambio de su información para fines específicos.

Muy pocos modelos de intercambio electrónico han permitido una granularidad total en la elección del tipo de datos intercambiados, pero algunos han permitido que los pacientes elijan qué Prestadores de salud pueden acceder a sus datos a través del intercambio. Esta práctica es muy difícil de administrar, es por esto y otras razones que rara vez, se ha implementado [34].

Opt-in

Es un modelo opcional. El conjunto de datos no es compartido en el intercambio a no ser por expresa voluntad del paciente que desee hacerlo. Los que deseen poner a disposición su información médica en el intercambio, deben expresarlo. Este modelo no permite ninguna granularidad de preferencia del paciente, la información se comparte en el intercambio de forma completa. Una vez que el paciente acepta el intercambio, no tiene control sobre qué información se comparte, cómo, con quién o con qué propósito. Existe la posibilidad de que el paciente revoque el permiso [34].

Opt-in con excepciones

Es un modelo opcional con restricciones. Se aplica lo mencionado en el modelo anterior, luego tienen la opción de hacer que toda su información sea elegible para el intercambio [34]:

1. Incluir sólo categorías específicas de datos o elementos de datos;

2. Permitir que la información fluya solo a proveedores específicos; y/o

3. Permitir que su información se intercambie solo para fines específicos.

Cada uno de estos modelos de consentimiento representa, en teoría, una opción clara sobre cómo se puede abordar el consentimiento del paciente para el intercambio electrónico de su información clínica. Aunque las categorías de consentimiento anteriores parecen ser mutuamente excluyentes, algunos sistemas de intercambio electrónico tienen marcos de política lo suficientemente flexibles como para permitir que coexistan múltiples modelos de consentimiento [34].

También hay múltiples modelos de consentimiento del paciente, que van desde el no consentimiento que se produce automáticamente (que se aplica al personal en servicio de salud), a varias opciones de exclusión (se produce por defecto) y la suscripción (se requiere autorización por escrito). Los enfoques centrados en el paciente, en los que cada uno de ellos recibe un identificador único y luego accede para especificar sus preferencias, ofrecen el control sobre quién obtiene sus datos, para qué fines y durante qué período de tiempo [35].

2.1.4.3. Granularidad del Consentimiento

La granularidad del consentimiento es una forma de abordar la preocupación del paciente sobre el intercambio electrónico de su información clínica o partes de ella, permitiendo restringir el acceso a la información solo a aquellas Instituciones de salud aprobadas por el paciente. Los enfoques principales son [34]:

1. El paciente tiene la opción de permitir el acceso solo a Instituciones específicas

2. El paciente tiene la opción de permitir el acceso solo a Instituciones específicas o especialidades del personal de salud

2.1.5. Control Granular de la Información de Salud

En esta sección se describe la temática del control de acceso granular en la información del área de la salud.

2.1.5.1. Descripción general

Saber cuánta información médica brindar de los pacientes siempre fue un tema de discusión. Con la HCE los datos se almacenan de forma electrónica, las mismas son pasibles de intercambios entre Prestadores de salud, por ello dentro de ciertas limitaciones, los pacientes deberían poder controlar qué información es puesta a disposición del personal de la salud. Esto adquiere complejidad, no solo para compartir sus datos médicos, sino análisis de laboratorio, diagnósticos, entre otros [36].

Pero tanta información y de diferente tipo puede crear barreras éticas y legales, sobre todo por el alcance adecuado de dicho control de acceso. Solicitar a un paciente que considere la divulgación de sus datos médicos para posibles destinatarios de la salud puede ser abrumador. Por ejemplo, un paciente puede desear que sus estudios psiquiátricos no sean vistos por un cardiólogo o el médico de cabecera de su familia, entre un sinfín de casos posibles [36].

Sea cual sea la situación, esas acciones tienen consecuencias, si bien son beneficios para los pacientes, conllevan profundos desafíos desde logísticos, éticos, entre otros. A pesar de que estas herramientas están siendo utilizadas, hay áreas grises, particularmente en la intersección de la información de salud y la toma de decisiones. Debe existir la protección de la privacidad innata y sólida en los datos, tanto en reposo como en tránsito, pero hay que tener sumo cuidado ya que un paciente puede tener un control granular desorganizado de la información médica [36].

El control granular está dentro del interés fundamental que tienen las personas en la privacidad de la información, que generalmente se ejerce mediante la capacidad de limitar el acceso de otros a la información médica personal. Se puede considerar que brindar este control equilibra la relación médico-paciente, promoviendo la confianza y mejorando la calidad en la atención [36].

Para que el paciente tenga un control granular sobre su información médica, debe existir una plataforma para que los informáticos desarrollen interfaces de usuario, soporte de decisiones y almacenamiento que debe estar disponible para los usuarios finales. El intercambio de información entre Prestadores de salud y pacientes debe ser transparente y sin interrupciones [36].

Si se logra una capacitación adecuada tanto para el personal de salud como al paciente, se visualizará transparencia en el proceso de ejercer control granular de la información clínica, de forma segura y precisa [36].

2.1.5.2. Ejercer el control granular

Es necesario que los desarrolladores y analistas de sistemas tomen tiempo en diagramar el sistema de control de divulgación y no divulgación de información clínica de un paciente, no solo internamente sino también, en la usabilidad del sistema para el paciente. Desde un extremo, se podría presentar al paciente la opción de permitir o limitar el acceso a cada elemento de dato individual, como puede ser una consulta médica determinada o un examen de laboratorio puntual. Este extremo tiene la ventaja de ofrecer al individuo un nivel tal de granularidad que ejercería un control preciso. Pero tiene como desventaja la abrumadora cantidad de información que puede divulgar o limitar el paciente. En el otro extremo se le puede presentar al paciente solo categorías amplias de datos como ser: personal de la salud (p. ej. médicos, especialistas, no médicos, etc.), tratamiento (p. ej. recetados, urgentes, etc.), sensibilidad de los datos (p. ej. salud reproductiva, mental, abusos, enfermedades de transmisión sexual, etc), únicos diagnósticos (p. ej. diabetes, tiroides, etc). De esta forma podría ser más sencillo para el paciente comprender las opciones en estos niveles más gruesos de control granular [36] [37].

De igual forma se puede ejercer la granularidad para los destinatarios de los datos, es decir el sistema podría permitir que los pacientes determinen el acceso a médicos de forma individual o de forma más amplia, determinar el acceso a los médicos de una Institución de salud, entre otros [36] [37].

Otro nivel de granularidad podría ser variable, el paciente decide si el nivel de granularidad es fino o grueso, pero aquí se complejiza todo el esquema, ya que al paciente también se le complejizan las decisiones que debe tomar junto con la capacitación que hay que brindarles [36] [37].

Finalmente, se puede tener control granular por tiempo determinado, por ejemplo, un paciente desea dar control sobre un determinado análisis clínico, a un determinado profesional de la salud, por un período de tiempo acotado [36] [37].

El sistema debe informar de alguna manera las preferencias de acceso / restricciones de datos por parte de un paciente cuando un profesional o la Institución de salud accedan a su historial de salud. Sea cual sea la forma de notificarlo, puede suceder que se dañe o afiance la confianza entre el profesional y el paciente [36] [37].

Cuando un Profesional de salud acceda a la HCE, el sistema puede:

- Mostrar qué información existe y es accesible y qué información existe pero está restringida debido a la configuración de privacidad del paciente.
- Mostrar únicamente la información permitida por la configuración de privacidad del paciente, sin revelar la existencia de información sujeta a privacidad.

Está claro hasta aquí, pero qué sucede frente a situaciones de emergencias que peligra la vida y que el paciente tiene restringida la información para una determinada área, siendo el caso del ingreso a emergencias. Es deseable que las Instituciones de salud tengan la posibilidad de anular las restricciones del paciente y el sistema solicite que el Profesional de salud a cargo justifique dicha anulación, quedando registro en la HCE. Es deseable que esta anulación emita una notificación al paciente si es que éste, así lo configuró, ya que se ampara bajo el Principio Ético de respeto a la autonomía del paciente [36] [37].

2.2. Historia Clínica Electrónica en Uruguay

En esta sección se presenta el desarrollo de la HCEN en Uruguay, en particular, describiendo aspectos de privacidad.

2.2.1. Descripción General

En Uruguay existe el Programa Salud.uy que es una iniciativa entre diferentes entidades estatales[1]. En el marco de este programa se desarrolló la Plataforma Salud.uy que, en particular, da soporte a la gestión del consentimiento de los usuarios sobre el acceso e intercambio de sus registros clínicos [38].

En la Figura 2.7 se observa el ecosistema de salud de Uruguay, en el que la historia clínica de un paciente está distribuida en los distintos actores que tuvo o tiene vinculación [38].

[1] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/2019-01/Folleto%20Institucional%20Salud.pdf

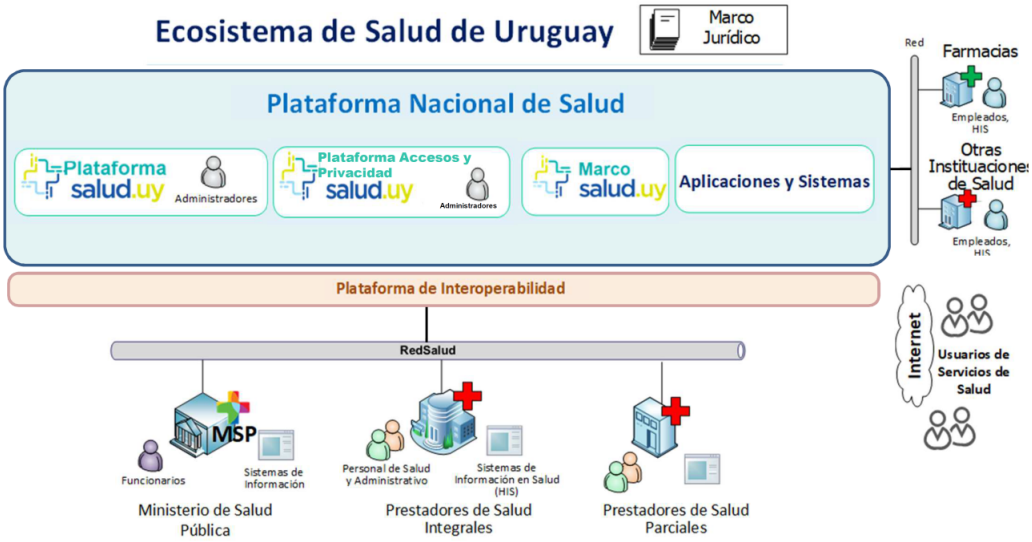

Figura 2.7: Ecosistema de Salud de Uruguay [38]

La plataforma de interoperabilidad es provista por AGESIC[1], tanto a nivel técnico como normativo. La RedSalud[2] es una red segura de alta velocidad que permite que actores de la salud se conecten a la Plataforma Nacional de Salud (PNS). Es provista por la Administración Nacional de Telecomunicaciones (ANTEL)[3] y se instala en cada prestador de salud [38].

Los prestadores de salud se categorizan en integrales y parciales. Los integrales brindan todos los servicios de salud incluido el Centro de Tratamiento Intensivo (CTI), establecido en el marco jurídico, como por ejemplo Asociación Española[4], CASMU[5], entre otros. Los parciales solo ofrecen un subconjunto de estos servicios, como ser las emergencias móviles por ejemplo SUAT[6], SEMM[7], entre otros [38].

Los prestadores de salud cuentan con Sistemas de Información en Salud, HIS (por sus siglas en inglés Health Information Systems) propios para gestionar la información de sus pacientes, pudiendo realizar intercambios de la misma a través de la Plataforma Salud.uy la cual se apoya en RedSalud [38].

El Ministerio de Salud Pública (MSP)[8] tiene un rol importante sobre la

[1] http://www.agesic.gub.uy/
[2] https://centrodeconocimiento.agesic.gub.uy/web/salud.uy/red-salud
[3] https://www.antel.com.uy/
[4] https://www.asesp.com.uy/home
[5] https://casmu.com.uy/
[6] https://suat.com.uy/
[7] https://www.semm.com.uy/
[8] https://www.gub.uy/ministerio-salud-publica/home

PNS, le provee varios sistemas de información, como por ejemplo certificado de nacidos vivos. De acuerdo a sus intereses, potestades, privilegios y servicios específicos, el MSP cumple un rol de auditoría y contralor en el ecosistema [38].

El MSP cuenta también con sistemas de información de uso interno y provee también sistemas que utilizan otros actores (p. ej. Certificado de Nacido Vivo Electrónico) así como sistemas que son necesarios para la HCEN (p. ej. Registro Único de Cobertura de Asistencia Formal, RUCAF) [38].

El ecosistema se completa con la participación de las farmacias y otras Instituciones de salud como ser laboratorios, clínicas privadas, etc. Las farmacias tienen un rol importante dado que en corto plazo se avanzará en el desarrollo de un sistema de prescripción electrónica [38].

La Plataforma tecnológica Salud.uy está desarrollada para dar soporte al Sistema Nacional Integrado de Salud (SNIS), principalmente al intercambio de información clínica. La Figura 2.8 muestra los componentes de la plataforma Salud.uy [38].

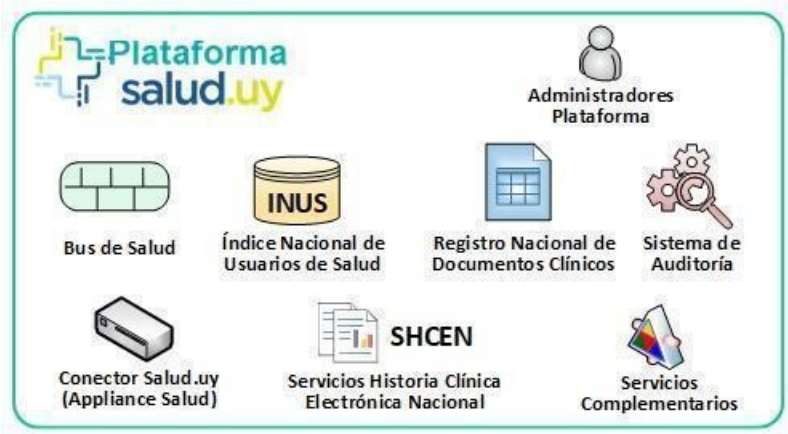

Figura 2.8: Plataforma Salud.uy del Ecosistema de Salud [38]

Esta plataforma está compuesta por: un Bus de Salud, el Índice Nacional de Usuarios de Salud (INUS), el Registro Nacional de Documentos Clínicos, un Sistema de Auditoría, el Conector Salud.uy (Appliance Salud), Servicios que dan soporte a la HCEN, Servicios de Acceso a Diccionarios y Servicios Externos [38].

El **INUS** gestiona los datos patronímicos de los pacientes y tiene como finalidad identificarlos unívocamente dentro de la plataforma [38].

El **Registro Nacional de Documentos Clínicos** permite conocer en

qué prestador se encuentra cada documento clínico electrónico que conforma la historia clínica de un paciente [38].

Los **Servicios HCEN** dan soporte a la HCEN permitiendo el intercambio de información clínica entre los diferentes actores del sistema. Principalmente estos servicios permiten a un prestador de salud dar de alta a usuarios en el INUS, registrar un documento clínico en el Registro Nacional de Documentos Clínicos, recuperar de este registro la lista de documentos clínicos asociados a un paciente y recuperar documentos clínicos alojados en otros prestadores [38].

El **conector de Salud.uy** es un componente que se ejecuta localmente en cada prestador de salud y permite facilitar su integración con la plataforma. Principalmente, resuelve temas de seguridad, auditoría y publicación de servicios web, entre otros [38].

El componente **bus** de Salud.uy es un componente especializado en resolver problemáticas de integración [38].

El **Sistema de Auditoría** brinda mecanismos para posibilitar auditorías en la plataforma, en relación a aspectos del negocio y aspectos técnicos [38].

Los **Servicios Complementarios** son servicios ofrecidos tanto por Salud.uy como por terceros que se ponen a disposición a través de la plataforma. Los Servicios Complementarios contienen: Servicios Terminológicos, Servicios de Accesos a Diccionarios y servicios del MSP [38].

Los **Servicios Terminológicos** brindan acceso a los servidores terminológicos del Hospital Italiano de Buenos Aires (HIBA[1]). Los **Servicios de Accesos a Diccionarios** brindan acceso a diccionarios elaborados por Salud.uy (p. ej. terminología farmacéutica). El MSP brinda servicios que posibilitan realizar consultas relacionadas con afiliaciones de usuarios, a prestadores de salud, entre otras.

La Plataforma de Accesos y Privacidad Salud.uy es la solución tecnológica desarrollada para dar soporte a la gestión del consentimiento de los usuarios sobre el acceso e intercambio de sus registros clínicos que se encuentran indexados en la Plataforma Salud.uy [38].

Como se puede ver en la Figura 2.9, esta plataforma esta compuesta por un Repositorio de Políticas, en donde se almacenan la políticas de acceso que reflejan los consentimientos almacenados por los usuarios, y un Sistema de Decisión a través del cual se evalúa si un determinado acceso a la información

[1] https://www.hospitalitaliano.org.ar/#!/home/principal

clínica de un usuario, desde alguna Institución de salud, bajo circunstancias asistenciales, es válido según los consentimientos almacenados [38].

Figura 2.9: Platorma Accesos y Privacidad [38]

2.2.2. Flujo para Consulta y Recuperación de Documentos Clínicos

A modo de ejemplificar el funcionamiento de la plataforma, en esta sección se describen las interacciones que se realizan cuando un prestador de salud quiere consultar y recuperar un documento clínico de otro prestador. Para ello nos basamos en la Figura 2.10 y Figura 2.11 [38].

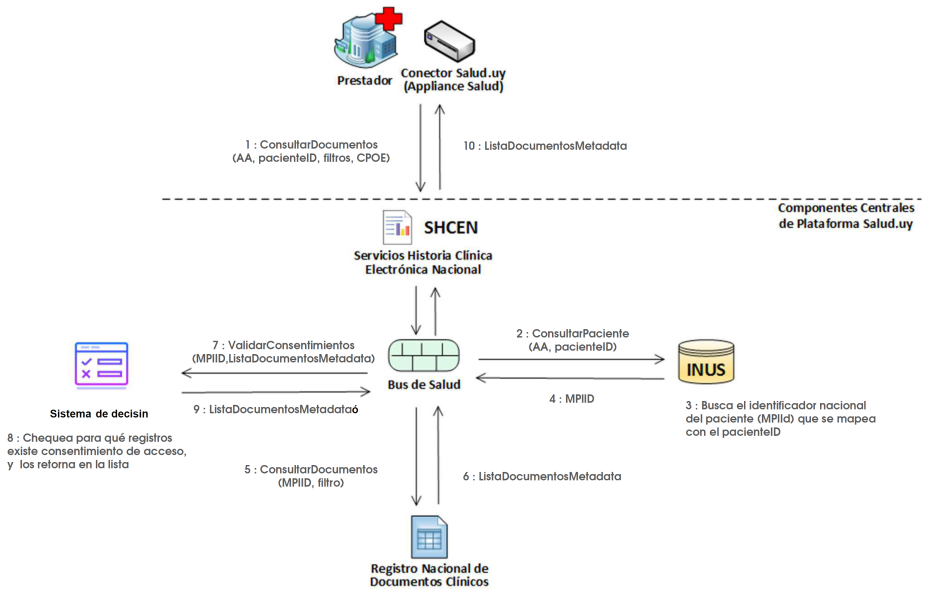

Figura 2.10: Consultar documentos - Plataforma de Accesos Salud.uy [38]

Consultar Documento es una interacción iniciada por un prestador, invocando un servicio HCEN con el objetivo de consultar documentos clínicos (1)

[38].

El prestador invoca un servicio HCEN a través del Appliance Salud. El Bus de Salud le envía al INUS una consulta para obtener el identificador nacional del paciente (2). Una vez obtenido este dato (4), envía una nueva consulta de documentos al Registro Nacional de Documentos Clínicos (XDS) con el identificador nacional del paciente (5), los filtros de búsqueda recibidos y la lista de convenios encontrados (6). El XDS resuelve la consulta (8) y devuelve la lista de metadatos de los documentos encontrados (9). Una vez recibidos estos datos, y teniendo en cuenta que la consulta de documentos no ocurrió bajo un evento asistencial de emergencia (*breaking the glass*), el BUS de Salud deberá validar contra la Plataforma de Accesos y Privacidad si existe el consentimiento del paciente para compartir estos datos con el prestador que inició el flujo (10) [38].

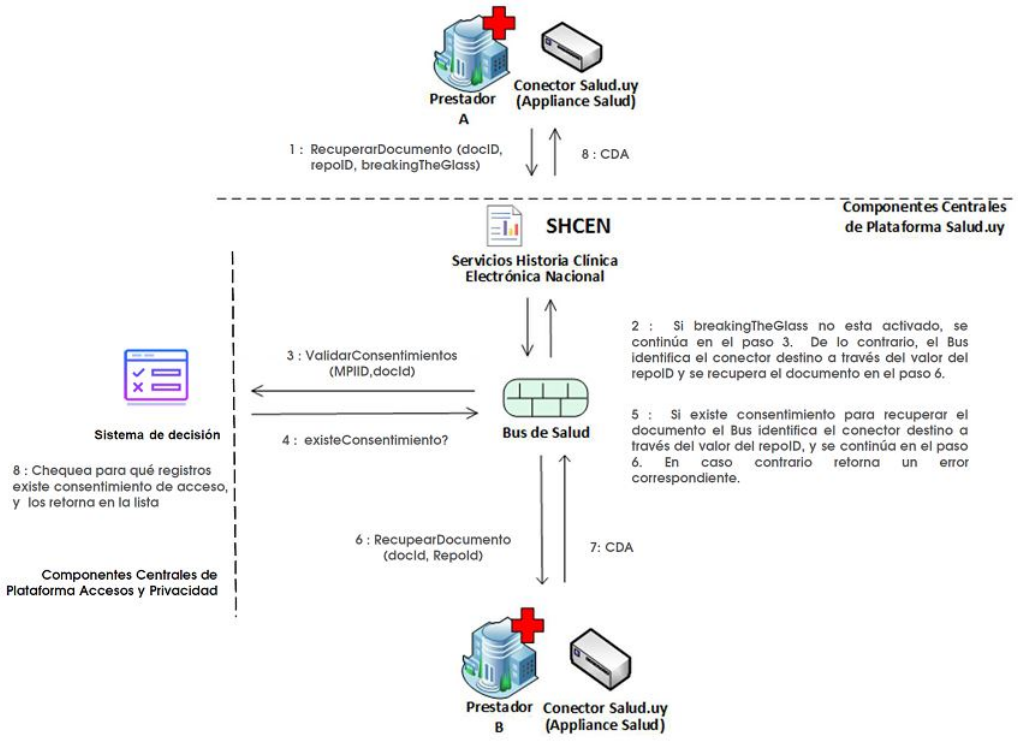

Figura 2.11: Recuperar documentos - Plataforma de Accesos Salud.uy [38]

Recuperar Documento es una interacción iniciada por un prestador, invocando un servicio HCEN con el objetivo de obtener documentos clínicos (1)[38].

Usualmente, el usuario realizará primero la interacción **Consultar Documentos** a través de la cual obtendrá los metadatos de los documentos asocia-

dos a un paciente (8). A continuación podrá realizar la interacción **Recuperar Documento** (1) para ver los detalles de alguno de ellos siempre y cuando exista el consentimiento para tal fin (6). Este documento estará registrado en el **Registro Nacional de Documentos Clínicos** y alojado en el repositorio de otro prestador (7). Previamente a recuperar el documento desde el prestador correspondiente, y teniendo en cuenta que el flujo para recuperar el documento no ocurrió bajo un evento asistencial de emergencia (*breaking the glass*)(2), el BUS de Salud valida contra la Plataforma de Accesos y Privacidad Salud.uy (3) si existe consentimiento del paciente para acceder al documento clínico (8)[38].

2.2.3. Plataforma de Accesos

De acuerdo a lo mencionado en la página oficial [39], el sistema actual de la plataforma de Accesos Salud.uy tiene por objetivo principal asegurar la continuidad de la asistencia médica al usuario en el SNIS. Para esto la información clínica debe estar disponible en cualquier parte del país y en cualquier prestador de salud. Con este fin, se habilita el acceso al personal de salud a los registros clínicos digitales del usuario, en las siguientes situaciones [39]:

1. Durante una consulta clínica.

2. Ante una emergencia asistencial.

Para ello el usuario en la plataforma puede cambiar el acceso a su HCEN a los prestadores de salud, todas las veces que lo considere necesario. Cuenta con tres opciones [39]:

1. **Habilitar** el acceso al personal de salud de los prestadores del SNIS a la información clínica digital del usuario (paciente), solo con fines asistenciales.

2. **Habilitar parcialmente** el acceso de forma temporal al personal de salud de los prestadores del SNIS a la información clínica digital del usuario (paciente), solo con fines asistenciales.

3. **No habilitar** el acceso del personal de salud de los prestadores del SNIS a la información clínica digital del usuario (paciente), excepto situaciones de emergencia asistencial.

Aclaración: las opciones habilitar parcialmente y no habilitar, aplican a [39]:

1. El acceso del personal de salud de prestadores a los que el usuario (paciente) sí está afiliado, pero a eventos asistenciales que tuvo en otros prestadores.

2. El acceso del personal de salud de prestadores a los que el usuario (paciente) no está afiliado.

3. La opción habilitar parcialmente solo está disponible ingresando al aplicativo Mi Historia Clínica Digital[1].

2.2.3.1. Descripción general

Esta sección permite conocer brevemente la aplicación **Mi Historia Clínica Digital** desarrollada por la plataforma de Accesos Salud.uy. Una vez dentro del sistema, se podrá observar un menú de opciones para acceder directo a *Mi historia clínica*, para conceder/revocar permisos, como también visualizar el historial de accesos que tiene actualmente la HCEN. Se verá símil a la Figura 2.12 [39]

2.2.3.2. Ejemplo de uso

Se expone brevemente un caso real de un usuario el cual accede a dicho aplicativo, no se pretende profundizar en su funcionamiento pero si dar una recorrida por el mismo, cuando aparezcan datos sensibles se ocultarán. El usuario se registra y procede al login con un lector de cédulas. Una vez dentro, se visualiza como muestra la Figura 2.13

[1] https://mi.iduruguay.gub.uy/login?process_state=z-i-bBwJWerpKMIy7uaR43RQn8nxEKDnYdcNEkkPLYc

Figura 2.12: Pantalla principal del sistema en línea [39]

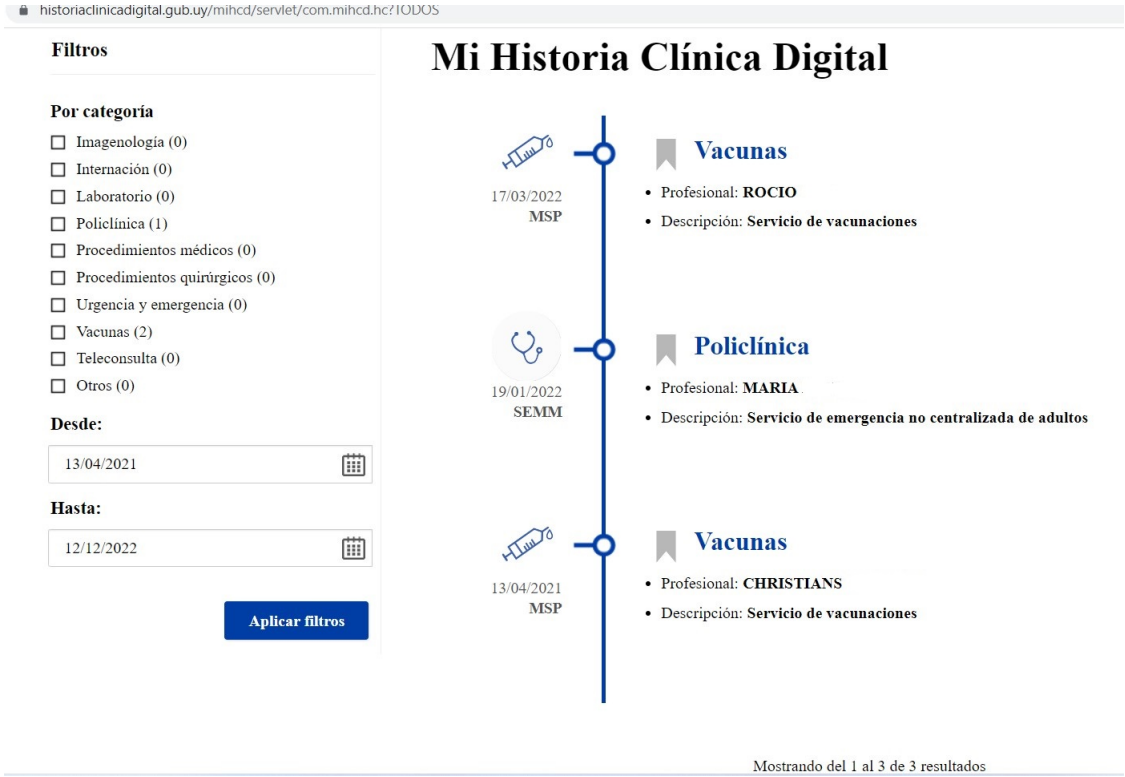

Figura 2.13: Pantalla principal del sistema en línea [39]

En este caso es la primera vez que el usuario ingresa a la plataforma de Accesos, se puede ver en la Figura 2.14 que se crea un registro asociado a dicho evento.

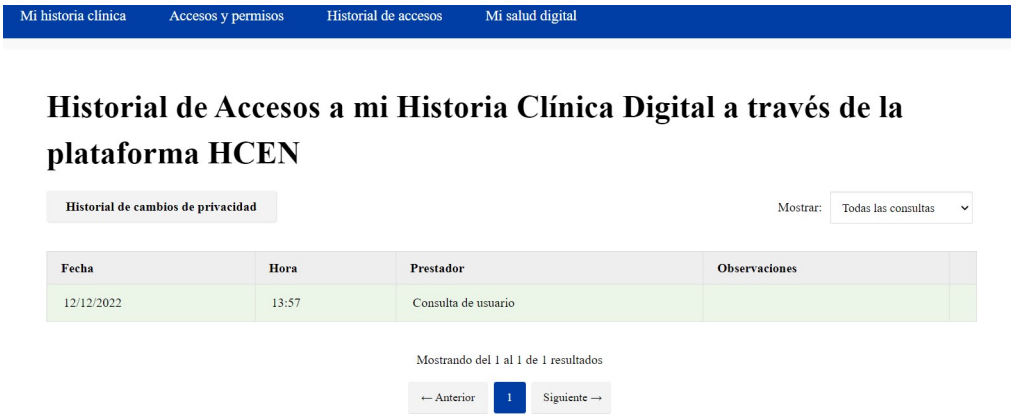

Figura 2.14: Pantalla de accesos [39]

A continuación se ingresa a la configuración de privacidad de la plataforma. Dentro de la configuración de acceso parcial de la HCEN, se ven los campos de selección correspondientes, como muestra Figura 2.15

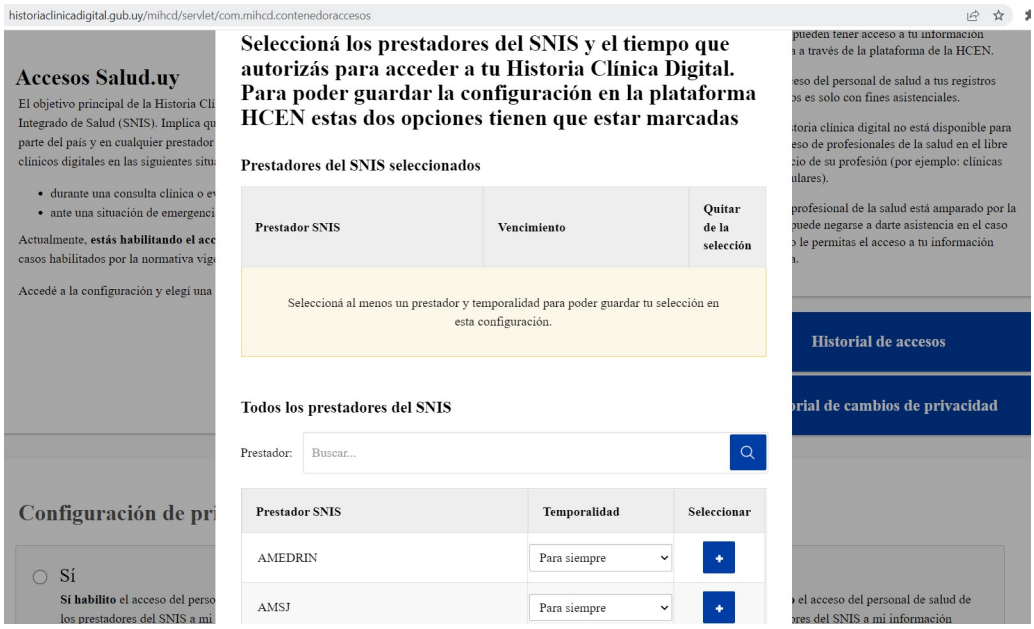

Figura 2.15: Pantalla de configuración de privacidad [39]

En la parte superior de la ventana emergente se listan los Prestadores de salud configurados y en la parte inferior se listan todos los prestadores de salud

asociados al SNIS elegibles para configuración de privacidad.

2.3. Historia Clínica Electrónica en Otros Países

Esta sección presenta los resultados de un relevamiento de iniciativas de la HCE en otros países, con foco en la privacidad de datos. Este relevamiento tuvo como objetivo conocer iniciativas vinculadas a la presente tesis así como aportes que pudieran brindar a este trabajo. En este contexto, destacamos a la iniciativa Red Americana de Cooperación sobre Salud Electrónica (RACSEL) [40], cuyo detalle se presenta en el Apéndice 1, dado que brindó insumos importantes para esta sección.

2.3.1. Descripción del relevamiento

El relevamiento se realizó para varios países de América Latina y de la Unión Europea. Para acotar el análisis se hizo foco en un subconjunto de países, en particular Argentina, Chile, Colombia, Costa Rica, Perú y Reino Unido.

Dicho relevamiento se desarrolló entre los meses de febrero y mayo aproximadamente del año 2020.

Una vez definidos los países a considerar en el estudio, se realizó la búsqueda de documentación a partir del año 2010 en adelante, tanto en idioma español como inglés, filtrando por lo que a nuestro saber era información fidedigna, tanto en su formato de contenido, el desarrollo de la información, su tipo de exposición, la seriedad de la publicación, la forma de redacción, entre otros. No fueron tomados en cuenta formatos blogs o similares.

Los portales de búsqueda tenidos en cuenta fueron aquellos donde es fehaciente el desarrollo del tema salud, seleccionando artículos técnicos y académicos, como también portales específicos de Instituciones de salud y análisis de Profesionales en la salud que exponen sus trabajos a la comunidad.

Las palabras claves de búsqueda realizadas en Google, fueron:

- (+ privacy + “privacy electronic health record” + ehr)
- (“privacy and electronic health record” + consent)

- (privacy + ehr + consent)
- Combinaciones de las anteriores + nombre del país seleccionado. Esta búsqueda permitió hacer foco por país y así, desarrollar cada uno de los apartados específicos.
- (+ privacy + "privacy electronic health record" + ehr + European Union)
- ("privacy and electronic health record" + consent + European Union)
- (privacy + ehr + consent + European Union)

La búsqueda dio como resultado los siguientes trabajos para cada país que se exponen en la Tabla 2.1:

Tabla 2.1: Resultados de trabajos seleccionados por país

País	**Trabajos seleccionados**
Argentina	[41] [42] [43] [44] [45] [46] [47]
Chile	[48] [49] [50] [51] [52] [53] [54] [55] [56]
Colombia	[57] [58] [59] [60] [61]
Costa Rica	[40] [62] [63] [64] [65] [66]
Perú	[67] [15] [68] [69] [70] [71]
Reino Unido	[72] [73] [55] [74] [75]

2.3.2. Detalles del relevamiento

En esta sección se analizan aspectos de los trabajos relevantes seleccionados para la presente tesis:

1. Avance de la HCE: Refiere al grado de avance de la HCE a nivel país.
2. Normativa y Privacidad: Refiere a la legislación sobre la cual se basa la HCE, haciendo foco en la privacidad de datos.
3. Intercambio entre prestadores: Una mirada de cómo está actualmente la interoperabilidad entre prestadores de salud.
4. Estado de informatización actual: Refiere al grado de avance relativo a la informatización de la HCE.
5. Solución a la HCE: Refiere a cómo se implementa la HCE a nivel país.

6. Intercambio de información en HCE: Refiere a los mecanismos a ejecutar para lograr el intercambio de la información de la HCE entre prestadores de salud.

7. Gestión de privacidad: Refiere a los mecanismos para gestionar la privacidad de datos de la HCE.

A continuación se presenta un análisis resumido de los aspectos mencionados.

2.3.2.1. Descripción general del avance de la HCE

De acuerdo a los trabajos seleccionados, Uruguay refleja un gran avance al respecto. Se entiende así porque es el que tiene más información pública disponible y eso permite hacer esta valoración.

Se observó que Chile recién en su agenda digital del año 2020 trató fuertemente el área de salud con exclusividad en la HCE, lo que hace pensar que no tiene el mismo grado de avance como lo tiene Uruguay a la misma fecha, pero sin poder afirmar qué tan avanzado o retrasado está en este punto [52] [48]. Para Argentina sin embargo, se pudo conocer que para el año 2019 la intención fue integrar hospitales, centros de diagnósticos por imagen y laboratorios a la HCE [46].

Colombia, para el año 2020 contaría con un único sistema o herramienta digital que gestione la documentación e información de los usuarios del sistema de salud en el país [58]. A su vez, han establecido que la HCE sería de obligatoria aplicación para fines del año 2013 [61].

Sobre Costa Rica no se ha encontrado información que permita conocer con precisión qué nivel de avance tienen con la HCE a nivel país. Pero si se dio a conocer la creación de la Ley EDUS (Expediente Digital Único en Salud) para generar un ámbito y establecer mecanismos de acción requeridos para digitalizar las historias clínicas desde una perspectiva país. Es de orden público y es de aplicación obligatoria en todos los procesos de desarrollo, implementación y uso del expediente electrónico único en salud [63].

En Perú se pudo conocer su plan de acción. Sobre el año 2021 proyectó un 70 % de implementación de la HCE a nivel nacional. Reino Unido estimó que sobre el año 2020 pondría en marcha los servicios de salud electrónicos, siempre y cuando los diferentes países que lo componen alcanzaran con éxito

la implantación y extensión de los servicios de HCE [68].

No se ha encontrado información relevante de los otros países para poder destacar o mencionar más fehacientemente que incorporaron los cambios y procesos para lograr un avance tal de la HCE como se ha visto en Uruguay.

2.3.2.2. Normativa y Privacidad

De acuerdo a los trabajos seleccionados, tanto Uruguay como Argentina fueron los países que más detallaron de forma pública la normativa aplicada a las HCE, conformando un compendio amplio de leyes y regulaciones. Puede especularse que no todo fue expuesto en los trabajos recogidos para el desarrollo del presente estudio, pero fueron lo suficiente para dar una noción sobre las normas que se utilizan [45] [38].

Chile comprende un conjunto de leyes y normativas bien detalladas en las cuales se basa la HCE [50] [51] [53].

En Colombia se menciona que tienen historia clínica electrónica interoperable gracias a la aprobación en el Congreso de la Ley 2015 del 31 de enero, facilitando y garantizando el acceso y ejercicio de los derechos a la salud y a la información de las personas, respetando el Hábeas Data y la reserva de la misma [57].

En Costa Rica se maneja un marco regulatorio que delinea al proyecto del Expediente Electrónico con apoyo en la ley 9162 del Expediente Digital Único de Salud, creando un único expediente digital en salud en beneficio de todas las personas [63].

En Perú se ha creado el Registro Nacional de Historias Clínicas Electrónicas que tuvo como fin principal establecer los objetivos, administración, organización, implementación, confidencialidad y accesibilidad de la misma [70],

En tanto en Reino Unido, se consideran las normativas locales de cada país que lo conforma. Se definieron principios para proteger al ciudadano en su movilidad dentro del Reino Unido sin omitirle asistencia, siendo cada país responsable de su sistema de salud como también, de sus garantías. En general todos los países del estudio cuentan con respaldo legal para la aplicación e interoperabilidad de la HCE [55].

En líneas generales todos los países tienen claro que deben tratar fuertemente la privacidad apoyándose no solo en la normativa vigente y establecida en su país, sino también en las TIC's para lograr tal fin, estableciendo meca-

nismos para facilitarlo. Reino Unido a pesar de los esfuerzos que realiza para tener una legislación en común y que la privacidad se apoye en ésta, a la hora de la definición de intercambio de información surgen conflictos entre las legislaciones de los diferentes países que la componen, limitándose o en algunos casos obligando a ejecutar acciones específicas para solventarlo. En los demás países que componen el estudio: Argentina, Chile, Colombia, Costa Rica y Perú, independientemente de si la implementación está avanzada o no, tienen claro que es requerido el tratamiento específico de los datos sensibles que corresponden a los ciudadanos. A su vez, se apunta a que una vez implantada la HCE el paciente pueda ser dueño de dictaminar qué datos son los que desea compartir y con quién [55].

2.3.2.3. Intercambio entre Prestadores

De acuerdo a los trabajos seleccionados, los países que componen el estudio contemplan hacia dónde deben apuntar con el intercambio de HCE entre Prestadores de salud, teniendo en cuenta que es crucial para brindar un servicio completo a nivel país a sus ciudadanos, siendo un gran desafío la estandarización e interoperabilidad. Para ello se necesita una arquitectura muy bien diseñada para soportarlo, contemplando la seguridad a nivel de información e intercambio [47] [56] [58] [65] [69].

No se ha encontrado información relevante de los países analizados para poder mencionar más fehacientemente si tienen implementado o aún no, el intercambio a nivel país entre todos los prestadores de salud de la HCE.

Sin embargo, la Unión Europea ejecuta el intercambio transfronterizo de la HCE basándose en la directiva común de protección de datos, para lo cual las TIC's establecen mecanismos para facilitarlo [55].

2.3.2.4. Estado de informatización actual

En Argentina, si bien todas las organizaciones tienen algún grado de informatización, la implementación de la HCE es más lenta de lo deseable debido a que no existe una legislación que oriente la implementación de los proyectos. A esto, hay que sumar barreras estructurales y técnicas, así como dificultades financieras [45].

De acuerdo a los trabajos seleccionados, Colombia por un tema de conectividad y falta de recursos económicos no ha podido digitalizar la historia clínica

en todo el país, sin embargo, en junio del año 2019 se aprobó una ley para reducir la brecha digital. El Gobierno Nacional no puede financiar toda la HCE porque éstas se diseñan según los requerimientos de cada Prestador de salud dado que los servicios prestados no son homogéneos y dependen de la demanda poblacional [61].

En Perú, en base a la información recabada, no se detalla de forma explícita un caso de éxito, pero tampoco, se niega su existencia, lo cual no permite conocer qué tan avanzado están en este punto [69]. En Chile y Costa Rica, en mayor o menor medida cuentan con casos de éxito en la HCE.

2.3.2.5. Solución a la HCE

De acuerdo a los trabajos seleccionados, Colombia presenta dificultades para su implementación ya que por razones de costos no llegan a sostener la implementación de la HCE, incluso algunos Prestadores de salud se les hace insostenible afrontar dichos costos [61].

En Chile se pudo conocer que existen diversas plataformas inteligentes capaces de cruzar datos por medio de algoritmos, como ser TrakeCare y Rayen Salud que son definidos de acuerdo a la información que vayan ingresando los funcionarios de los centros médicos. A su vez permiten el almacenamiento de información de manera interoperable, es decir, pueden leer los distintos formatos que manejan las instituciones de salud, pudiendo ser públicos o privados. Los profesionales sanitarios ingresan la información del paciente de acuerdo al tipo de atención [52] [48].

Las autoridades de Costa Rica implementaron el 28 de setiembre de 2018 en los veintinueve hospitales del país el expediente médico digital, una plataforma tecnológica que permitirá una mejor atención, la modernización de los servicios y fácil acceso de los usuarios a su información médica [64].

En Perú, el marco legislativo del RENHICE planteó tener centralizada la historia clínica de los pacientes. Por ello RENHICE ha estudiado que lo más conveniente es trabajar con un modelo de arquitectura de interoperabilidad semi centralizado. Este modelo permite que un ciudadano pueda tener disponible su historia clínica básica sin importar el lugar en donde se encuentre. Además, funciona bien con la situación del país donde tiene centros de salud organizados jerárquicamente y distribuidos por regiones. Bajo este modelo de interoperabilidad, el RENHICE como entidad, expone a los centros de salud afiliados un

servicio para que puedan acceder a las historias clínicas compartidas [69].

Tanto en la Unión Europea como Uruguay y Argentina permiten conocer que ya están implementando la solución de la HCE y su implantación en determinados Prestadores de salud [74] [47] [38].

2.3.2.6. Intercambio de información en HCE

Como se pudo saber de los trabajos seleccionados, Argentina cuenta con la Red Nacional de Interoperabilidad en Salud que provee un Bus de Interoperabilidad que articula la comunicación entre nodos, permitiendo ser una herramienta para la integración de los sistemas de información en todas las jurisdicciones y sectores del sistema de salud del país, abarcando a los Prestadores de salud públicos y privados. El Bus de Interoperabilidad está basado en los estándares recomendados por la Secretaría de Gobierno de Salud del Ministerio: SNOMED, HL7 y CIE-10/CIE-11 [47].

En Chile se pudo conocer que existen diversas plataformas inteligentes capaces de cruzar datos por medio de algoritmos, como ser TrakeCare y Rayen Salud [52] [48]. Sin embargo, no se ha encontrado información en el trabajo seleccionado para conocer con mayor certeza qué tipo de mecanismos utilizan para lograr el intercambio dichas plataformas.

Si bien Colombia se vio que aún no cuenta con la HCE implementada en Prestadores de salud tiene presente los pasos a seguir para lograr el intercambio de información. No se pudo obtener más información al respecto sobre los mecanismos posibles a utilizar para el intercambio de HCE entre Prestadores [61] [59].

En Costa Rica, Sinirube es una plataforma que debe integrar los datos de todos los ciudadanos. Con la vinculación de esta plataforma con el EDUS, se fortalecerá el enfoque biológico y social de los usuarios del sistema de seguro social. En el trabajo seleccionado no se pudo obtener información certera sobre los mecanismos para el intercambio que utiliza [65][66].

Con respecto a Perú, se plantea para la HCE la creación de un directorio de centros de salud a nivel nacional y tener centralizada la historia clínica de los pacientes; por ello se ha estudiado que lo más conveniente es trabajar con un modelo de arquitectura de interoperabilidad semi centralizado. Este modelo permitirá que un ciudadano pueda tener disponible su historia clínica básica sin importar el lugar en donde se encuentre. No se ha podido obtener información

concreta sobre los mecanismos de intercambio de HCE entre Prestadores en el trabajo seleccionado para poder conocerlos [69].

Por otra parte, Reino Unido que si bien ya tiene implementaciones realizadas sobre el intercambio de información de las HCE, se enfrenta a una dificultad la cual debe vencer día a día con el intercambio de datos a nivel internacional con los países que lo componen. Dicho esfuerzo se enfoca principalmente en que la semántica sea interpretada de igual manera en todos sus países ya que está fuertemente ligado con la protección de datos a nivel legal y normativo en cada país, teniendo sus características particulares. Sin embargo, no se ha podido obtener información precisa sobre los mecanismos para el intercambio de HCE que utilizan [55].

2.3.2.7. Gestión de privacidad

En Argentina, en base al trabajo seleccionado, se pudo conocer que los datos de pacientes están contenidos dentro de lo que se denominan datos sensibles. Por este motivo, se debe tener especial consideración y cuidado teniendo en cuenta tres aspectos importantes: confidencialidad, privacidad y seguridad. La seguridad se enfoca en procesos y controles que resguarda la información de posibles daños, garantizando la confidencialidad y evitando la vulnerabilidad de la privacidad [44].

De acuerdo a los trabajos seleccionados, en Chile se pudo conocer que *"es necesario tener una política nacional de ciberseguridad, que impulse la creación de un marco donde los datos del paciente estén resguardados, sin temores de hackeos o fugas"* [54].

En Colombia, la gestión de la información relativa a la salud de los ciudadanos constituye un aspecto fundamental para la efectiva prestación del servicio de salud y mejora el acceso a los servicios médicos en el menor tiempo posible. Debido a la multiplicidad de actores que participan en el Sistema de Salud Colombiano, se hace necesario el intercambio de información del paciente, garantizando la efectiva prestación del servicio con el uso de Big Data [76].

Costa Rica entiende que toda información contenida en el expediente digital único de salud se considera privada, ya que contiene datos sensibles y como tal se deberán adoptar medidas de índole técnica para garantizar la seguridad de los datos. Dichas medidas deben incluir al menos, la seguridad física y lógica más adecuada para garantizar la protección de la información almacenada [63].

En base al trabajo seleccionado, en Perú en cuanto a seguridad en el acceso a los datos de las HCE, se busca garantizar la identificación de los pacientes con un código único para los ciudadanos dentro del país como es el DNI electrónico. Para garantizar la privacidad de los datos de los pacientes utilizan diferentes métodos y técnicas, entre las que se destacan: encriptación, anonimización y pseudonimización [69].

En Reino Unido, la seguridad de los datos no se logra únicamente con las TIC's adecuadas, sino que también exige la existencia de adecuadas normas internas de organización. Ofrecen al personal de salud formación y educación adecuadas sobre la seguridad de los datos, ya que también es un elemento importante de las precauciones de seguridad efectivas que deben adoptarse, como también los ensayos de penetración y los sellos de calidad [75].

En general los países analizados deben garantizar mediante mecanismos precisos la privacidad de los datos sensibles a nivel salud de sus ciudadanos, tanto en su Prestador de salud como en el intercambio con otros prestadores. Tienen el conocimiento que si la privacidad no se resuelve de forma adecuada pueden ocasionar que la información de los pacientes se revele, provocando un grave perjuicio para ellos.

2.3.3. Resumen y Conclusiones

Como se puede observar en el resumen comparativo expuesto anteriormente, el avance en los países analizados es heterogéneo pero sin mucho soporte en privacidad. Se destaca Uruguay en la disponibilidad de información pública vinculada a la HCEN.

El relevamiento aportó a esta tesis para un mayor entendimiento de la temática, pero no se identificaron soluciones que se pudieran aprovechar para este trabajo.

2.4. Trabajo relacionado

En esta sección se analizan trabajos relacionados a la tesis, que abordan temas de privacidad en el área de la salud en base a BPPC, XACML y pseudoanonimización. Además, se analiza lo propuesto por dos tesis de grado de la Facultad de Ingeniería, que se enfocan en estos aspectos en el contexto uruguayo.

Con respecto a trabajos basados en BPPC, en [8] se aborda la problemática de la falta de un mecanismo para que los pacientes habiliten el consentimiento para acceder a partes de su HCE. Sólo está permitido el consentimiento de acceso total a la HCE. Frente a esta situación, [8] propone utilizar el perfil BPPC y el estándar HL7 para desarrollar políticas de privacidad y mecanismos de protección para la HCE del paciente. En [77] proponen una solución similar para la creación y gestión del consentimiento del paciente basándose en el perfil BPPC y el estándar HL7. Con esto, el paciente puede: habilitar la opción de permitir acceder a todo o nada, sobre algunos informes, quién accederá, con qué propósito y un período de tiempo configurable desde-hasta. Otros trabajos basados en BPPC proponen soluciones similares [30] [32] [78] [7]. En comparación con nuestra propuesta de tesis, nuestro trabajo no utiliza BPPC sino que se basa en XACML que es lo utilizado en la Plataforma Salud.uy, agregando además la especificación formal con FACPL. Por lo cual, esta propuesta de tesis permite habilitar el consentimiento para partes de la HCE, para qué especialidad y, específicamente, para qué especialista, por un lapso de tiempo determinado, y a qué Instituciones de salud (integrales y parciales, públicos/privados) pertenecientes al sistema.

Con respecto a trabajos basados en XACML, en [30] se propone una arquitectura para el flujo del manejo de consentimientos que permite almacenar los mismos con formato XACML en una base de datos. De esta manera se manejan las solicitudes de consentimientos con un nivel de granularidad arbitrario, siendo evaluadas con XACML. En comparación con esta propuesta de tesis, se propuso de igual manera el manejo de consentimiento con el uso de políticas XACML, permitiendo especificar políticas de privacidad con más granularidad (p. ej. partes de la HCE) considerando a su vez aspectos temporales.

Con respecto a trabajos basados en seudonimización, en [79] se propone una metodología para la seudonimización de datos médicos que almacena datos de salud desvinculados de la información de identificación del paciente correspondiente, brindando una solución para la privacidad de los datos. En comparación, nuestra propuesta de tesis no utiliza seudonimización, sino que propone el uso de políticas XACML que permite decidir sobre el acceso a un recurso, para una petición de acceso. Por más detalles de este trabajo relacionado ver el Apéndice 3.

Además, existen algunos trabajos de fin de carrera de la Universidad de la República centrados en privacidad en el área de la salud en el contexto uruguayo. En particular [80] propone una solución para crear los consentimientos digitales de los pacientes en un formato estándar que debe tener una HCE, para la interoperabilidad entre sistemas. En dichos consentimientos incluyen referencias a políticas de privacidad seleccionadas por los pacientes, las cuales fueron definidas utilizando el estándar XACML y el perfil BPPC. En comparación con esta propuesta de tesis, se propuso de igual manera el manejo de consentimiento con el uso de políticas XACML, permitiendo especificar políticas de privacidad con más granularidad (p. ej. partes de la HCE) considerando a su vez aspectos temporales.

Por otro lado, en [81] la integración e interoperabilidad de sistemas en el área de la salud todavía se dificulta, debido a que no todas las organizaciones cuentan con sistemas de apoyo de atención en salud adheridos a estándares o buenas prácticas. Este trabajo hace mención a Salud.uy y comenta que si bien ha sido un avance importante, quedan aún varios problemas por resolver como por ejemplo, lograr la integración y compatibilidad de la Plataforma de Gobierno Electrónico (PGE) con los estándares y buenas prácticas más utilizados en el área de la salud a nivel mundial. A su vez, abordó la seguridad e interoperabilidad en el área de salud en el contexto uruguayo. Para realizar el control de acceso utilizaron XACML y el conjunto de políticas será definido por la comunidad de Uruguay. A su vez, para los consentimientos informados de los pacientes, se menciona que fue utilizado el perfil BPPC. En comparación con nuestra propuesta de tesis, se propuso una extensión a la actual Plataforma Salud.uy por lo cual es un avance en este sentido ya que se toma como punto de partida una plataforma integrada y compatible con PGE, estándares y buenas prácticas en la salud. También abordó de igual manera el manejo de consentimiento con el uso de políticas XACML, permitiendo especificar políticas de privacidad con más granularidad.

2.4.1. Resumen Trabajo Relacionado

De acuerdo a lo analizado en los trabajos relacionados, se entiende que las políticas de privacidad refieren a una única Institución de salud. La propuesta de tesis no se centra en una única Institución, sino en las Instituciones de salud pertencientes al sistema, como también políticas para el intercambio de datos

clínicos entre éstas (p. ej. cuando un profesional en salud quiere acceder a datos de salud de un paciente que fueron generados en otra Institución de salud). Cabe destacar que esta propuesta de tesis no aborda políticas de consentimientos dentro de una Institución de salud. Además, los trabajos relacionados vistos se centran en la especificación de políticas de privacidad, mientras que en nuestra propuesta de tesis se identifican requerimientos más amplios (p. ej. capacitación, privacidad, auditoría) y para distintos actores (p. ej. pacientes, profesionales en salud, otros).

En la propuesta de tesis se propone una operativa de definición de consentimientos más granular (p. ej. por partes de la HCEN, especialidad, especialista, período de tiempo) permitiendo así que el paciente tenga mayor control sobre sus datos en salud. También cuenta con la posibilidad de delegar el manejo de su HCEN a una persona de su confianza (tutor), opción que no se ha encontrado en trabajos seleccionados para la elaboración de la presente tesis.

A nuestro leal saber y entender consideramos que no se ha desarrollado una solución similar a esta propuesta de tesis, en un contexto interorganizacional, que: i) brinde el nivel de granularidad para la configuración de consentimientos del paciente sobre su HCE, ii) que estos consentimientos sean perdurables en el tiempo y configurables para el intercambio de datos clínicos entre Instituciones de salud (integrales y parciales, públicas/privadas), y iii) que contemple la diversidad de actores y requerimientos definidos para cada uno.

Capítulo 3

Análisis de la problemática

En este capítulo se identifican actores y requerimientos asociados, que se considerarán para abordar la problemática planteada en esta tesis.

La Sección 3.1 describe las fuentes de análisis utilizadas para identificar tanto a los potenciales actores como los requerimientos asociados a cada uno de ellos. La Sección 3.2 desarrolla la identificación y descripción de los potenciales actores. La sección 3.3 identifica y desarrolla los requerimientos asociados a cada uno de los actores identificados. La Sección 3.4 identifica otras líneas de trabajo posibles.

3.1. Fuentes de análisis

Esta sección describe las fuentes de análisis utilizadas para identificar tanto a los actores como los requerimientos correspondientes a cada uno de ellos, como se visualiza en la Figura 3.1.

Figura 3.1: Fuentes de análisis.

A partir de lo analizado en el Capítulo 2, se llega a conformar una idea global de la situación actual en la que se encuentra la HCE a nivel nacional e internacional.

La experiencia personal y profesional tanto de la tutora como de la autora de la presente tesis, en el área informática y laboral, y experiencias personales brindaron buenas fuentes de referencia. Se realizó también una encuesta a usuarios que hacen uso del sistema de salud, en base a un cuestionario anónimo (Sección 5.2 del Capítulo 5).

A su vez, se encuestó brevemente a diferentes personas cuyo rol laboral se encuentra dentro del ámbito de la salud, que aportaron su experiencia en el día a día, como también personas involucradas en el área legal (Sección 3.4.2 del Capítulo 3).

Fue de gran aporte la instancia de validación con personal de la Plataforma Salud.uy, que permitió retroalimentar cada uno de los requerimientos y actores definidos en el presente capítulo.

Gracias al desarrollo del trabajo relacionado y HCE en otros países (Sección 2.4 del Capítulo 2), se pudo conocer la realidad desde la óptica del usuario de la salud, las limitaciones y necesidades actuales sobre sus datos e información clínica, permitiendo identificar potenciales requerimientos, que serán de aporte en la solución propuesta y extensión de la actual Plataforma Salud.uy.

Con estos insumos, se elaboraron requerimientos los cuales se dividieron en categorías: capacitación, privacidad y auditoría.

3.2. Identificación de actores

Cuando se habla de actor se hace referencia a aquella entidad externa que interactúa con el sistema.

En la Tabla 3.1 se presentan y describen los actores que se identificaron al analizar la problemática planteada, para los cuales se deberían abordar requerimientos de privacidad de datos en el contexto de la Plataforma Salud.uy.

Tabla 3.1: Actores

Actor	**Descripción**
Prestador de salud	Institución parcial o integral que brinda servicios de salud.
Paciente	Persona que hace uso de los servicios de salud de Uruguay.
Profesional de la salud	Profesional que trabaja en prestadores de salud.
Técnico en salud	Persona que trabaja en Prestadores de salud, con tareas diferentes a las del profesional en salud (p. ej. nurse, enfermeros, radiólogos, entre otros).
Especialista en privacidad	Profesional informático que trabaja en Salud.uy, dedicado a temas vinculados a la privacidad de datos en HCEN.

3.3. Identificación de requerimientos

Definidos los actores, se profundiza en la identificación de los requerimientos orientados a la privacidad de datos. La nomenclatura de la identificación de los requerimientos y su descripción se visualiza en Tabla 3.2

Tabla 3.2: Identificación y descripción de los requerimientos

Codificación	**Descripción**
AD	Auditoría
CP	Capacitación
HB	Privacidad (habilitación y revocación)

3.3.1. Auditoría

Este requerimiento refiere al registro, visualización y notificación de eventos sobre la HCEN de un paciente.

Surge principalmente del análisis con la tutora y entrevistas realizadas, como también experiencia personal y profesional de la autora de la presente tesis. A su vez, se apoya en los trabajos relacionados [36] [37].

AD01. Auditoría para conocer quién y cuándo se accedió al historial médico y a qué parte precisamente. Cuando este acceso ocurre, se debe generar una notificación relacionada **Actor**: Paciente.

3.3.2. Capacitación

Este requerimiento refiere a la capacitación para pacientes. Surge principalmente de los trabajos relacionados [64] [36] [37] y experiencia de familiares. El requerimiento que se identificó es el siguiente.

CP01. Desde la plataforma brindar capacitación para pacientes en cuanto a formación sobre seguridad y privacidad para evitar en lo posible, exponer información sensible. **Actor**: Paciente.

3.3.3. Privacidad

Estos requerimientos refieren a la habilitación y revocación de permisos sobre la HCEN de un paciente hacia un Prestador de salud como puede ser también a un determinado profesional de la salud, en su máxima granularidad posible.

El compendio de requerimientos identificados surgen principalmente de los trabajos relacionados [43] [44], análisis con la tutora y entrevistas realizadas, como también experiencia personal y profesional de la autora de la presente tesis.

HB01. Configuración de permisos para acceder a datos clínicos de los pacientes. Esta configuración se debe poder realizar a nivel granular de quién y cuándo accede a la HCEN, sea un determinado Prestador de salud, especialidad y/o especialista. **Actor**: Paciente.

HB02. Configuración de permisos a un tutor (persona de confianza) para acceder a la HCEN del paciente. **Actor**: Paciente.

HB03. Configuración de permisos sobre la HCEN, en momento posterior al fallecimiento del paciente, al tutor para que tome el control de la HCEN.

Actor: Paciente.

HB04. Configuración de permisos para disponibilizar la HCEN de un paciente ya fallecido, de forma total o parcial, a un Prestador de salud para ser aporte a la medicina. Se puede habilitar el acceso por una determinada cantidad de años. **Actor**: Paciente.

HB05. Configuración de permisos a otro profesional con el consentimiento previo del paciente. **Actor**: Profesional de la salud.

HB06. Configuración de políticas de acceso para permitir acceder a la HCEN de un paciente en situaciones *breaking the glass* (ocurre bajo un evento asistencial de emergencia). **Actor**: Especialista en Privacidad.

3.3.4. Detalles adicionales de requerimientos

Se sugiere que los Prestadores de salud tengan la posibilidad de brindar capacitación a los pacientes sobre seguridad de los datos y cómo se comparte la HCEN. La idea principal es desarrollar una plataforma de capacitación para que todos los usuarios de salud puedan informarse y entender el procedimiento para configurar los permisos granulares sobre su HCEN.

Los requerimientos codificados como HB hacen foco en la habilitación, configuración y/o revocación sobre privacidad, es decir, en la configuración de privacidad.

Las notificaciones que visualicen los pacientes deben ser en un formato y lenguaje claro, conciso, no ambiguo. Se generan siempre y cuando el paciente haya configurado las auditorías (AD01).

3.4. Otras líneas de trabajo

En esta sección se describen otras posibles líneas de trabajo, que si bien se analizaron, quedaron por fuera del alcance de la tesis. Para profundizar en ellas, ver Apéndice 4.

3.4.1. Comunicación transfronteriza

Surge principalmente de los trabajos seleccionados [55] [72] [73] y análisis con la tutora.

En Uruguay hoy en día, no se han encontrado trabajos académicos o científicos que permitan conocer si actualmente se han realizado primeras experiencias sobre la comunicación transfronteriza entre países, como tampoco un caso de éxito al respecto. En este contexto, sería de interés que la Plataforma Salud.uy brindara la posibilidad del soporte para la comunicación transfronteriza, entre Uruguay y países limítrofes, como primer avance.

Entendemos que las principales problemáticas o temas a abordar son los siguientes:

- Un número elevado de personas suele viajar de un país a otro, por temas de su interés, generándose una mayor movilidad en el país destino, con posibilidad de incrementarse la atención médica. De requerirlo, la persona se atiende en un servicio de salud local, pero lo que el médico tratante genere en un archivo clínico en ese momento, sea papel o electrónico, no va a poder adjuntarse a su actual HCE de su país residente.

- Abordar el marco legal de los países con los que Uruguay puede llegar a interoperar con la HCEN.

- Cuando una persona contrate un seguro de viajero, tenga la posibilidad de configurar el consentimiento informado en Instituciones de salud asociadas con su cobertura de seguro, por un tiempo acotado (p. ej. la duración de su viaje).

3.4.2. Acceso Judicial

Para este apartado, se generó una entrevista informal con la doctora en leyes Sandra Dene. Ella explicó que los jueces cuando toman un caso que surge de temas relacionados con la HCEN de una persona, el Juez actualmente no tiene forma de visualizar online la HCEN.

La conversación sostenida con la Dr Dene, permitió conocer el procedimiento actual. El Juez emite una orden judicial para que su cliente le lleve la HCE impresa. Una vez recibida, la estudia, trabaja y una vez emitida la orden judicial del caso, el Juez registra en la carátula de la HCE el nro de siniestro,

retornando a la Institución de salud por medio del dueño.

En este contexto sería de interés que la Plataforma Salud.uy brindara la posibilidad del soporte para la comunicación entre el Poder Judicial y las Instituciones de salud del país, como primer avance.

Algunos ejemplos en los cuales esto podría ser necesario son:

- Existe una investigación penal sobre un paciente de una Institución de Salud;
- En la historia clínica hay datos que pueden incriminar penalmente al paciente, la Justicia solicita el original de esa historia clínica;
- Un Juez solicita la historia clínica por una sentencia en el caso que un menor sea un donante de órganos.

En líneas generales se puede decir que mediante una orden judicial se obtiene una historia clínica de un paciente para ser analizada por la Justicia. El formato en el cual hoy predomina su transporte, es copia en papel de la misma de forma personal.

3.4.3. INDT: Instituto Nacional de Donación y Trasplantes de Célula, Tejidos y Órganos

Otro tema analizado surgió al intercambiar información proveniente de un trasplante de riñón de una pareja allegada a la autora de la presente tesis. Se describe brevemente los trámites que tuvieron que realizar para poder gestionar la donación de órganos.

Para conocer la situación por la cual tuvieron que atravesar, se generó una reunión informal entre la autora del presente documento y la pareja, pidiéndoles contaran brevemente cómo fue la solicitud para la solicitud del trasplante de riñón. Primeramente dicha solicitud se realizó de forma manual, se presentaron en el 4to piso del Hospital de Clínicas y se les entregó una serie de formularios para llenar. A su vez el paciente debió presentar una copia de su historia clínica. Se le solicitó un resumen de la misma con un lapso no mayor a seis meses junto a otra documentación vigente.

En otros casos de trasplantes, el procedimiento es similar, siempre se abre una historia clínica en particular para ese trasplante y se adjunta una serie de formularios y documentación vigente para proceder a la intervención [82].

De lo anteriormente expuesto se desprende que en estos casos se les solicita a los pacientes información clínica que se podría obtener directamente a través de la HCEN:

- Existe un paciente que necesita de un trasplante de órganos, perteneciente a una Institución de salud (pública o privada).
- Puede llegar a ser una situación propensa a la pérdida de información.

Capítulo 4

Solución propuesta

Este capítulo desarrolla la solución propuesta para la incorporación de funcionalidades más avanzadas a la actual Plataforma Salud.uy.

La Sección 4.1 brinda una breve introducción al capítulo. La Sección 4.2 describe el modelo conceptual tomado como base para el presente trabajo para la definición de HCEN. La Sección 4.3 describe qué aspectos se utilizan para definir las políticas y reglas de control de acceso. Entre la Sección 4.4 y la Sección 4.10 se brindan detalles de cómo se abordaron los requerimientos identificados (HB01 a HB06 y AD01).

4.1. Introducción

Esta sección permite conocer dónde se ubican las extensiones propuestas que se desarrollarán en este capítulo. La Figura 4.1 muestra la integración de estas extensiones (solución propuesta) con la actual Plataforma Salud.uy.

Estas extensiones incluyen políticas y reglas más concretas a las que hoy se definen, así como interfaces gráficas para que el paciente pueda tener más control granular sobre su privacidad.

A nivel de la aplicación web actual (Mi Historia Clínica Digital), estas nuevas interfaces gráficas dan soporte a nuevas funcionalidades que permiten extender dicha aplicación web.

A nivel de plataforma, se propone un diseño de políticas que den soporte a ese nivel de granularidad.

Estas extensiones se integrarían por una parte, en la actual aplicación web Mi Historia Clínica Digital (Capítulo 2, Sección 2.2.3.1) ya que desde aquí ella

accedería a las funcionalidades adicionales para que los usuarios interactúen con dicha aplicación. Por otra parte, las extensiones de políticas y reglas para las funcionalidades adicionales de la solución propuesta que integrarían al sistema actual de la Plataforma Salud.uy.

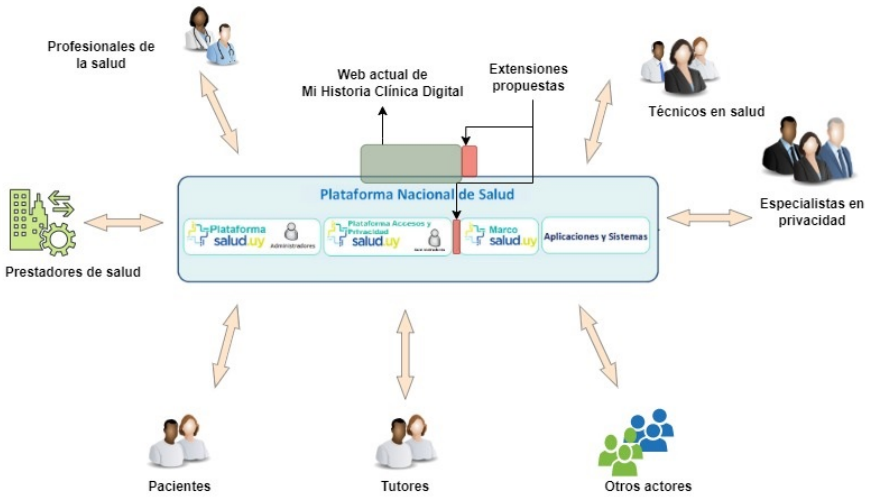

Figura 4.1: Extensiones propuestas al modelo existente de la Plataforma Salud.uy.

4.2. Modelo Conceptual

En la Figura 4.2 se presenta el modelo conceptual resumido de la HCEN tomado como base para la solución propuesta, el cual está inspirado en la estructura real[1].

[1] https://centrodeconocimiento.agesic.gub.uy/documents/207224/425682/Gu%C3%ADa+T%C3%A9cnica+de+Metadatos+XDS+-+Versi%C3%B3n+18.pdf/85111dc2-4f8b-9b9c-3efb-3a8eb6413251

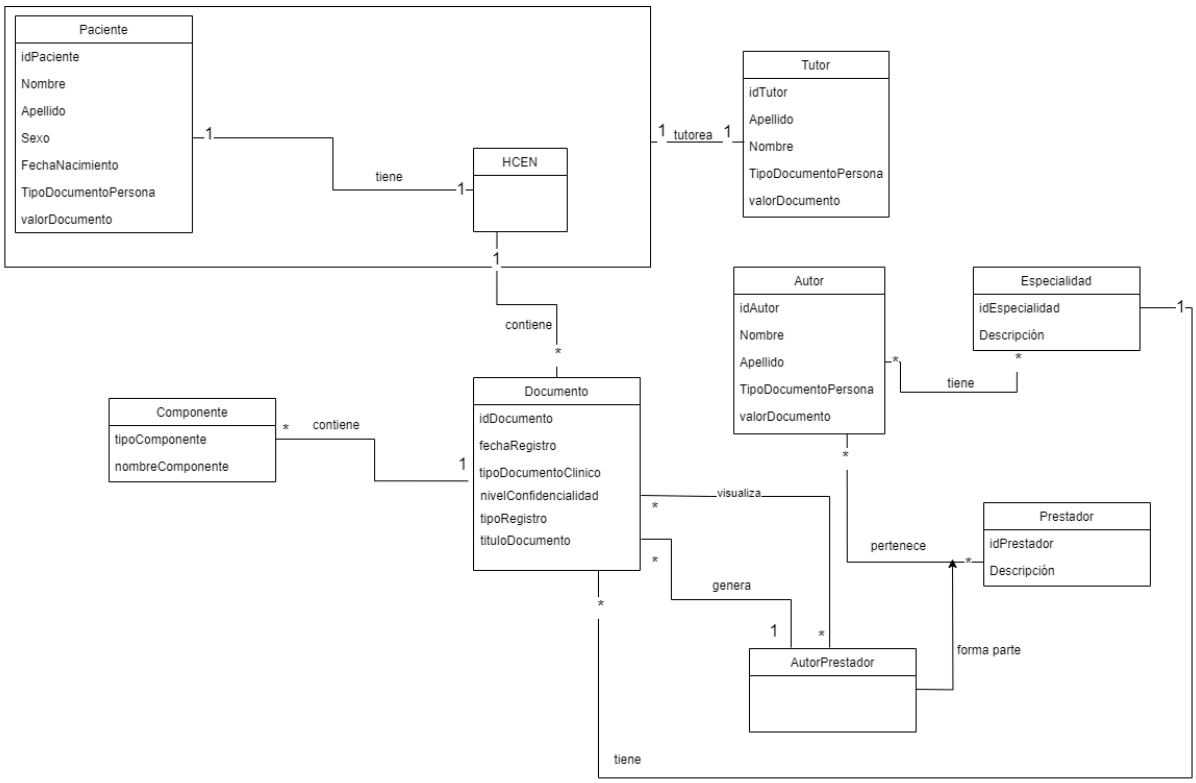

Figura 4.2: Diagrama de clases de la HCEN resumida para la solución propuesta.

Cada entidad HCEN está compuesta por uno o varios documentos y éstos tienen uno o más componentes asociados. A su vez, cada HCEN pertenece a un único paciente y un tutor puede tutorear la HCEN de un determinado paciente. Cada autor (p. ej. profesional de salud) tiene una especialidad médica asociada y éste pertenece a uno o más prestadores de salud. Este autor visualiza y/o genera, según corresponda, uno o más documentos de las HCEN de sus pacientes. A continuación, se detallan los atributos que interesan saber de cada entidad.

Para una mejor visualización, en la Figura 4.3 se presentan los enumerados que forman parte del modelo conceptual presentado anteriormente.

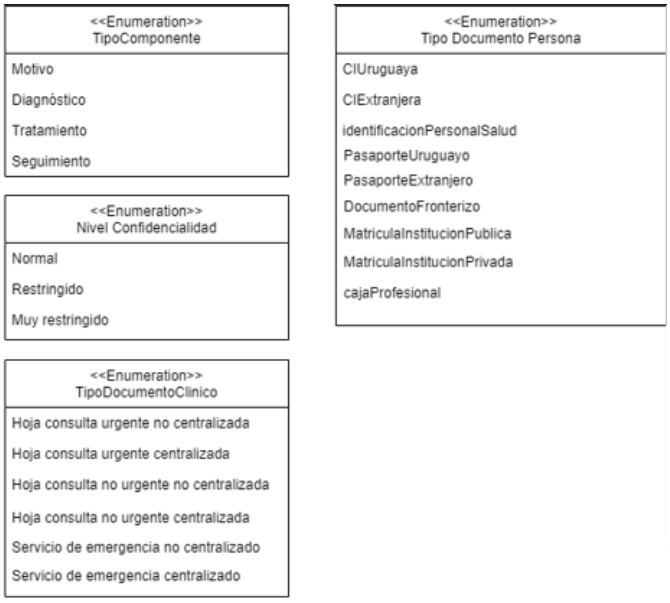

Figura 4.3: Enumerados del Diagrama de clases de la HCEN resumida para la solución propuesta.

Las siguientes tablas describen los atributos que componen el diagrama de clases de la HCEN. Se tomó como base el conocimiento publicado en la Plataforma Salud.uy[1].

Los atributos que interesa tener presente de la entidad de un paciente, se describen en la Tabla 4.1.

Tabla 4.1: Entidad Pacientes

Atributo	**Descripción**
idPaciente	Identificador único del paciente. Con este dato se obtiene toda la información del mismo.
Nombre	Refiere al nombre del paciente.
Apellido	Refiere al apellido del paciente.
Sexo	Refiere al identificador del sexo del paciente.
fechaNacimiento	Refiere a la fecha de nacimiento del paciente.
TipoDocumentoPersona	Refiere al identificador del tipo de documento del paciente.
valorDocumento	Refiere al número de documento del paciente.

Los atributos que interesa tener presente de la entidad de un tutor, se describen en la Tabla 4.2.

[1] https://centroderecursos.agesic.gub.uy/web/arquitectura-salud.uy/inicio/-/wiki/Arquitectura+para+Salud/Arquitectura+de+Datos

Tabla 4.2: Entidad Tutor

Atributo	**Descripción**
idTutor	Identificador único del tutor. Con este dato se obtiene toda la información del mismo.
Nombre	Refiere al nombre del tutor.
Apellido	Refiere al apellido del tutor.
fechaNacimiento	Refiere a la fecha de nacimiento del tutor.
TipoDocumentoPersona	Refiere al identificador del tipo de documento del tutor.
valorDocumento	Refiere al número de documento del tutor.

Los atributos que interesa tener presente de la entidad de un autor, se describen en la Tabla 4.3.

Tabla 4.3: Entidad Autor

Atributo	**Descripción**
idAutor	Identificador único del autor. Con este dato se obtiene toda la información del mismo.
Nombre	Refiere al nombre del autor.
Apellido	Refiere al apellido del autor.
fechaNacimiento	Refiere a la fecha de nacimiento del autor.
TipoDocumentoPersona	Refiere al identificador del tipo de documento del autor.
valorDocumento	Refiere al número de documento del autor.

Los atributos que interesa tener presente de la entidad de un Prestador de salud, se describen en la Tabla 4.4.

Tabla 4.4: Entidad Prestador de Salud

Atributo	**Descripción**
idPrestador	Identificador único del prestador de salud. Con este dato se obtiene toda la información del mismo.
Descripción	Brinda una descripción del prestador.

Los atributos que interesa tener presente de la entidad de una especialidad referente a un profesional de la salud, se describen en la Tabla 4.4.

Tabla 4.5: Entidad Especialidad.

Atributo	Descripción
idEspecialidad	Identificador único de la especialidad médica. Con este dato se obtiene toda la información del mismo.
Descripción	Brinda una descripción de la especialidad.

Los atributos que interesa tener presente de la entidad de un componente del documento de la HCEN, se describen en la Tabla 4.6.

Tabla 4.6: Entidad Componente

Atributo	Descripción
tipoComponente	Identificador del componente del documento que compone una HCEN.
nombreComponente	Refiere al nombre del componente.

Los atributos que interesa tener presente de la entidad documento que forma parte de una HCEN, se describen en la Tabla 4.7.

Tabla 4.7: Entidad Documento

Atributo	Descripción
idDocumento	Identificador único del documento. Con este dato se obtiene toda la información del mismo.
fechaRegistro	Refiere al dato fecha del registro, cuando se genera el documento nuevo en la HCEN.
tipoDocumentoClinico	Tipo de identificador de documento clínico, que se genera en la HCEN del paciente por el profesional de salud (autor).
nivelConfidencialidad	Nivel de protección de confidencialidad para el documento de la HCEN.

Enumerado: Nivel Confidencialidad

La Tabla 4.8 muestra los niveles de confidencialidad definidos por la plataforma Salud.uy, que son los posibles valores que toma el atributo nivelConfidencialidad de la entidad Documento.

Tabla 4.8: Enumerado Nivel Confidencialidad

Código	Descripción
N	Normal
R	Restringido
V	Muy restringido

Las especialidades médicas no se profundizan en detalle su definición ya que

son un gran número. La Figura 4.4 permite visualizar algunas de ellas a modo de ejemplo, extraídas directamente de la página de la Facultad de Medicina.[1]

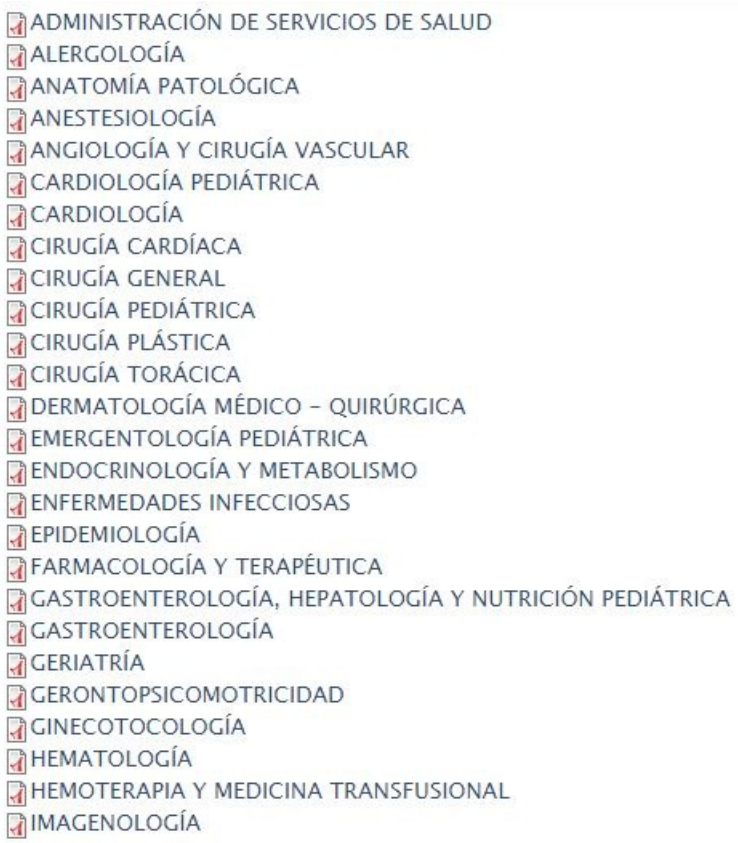

Figura 4.4: Especialidades de referencia de la Facultad de Medicina

4.3. Diseño de Políticas de Control de Acceso

Esta sección describe qué aspectos se utilizan en la presente tesis para definir las políticas y reglas de control de acceso.

En línea con lo que actualmente es utilizado por Salud.uy, las políticas de control de acceso se definen siguiendo el esquema de XACML: resource, subject, action y environment. La definición de estos parámetros permiten configurar las reglas necesarias sobre las políticas a desarrollar.

Resource (sobre qué): Hace referencia a la historia clínica de un paciente. En este trabajo se referencia con hce y se identifica con hce/pacienteId.

[1] http://www.egradu.fmed.edu.uy/programa-postgrados

Subject (quién): Hace referencia a quien quiere accede a la historia clínica de un paciente. En este trabajo se referencia como subject y se identifica como subject/id en el caso de un prestador de salud y subject/autorId en el caso de un profesional de la salud (autor).

Action (para qué): Hace referencia a la acción sobre la que se configura un permiso. En este trabajo solo se maneja permisos READ (actionid).

Environment (entorno): Hace referencia a datos del entorno. En particular, en este trabajo se considera solamente la fecha().

Accesos: Los resultados de un control de acceso pueden ser permitido (Permit) o denegado (Deny).

El diseño de políticas propuesto permite extender lo que actualmente provee Salud.uy de la siguiente forma:

- HCEN Entera
- A nivel documento
- A nivel componente del documento
- A nivel de especialidad de un profesional de salud
- A nivel de profesional de salud

En las secciones restantes del presente capítulo se detallan cómo se aborda cada uno de los requerimientos identificados con la solución propuesta. En particular, para cada requerimiento se describen los siguientes aspectos:

- Interfaz gráfica: Se presenta un posible diseño de interfaz gráfica junto a un breve detalle de su funcionamiento. Sería lo que se extendería de la actual interfaz gráfica de Salud.uy.
- Ejemplo ilustrativo: Se presenta un ejemplo del funcionamiento de la política a desarrollar, en un lenguaje común para su mejor entendimiento.
- Especificación política: Se define la política con parámetros para generalizar y entender su uso. Se realiza con FACPL. Representa lo que se extendería de las políticas actuales que pueden existir en la plataforma Saluy.uy.

Para el diseño de las políticas de control de acceso se asume que el PEP está configurado como deny-biased[1] y que el PDP lo está como deny-overrides[2].

4.4. Requerimiento: HB01

Este requerimiento refiere a que el paciente pueda configurar permisos de acceso sobre sus datos clínicos. En particular, este acceso se puede configurar a nivel granular, en relación a quién y cuándo accede a su HCEN, sea un determinado Prestador de salud, especialidad y/o especialista.

4.4.1. Diseño de Interfaz Gráfica

La Figura 4.5 presenta un posible diseño de interfaz de usuario para abordar este requerimiento. Para mejor comprensión, se presenta con datos de ejemplo.

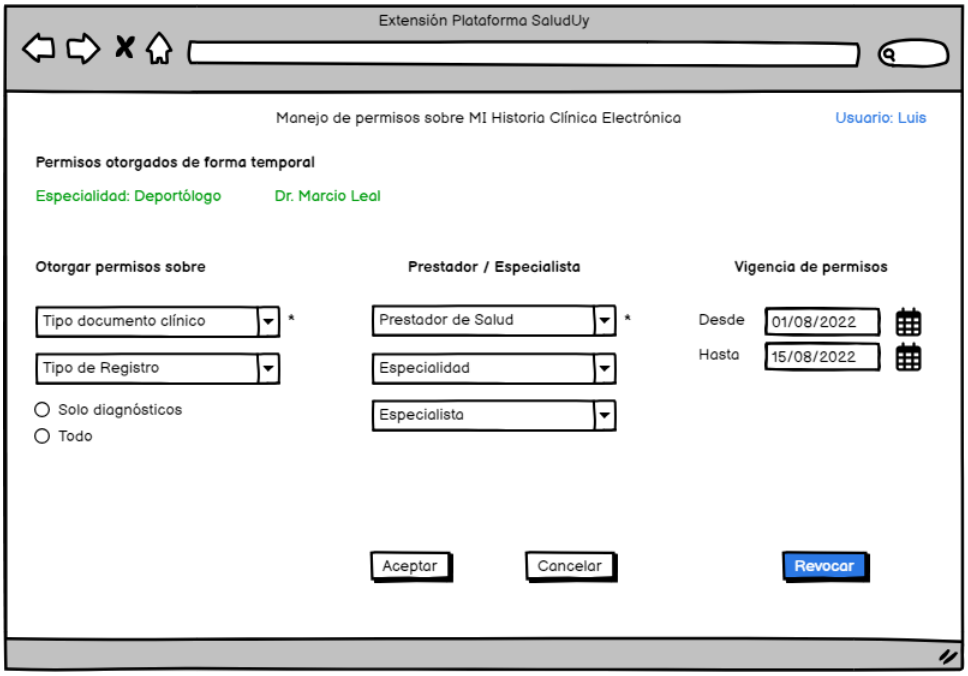

Figura 4.5: Diseño de interfaz gráfica: Requerimiento HB01

En el panel de la izquierda se presenta las opciones posibles sobre las cuales

[1]Si la decisión es *permit* el PEP permite el acceso. Si existen obligaciones asociadas a la decisión, el PEP permite el acceso únicamente si entiende que se cumplieron. En otros casos, no se permite el acceso [28].

[2]Esta configuración está pensada para casos en los que un decisión *deny* debe tener prioridad sobre una *permit* [28].

se puede otorgar permisos. El combo desplegable para el Tipo de documento clínico va a permitir filtrar por el tipo de consulta médica.

Una vez efectuada dicha selección, en el panel central es seleccionable el Prestador, Especialidad y Especialista para asignar permisos. El combo desplegable para selección del Prestador de Salud requiere que se seleccione un valor. Puede no seleccionarse una Especialidad, en este caso se está otorgando permisos a todos los especialistas del Prestador de Salud seleccionado. En el panel derecho, se ingresa el período de vigencia de activación de permisos.

Esta interfaz gráfica permite también eliminar el permiso otorgado, mediante el botón REVOCAR.

4.4.2. Ejemplo Ilustrativo

Un paciente tiene consulta con un médico de medicina general, para realizarse los análisis de rutina en el Británico, donde el paciente no es socio de dicho Prestador de Salud. El médico del Británico tiene la necesidad de visualizar los análisis anteriores para estudiarlos y saber qué estudios y/o análisis le solicitará al paciente.

La Tabla 4.9 muestra los elementos a considerar para diseñar una política que brinde soporte a este requerimiento.

Tabla 4.9: Elementos para política. Requerimiento: HB01

Elemento	**Detalle**
Paciente	Luis
Prestador de Salud	Británico
Especialidad/Especialista	Medicina Gral – Marcio Leal
Vigencia	Fecha Desde - Fecha Hasta

Si Paciente = ‘Luis’ AND PrestadorSalud = ’Británico’ AND Especialidad = ‘Medicina Gral’ AND Especialista = ‘Marcio Leal’ AND vigencia mayor a (’Fecha Desde’) y vigencia menor a (‘Fecha Hasta’) **Permite acceder** Sino **No permite acceder**

4.4.3. Especificación de Política

Se presenta la estructura de política que se define al momento de que el paciente configura las opciones para dar soporte al requerimiento HB01. Cuando se seleccionan todas las opciones en la interfaz gráfica con los elementos mencionados, se genera una política acorde al siguiente plantilla.

Listing 4.1: Especificación de Política FACPL: Req. HB01.

```
1  PolicySet ConfiguracionAccesoPaciente {deny−unless−permit
2    target: equal ("Nombre_Paciente", hce/pacienteid )
3    policies:
4      PolicySet readSpecialistHealth {deny−unless−permit
5
6          target: equal ("read", action/id)
7                          && equal ("Nombre_PrestadorSalud", subject/id)
8                          && equal ("Nombre_Especialidad", hce/titleDocument)
9                          && ( greater−than(datetime/id, "FechaDesde")
10                         && less−than(datetime/id, "FechaHasta"))
11                 policies:
12                   Rule readConfiguracionAccesoPaciente (permit
13                         target: equal ("Nombre_Especialista", subject/autorid)
14                       )
15     }
16 }
```

En la línea 2 se define al paciente para la ejecución de la política. El grupo de líneas de código de 3 a 10 en qué casos aplica la política, en un primer nivel de definición: el tipo de acceso que será READ, el período de tiempo configurado específicamente para permitir acceso, como el Prestador de Salud y la especialidad correspondiente.

El grupo de líneas de código de 11 a 13 define a quién se le permite el acceso, es decir al especialista.

4.5. Requerimiento: HB02

Este requerimiento refiere a que el tutor (persona de confianza del paciente) pueda acceder a la HCEN del paciente.

4.5.1. Diseño de Interfaz Gráfica

La Figura 4.6 presenta un posible diseño de interfaz de usuario para abordar este requerimiento. Para mejor comprensión, se presenta con datos de ejemplo.

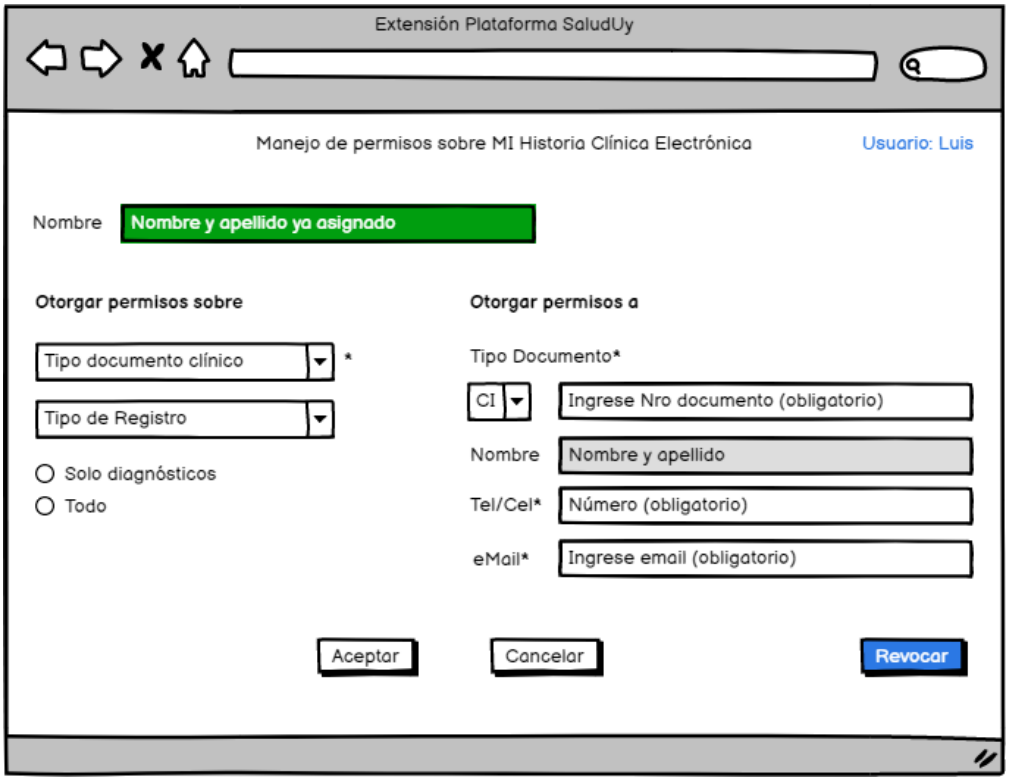

Figura 4.6: Diseño de interfaz gráfica: Requerimiento HB02

Permite que un paciente designe control sobre su HCEN a un tutor, para que gestione la misma o parte de ella, en caso de que él, por la razón que fuese no pueda realizarlo. El paciente puede cambiar de tutor las veces que desee.

En la parte superior de la pantalla se muestra el nombre y apellido del tutor de la HCEN automáticamente (si fue designado previamente). Sobre la izquierda se presentan las opciones posibles sobre las cuales se puede otorgar permisos. Sobre la derecha se ingresan los datos obligatorios a completar para designar al tutor. Ingresando el documento de identidad, mediante el uso del servicio de la DNIC[1], se obtiene el nombre y apellido que se completa de forma automática.

Esta interfaz gráfica permite también, de ser necesario, eliminar la tutoría otorgada, mediante el botón REVOCAR.

[1]Dirección Nacional de Identificación Civil

4.5.2. Ejemplo Ilustrativo

Un paciente configura los permisos de accesos a una persona de su confianza (tutor), quién podrá visualizar su HCEN.

La Tabla 4.10 muestra los elementos a considerar para diseñar una política que brinde soporte a este requerimiento.

Tabla 4.10: Elementos para política. Requerimiento: HB02

Elemento	**Detalle**
Paciente	Luis
Tutor	Angela Techera
CI	12345678
eMail	email@email.com
Tel/Cel	099999999

Si Paciente = 'Luis' AND Tutor = 'Angela Techera' AND CI = 12345678 AND eMail = 'email@email.com' AND Celular = 099999999 **Permite acceder** Sino **No permite acceder**

4.5.3. Especificación de Política

Se presenta la estructura de política que se define al momento de que el paciente configura las opciones para dar soporte al requerimiento HB02. Cuando se seleccionan todas las opciones en la interfaz gráfica con los elementos mencionados, se genera una política acorde al siguiente plantilla.

Listing 4.2: Especificación de Política FACPL: Req. HB02.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2    target: equal ("Nombre_Paciente", hce/pacienteid )
3
4    policies:
5      PolicySet readSpecialistHealth {deny-unless-permit
6
7          target: equal ("read", action/id)
8                  && equal (subject/cedula, "Dato_CedulaTutor")
9                   && equal (subject/email,"Direccion_eMail")
10                          && equal (subject/cel, "Dato_CelularTutor")
11                 policies:
12                     Rule readConfiguracionAccesoPaciente (permit
13                         target: equal ("Nombre_Tutor", subject/tutorid)
14                       )
15     }
16 }
```

En la línea 2 se define al paciente para la ejecución de la política. El grupo de líneas de código de 4 a 10 define el tipo de acceso que será READ, los datos del tutor configurado específicamente para permitir el acceso.

El grupo de líneas de código de 12 a 14 define el grupo de políticas, indicando el nombre del tutor para permitir el acceso.

4.6. Requerimiento: HB03

Este requerimiento refiere a que el tutor (persona de confianza del paciente) tome el control de la HCEN del paciente, en el momento posterior al fallecimiento de éste.

4.6.1. Diseño de Interfaz Gráfica

La Figura 4.7 presenta un posible diseño de interfaz de usuario para abordar este requerimiento. Para mejor comprensión, se presenta con datos de ejemplo.

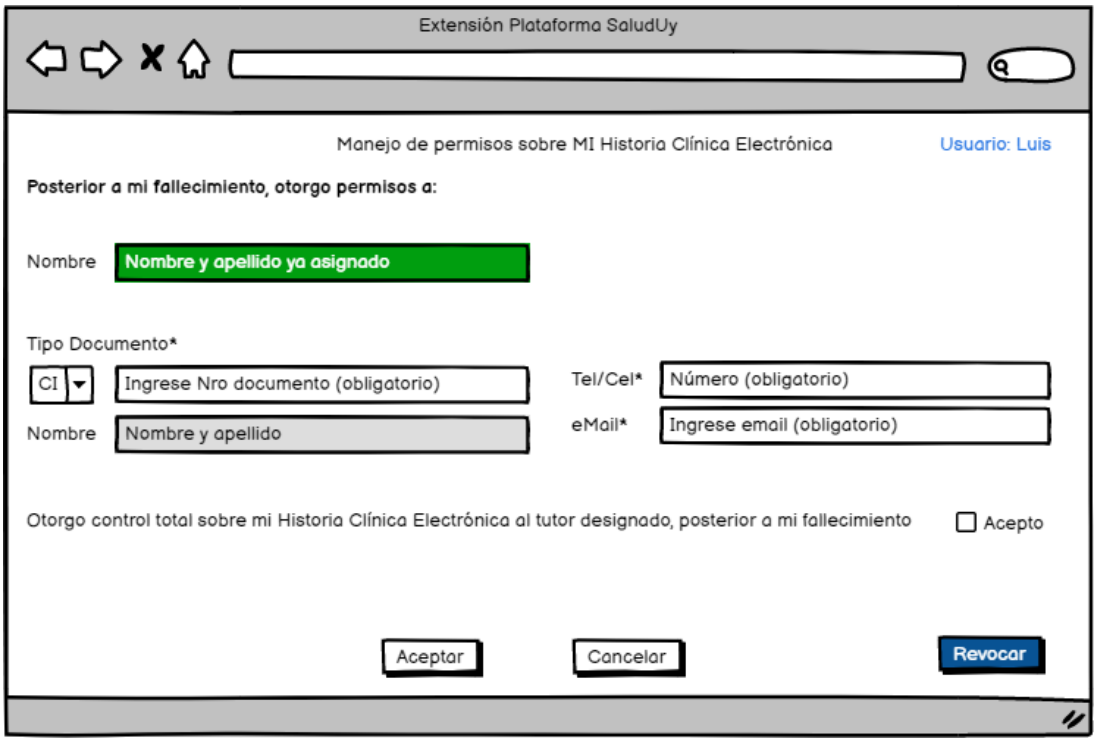

Figura 4.7: Diseño de interfaz gráfica: Requerimiento HB03.

Esta interfaz gráfica permite designar un tutor para tomar control sobre la HCEN, posterior al fallecimiento del paciente. El paciente puede cambiar de

tutor las veces que desee.

Esta interfaz gráfica permite también, de ser necesario, eliminar la tutoría otorgada, mediante el botón REVOCAR.

Nota: El paciente puede tener más de un tutor configurado en su HCEN, puede tener uno en vida y otro, posterior a su fallecimiento.

4.6.2. Ejemplo Ilustrativo

Un paciente configura los permisos de accesos a una persona de su confianza (tutor), quién podrá visualizar la HCEN posterior al fallecimiento del paciente.

La Tabla 4.11 muestra los elementos a considerar para diseñar una política que brinde soporte a este requerimiento.

Tabla 4.11: Elementos para política. Requerimiento: HB03

Elemento	**Detalle**
Paciente	Luis
Está fallecido	Verdadero
Tutor	Angela Techera
CI	12345678
eMail	email@email.com
Tel/Cel	099999999

Si Paciente = 'Luis' AND estaFallecido = Verdadero AND Tutor = 'Angela Techera' AND eMail = 'email@email.com' AND CI = 12345678 AND Celular = 099999999 **Permite acceder** Sino **No permite acceder**

4.6.3. Especificación de Política

Se presenta la estructura de política que se define al momento de que el paciente configura las opciones para dar soporte al requerimiento HB03. Cuando se seleccionan todas las opciones en la interfaz gráfica con los elementos mencionados, se genera una política acorde a la siguiente plantilla.

Listing 4.3: Especificación de Política FACPL: Req. HB03.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2    target: equal ("Nombre_Paciente", hce/pacienteid )
3    policies:
4      PolicySet readSpecialistHealth {deny-unless-permit
5
6          target: equal ("read", action/id)
7                  && equal (hce/isDead, Boolean)
8                  && equal (subject/cedula, "Dato_CedulaTutor")
9                  && equal (subject/email,"Direccion_eMail")
10                 && equal (subject/cel, "Dato_CelularTutor")
11                policies:
12                    Rule readConfiguracionAccesoPaciente (permit
13                        target: equal ("Nombre_Tutor", subject/tutorid)
14                        )
15     }
16 }
```

En la línea 2 se define al paciente para la ejecución de la política. El grupo de líneas de código de 4 a 10 define el tipo de acceso que será READ, el parámetro que indicará si el paciente es fallecido o no y los datos del tutor configurado específicamente para permitir el acceso.

El grupo de líneas de código de 11 a 13 define el grupo de políticas, indicando el nombre del tutor para permitir el acceso.

4.7. Requerimiento: HB04

Este requerimiento refiere a que un Prestador de Salud, de forma total o parcial, tenga acceso a la HCEN de un paciente, ya fallecido. Dicho acceso es por una determinada cantidad de años.

4.7.1. Diseño de Interfaz Gráfica

La Figura 4.8 presenta un posible diseño de interfaz de usuario para abordar este requerimiento. Para mejor comprensión, se presenta con datos de ejemplo.

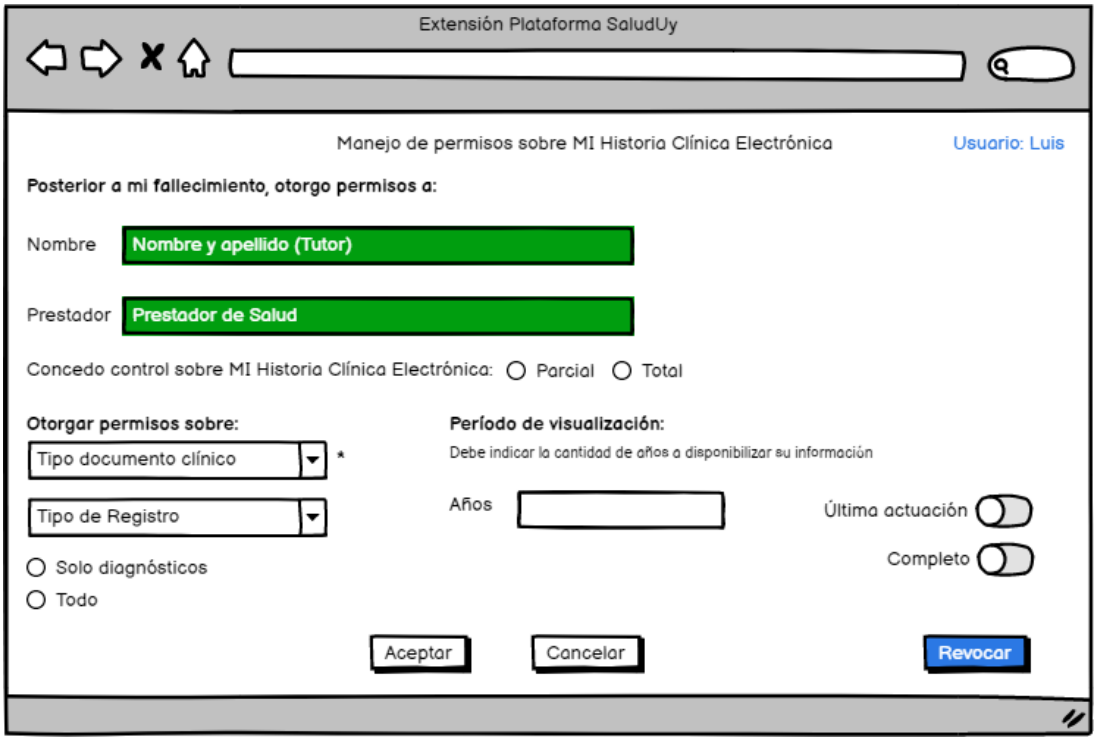

Figura 4.8: Diseño de interfaz gráfica: Requerimiento HB04.

Si el paciente opta por una vez fallecido, dar expreso consentimiento para que su HCEN sea aporte a la medicina como caso de estudio, puede otorgar permisos totales o parciales a un Prestador de salud. Si otorga **Parcial**, se habilitan las listas desplegables para que seleccione lo deseado. Si el control es **Total**, las listas desplegables no estarán disponibles para selección y quedan otorgados los permisos sobre todas las opciones.

Una vez realizadas las configuraciones, debe indicar la cantidad de años que deja disponible la HCEN. También es posible indicar la disponibilidad a partir de la última actuación o de forma completa la HCEN. Para ello tiene las opciones ÚLTIMA ACTUACIÓN / COMPLETO.

Esta interfaz gráfica permite también, de ser necesario, eliminar los permisos otorgados mediante el botón REVOCAR.

4.7.2. Ejemplo Ilustrativo

Un paciente configura los permisos de accesos a un Prestador de Salud quién podrá visualizar la HCEN de forma total o parcial por un lapso de tiempo estipulado, posterior a su fallecimiento.

La Tabla 4.12 muestra los elementos a considerar para diseñar una política que brinde soporte a este requerimiento.

Tabla 4.12: Elementos para política. Requerimiento: HB04

Elemento	**Detalle**
Paciente	Luis
Es Fallecido	Verdadero
Prestador de Salud	SUMMUN
Cantidad de años	8
Actuación	Completa

Si Paciente = 'Luis' AND EstadoFallecido = Verdadero AND Presador-Salud = 'SUMMUN' AND cantidadAños = 8 AND Actuación = Completa **Permite acceder** Sino **No permite acceder**

4.7.3. Especificación de Política

Se presenta la estructura de política que se define al momento de que el paciente configura las opciones para dar soporte al requerimiento HB04. Cuando se seleccionan todas las opciones en la interfaz gráfica con los elementos mencionados, se genera una política acorde a la siguiente plantilla.

Listing 4.4: Especificación de Política FACPL: Req. HB04.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2
3    target: equal ("Nombre_Paciente", hce/pacienteid )
4    policies:
5      PolicySet readSpecialistHealth {deny-unless-permit
6          target: equal ("read", action/id)
7                  && equal (hce/isDead, Boolean)
8                  && equal (subject/cantAnios, "Nro_CantAnios")
9                  && equal (subject/tipoActuacion, "TipoActuacion")
10                 policies:
11                 Rule readConfiguracionAccesoPaciente (permit
12                       target: equal ("Nombre_PrestadorSalud", subject/id)
13                 )
14     }
15 }
```

En la línea 3 se define al paciente para la ejecución de la política. El grupo de líneas de código de 5 a 9 define el tipo de acceso que será READ, la variable booleana que permite saber si el paciente está fallecido o no, la cantidad de años de disponibilidad y el tipo de actuación permitida específicamente para brindar el acceso.

El grupo de líneas de código de 10 a 12 define el grupo de políticas, indicando el nombre del Prestador de Salud para permitir el acceso.

4.8. Requerimiento: HB05

Este requerimiento refiere a que un Profesional de la salud, configura los permisos a otro Profesional de la salud suplente para que acceda a la HCEN de un paciente, con su consentimiento previo.

4.8.1. Diseño de Interfaz Gráfica

La Figura 4.9 presenta un posible diseño de interfaz de usuario para abordar este requerimiento. Para mejor comprensión, se presenta con datos de ejemplo.

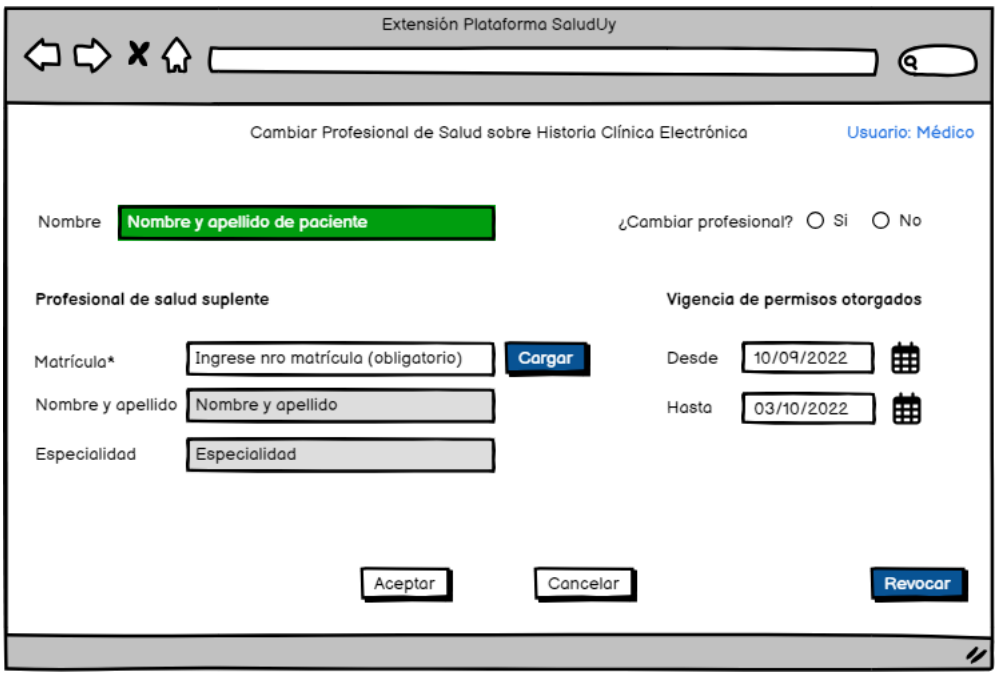

Figura 4.9: Diseño de interfaz gráfica: Requerimiento HB05

Esta interfaz gráfica tiene como precondición acceder primeramente a la HCEN de un paciente y tener el consentimiento del mismo para habilitar el cambio. Una vez dentro, el sistema trae automáticamente el nombre del paciente en cuestión (cuadro superior izquierdo). Lo que debe hacer el Profesional de salud es ingresar la matrícula del Profesional que lo suplantará temporalmente. El botón Cargar, permite cargar los datos personales asociados a dicha

matrícula. Luego, ingresa el rango de fechas de vigencia del otorgamiento de permisos sobre dicha HCEN.

Una vez culminada la temporalidad de permisos, retorna el control al profesional en salud tratante.

4.8.2. Ejemplo Ilustrativo

Un profesional de salud configura los permisos de accesos a otro profesional quién podrá visualizar la HCEN de un paciente determinado por un período de tiempo dado.

La Tabla 4.13 muestra los elementos a considerar para diseñar una política que brinde soporte a este requerimiento.

Tabla 4.13: Elementos para política. Requerimiento: HB05

Elemento	**Detalle**
Paciente	Luis
Profesional de Salud suplente	Pamela Díaz
Vigencia	FechaDesde a FechaHasta

Si Paciente = 'Luis' AND ProfesionalSuplente = 'Pamela Díaz' AND Vigencia = mayor(Desde) y menor(Hasta) **Permite acceder** Sino **No permite acceder**

4.8.3. Especificación de Política

Se presenta la estructura de política que se define al momento de que el paciente configura las opciones para dar soporte al requerimiento HB05. Cuando se seleccionan todas las opciones en la interfaz gráfica con los elementos mencionados, se genera una política acorde a la siguiente plantilla.

Listing 4.5: Especificación de Política FACPL: Req. HB05.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2
3    target: equal ("Nombre_Paciente", hce/pacienteid )
4    policies:
5      PolicySet readSpecialistHealth {deny-unless-permit
6
7          target: equal ("read", action/id)
8                          && equal ("Nro_Matricula", subject/matricula)
9                          && equal ("Nombre_Especialidad", hce/titleDocument)
10                         && ( greater-than(datetime/id, "FechaDesde")
11                         && less-than(datetime/id, "FechaHasta"))
12                 policies:
13                     Rule readConfiguracionAccesoPaciente (permit
14                         target: equal ("Nombre_ProfesionalSuplente", subject/autorid)
15                       )
16     }
17 }
```

En la línea 3 se define al paciente para la ejecución de la política. El grupo de líneas de código de 4 a 11 define el tipo de acceso que será READ, la matrícula, la especialidad, el período de fechas de vigencia para el acceso.

El grupo de líneas de código de 12 a 14 define el grupo de políticas, indicando el Profesional en salud suplente para permitir el acceso.

4.9. Requerimiento: HB06

Este requerimiento refiere a que un Especialista en Privacidad, configura las políticas de acceso para permitir a los Profesionales en salud, acceder a la HCEN de un paciente en situaciones *breaking the glass*.

Este requerimiento como tal, no presenta una interfaz gráfica específica ya que es una configuración a nivel general sobre la HCEN.

4.9.1. Ejemplo Ilustrativo

Si se requiere acceder a la HCEN de un paciente en situación de urgencia o emergencia, se accede a la misma por *breaking the glass*. No es requerida ninguna autorización previa del paciente ya que se trata de una situación límite en la que se requiere acceder a los datos de la HCEN para dar curso a la atención médica.

La Tabla 4.14 los elementos a considerar para diseñar una política que brinde soporte a este requerimiento.

Tabla 4.14: Elementos para política. Requerimiento: HB06

Elemento	Detalle
isBreakingTheGlass	Verdadero

Si isBreakingTheGlass = Verdadero **Permite acceder** Sino **No permite acceder**

4.9.2. Especificación de Política

Se presenta la estructura de política que se define para dar soporte al requerimiento HB06, generándose una política acorde al siguiente plantilla.

Listing 4.6: Especificación de Política FACPL: Req. HB06.

```
1  PolicySet ConfiguracionBreakingTheGlass {deny-unless-permit
2    policies:
3      PolicySet readBreakingTheGlass {deny-unless-permit
4          target: equal ("read", action/id)
5            policies:
6              Rule readBreakingTheGlassPaciente (permit
7                  target: equal (Boolean, hce/isBreakingTheGlass)
8                )
9    }
10 }
```

En la línea 4 se define el tipo de acceso que será READ. En la línea 7 se define la variable *breaking the glass* que permite saber si se encuentra en una situación de esa índole si al compararla con el valor booleano, devuelve true.

4.10. Requerimiento: AD01

Este requerimiento refiere a que un paciente, puede configurar la auditoría para conocer quién accedió y cuándo a su HCEN y a qué parte precisamente. Cuando este acceso ocurre, se debe generar una notificación relacionada.

4.10.1. Diseño de Interfaz Gráfica

La Figura 4.10 presenta un posible diseño de interfaz de usuario para abordar este requerimiento. Para mejor comprensión, se presenta con datos de

ejemplo.

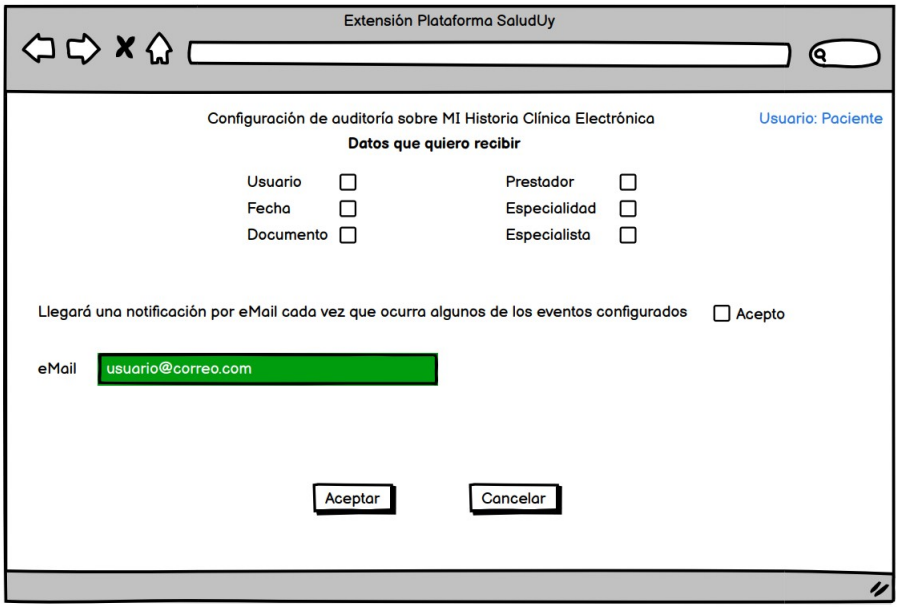

Figura 4.10: Diseño de interfaz gráfica: Requerimiento: AD01

Esta interfaz gráfica permite indicar los datos que se desea recibir mediante una notificación por mail cuando ocurren accesos a la HCEN del paciente. Esto aplica tanto si accede un prestador, una especialidad en concreto (de un especialista) o más granular, qué especialista accedió al historial médico.

4.10.2. Ejemplo Ilustrativo

Un paciente desea configurar las notificaciones para que se envíen según configuración de la auditoría. Aquí el sistema va a enviar un mail siempre y cuando esta parte esté configurada, según informe que desea recibir por mail.

La Tabla 4.15 muestra los elementos a considerar para diseñar una política que brinde soporte a este requerimiento.

Tabla 4.15: Elementos para política. Requerimiento: AD01

Elemento	**Detalle**
Paciente	Luis
Profesional de Salud	Marcio Leal
Fecha de acceso	01.08.2022
CI	12345678
Prestador de Salud	Británico

Si Paciente = 'Luis' AND ProfesionalSalud = 'Marcio Leal' AND FechaAcceso = 01.08.2022 AND CI = 12345678 AND PrestadorSalud = 'Británico'

AND estaConfigurado **Envía Mail de notificación** Sino **No envía mail de notificación**

4.10.3. Especificación de Política

Se presenta la estructura de política que se define al momento de que el paciente configura las opciones para dar soporte al requerimiento AD01. Cuando se seleccionan todas las opciones en la interfaz gráfica con los elementos mencionados, se genera una política acorde a la siguiente plantilla. Si no se configura esta auditoría, no se emite notificación.

Listing 4.7: Especificación de Política FACPL: Req. AD01.

```
1  PolicySet ConfiguracionAccesoPaciente {deny−unless−permit
2
3    target: equal ("Nombre_Paciente", hce/pacienteid)
4    policies:
5      PolicySet readSpecialistHealth {deny−unless−permit
6          target: equal ("read", action/id)
7                  policies:
8                  Rule readConfiguracionAccesoPaciente (permit
9                    target: equal (Boolean, hce/isConfigured)
10                 )
11     }
12     obl−p: [O mailTo('eMail_EnvioNotificacion, NombreEspecialista_Acceso,
13         FechaAcceso, CedulaAcceso, PrestadorSalud_Acceso')]
14 }
```

En la línea 3 se define al paciente para la ejecución de la política. El grupo de líneas de código de 4 a 9 define el tipo de acceso que será READ y a su vez se accederá a la auditoría si se configuró la misma. El parámetro isConfigured controla esto mencionado.

La línea 12 ejecuta el envío de la notificación, según parámetros configurados por el usuario.

Capítulo 5

Actividades de Evaluación y Validación

En este capítulo se describen las actividades de evaluación y validación que se desarrollaron en el marco de la tesis, en particular: ejecución de casos de prueba en base a FACPL, encuesta preliminar a usuarios y reunión con Salud.uy.

5.1. Ejecución de casos de prueba en base a FACPL

Esta sección describe la evaluación de las políticas propuestas en el Capítulo 4, mediante la ejecución de casos de prueba. Para cada requerimiento se definen políticas concretas en base a las genéricas propuestas en el capítulo 4 y además se definen los datos de pruebas correspondientes. La idea de estos casos es ver con un ejemplo concreto cómo se relaciona un caso con su política asociada al momento de que se ejecuta dicho caso de prueba.

5.1.1. Requerimiento: HB01

Como se vio en capítulos anteriores, este requerimiento refiere a que el paciente pueda configurar permisos de acceso sobre sus datos clínicos. En particular, este acceso se puede configurar a nivel granular, en relación a quién y cuándo accede a su HCEN, sea un determinado Prestador de salud, especialidad y/o especialista.

5.1.1.1. Definición de política

La política definida para este requerimiento se presenta en Listing 5.1.

Listing 5.1: FACPL Política: Req. HB01.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2    target: equal ("Luis", hce/pacienteid )
3    policies:
4      PolicySet readSpecialistHealth {deny-unless-permit
5
6          target: equal ("read", action/id)
7                          && equal ("Britanico", subject/id)
8                          && equal ("Medicina General", hce/titleDocument)
9                          && ( greater-than(datetime/id, 2022/07/31)
10                         && less-than(datetime/id, 2022/08/16))
11                 policies:
12                     Rule readConfiguracionAccesoPaciente (permit
13                         target: equal ("Marcio Leal", subject/autorid)
14                       )
15     }
16 }
```

Se definió de la siguiente manera. La política aplica a la HCEN de Luis (línea 2), a la acción READ y al resto de los atributos especificados (línea 6 -10). Se define quién tiene permitido el acceso, es decir a Marcio Leal (línea 12-13) en el marco de lo definido anteriormente.

5.1.1.2. Definición de datos de acceso

Los casos de pruebas en FACPL se presentan en Listing 5.2.

Listing 5.2: FACPL Casos de prueba: Requerimiento HB01.

```
1  Request:{ Request1 ( action/id , "read" ) (hce/pacienteid, "Luis")}
2  Request:{ Request2 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/id, "Britanico")
3  (hce/titleDocument, "Medicina General") (subject/autorid, "Marcio Leal") (datetime/id, 2022/08/01)}
4  Request:{ Request3 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/id, "Britanico")
5  (hce/titleDocument, "Medicina General") (subject/autorid, "Antonio Cardoso")
6  (datetime/id, 2022/08/15)}
7  Request:{ Request4 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/id, "Britanico")
8  (hce/titleDocument, "Nutricionista") (subject/autorid, "Marcio Leal") (datetime/id, 2022/08/10)}
9  Request:{ Request5 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/id, "SUMMUN")
10 (hce/titleDocument, "Medicina General") (subject/autorid, "Marcio Leal") (datetime/id, 2022/08/05)}
11 Request:{ Request6 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/id, "Britanico")
12 (hce/titleDocument, "Medicina General") (subject/autorid, "Marcio Leal") (datetime/id, 2022/08/31)}
```

Se definió un caso donde se permita el acceso a la HCEN de un paciente

(línea 2) y varios casos donde se deniegue, variando los distintos atributos utilizados en la política (lineas 4 a 11).

Por ejemplo, en línea 5 se varío el atributo subject/autorid que corresponde al profesional en salud y el atributo datetime/id que corresponde a la fecha de acceso por dicho profesional en salud a la HCEN del paciente (hce/pacienteid - línea 2). En línea 9 se varió el atributo subject/id que corresponde al Prestador de salud y el atributo datetime/id que corresponde a la fecha de acceso por dicho profesional en salud a la HCEN del paciente (hce/pacienteid - línea 2).

5.1.1.3. Resultados de ejecución

La Figura 5.1 muestra la salida del proceso de ejecución correspondiente a los casos de prueba en FACPL, aplicados a la política definida en Listing 5.1, para este requerimiento.

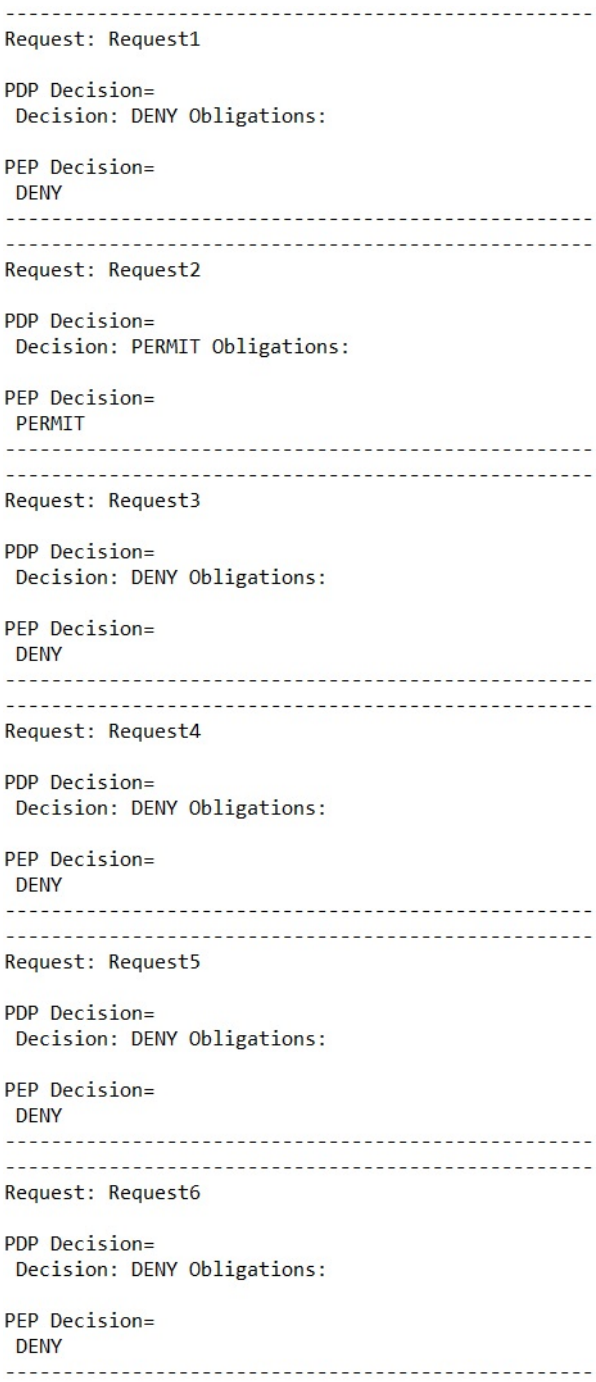

Figura 5.1: Req. HB01: Resultado del proceso de evaluación

Como se puede observar para el Request1 el resultado fue DENY porque no se definieron todos los atributos que permiten el acceso. Para el Request2 el resultado fue PERMIT ya que en dicho request se definieron todos los datos de acceso para que al evaluar los atributos definidos, la regla devuelve el acceso

permitido. Para los Request 3 al 6, el resultado fue DENY ya que se variaron los atributos con respecto al Request2 que fue el definido de acceso permitido.

5.1.2. Requerimiento: HB02

Como se vio en capítulos anteriores, este requerimiento refiere a que el tutor (persona de confianza del paciente) pueda acceder a la HCEN del paciente.

5.1.2.1. Definición de política

La política definida para este requerimiento se presenta en Listing 5.3.

Listing 5.3: FACPL Política: Req. HB02.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2    target: equal ("Luis", hce/pacienteid )
3
4    policies:
5      PolicySet readSpecialistHealth {deny-unless-permit
6
7          target: equal ("read", action/id)
8                  && equal (subject/cedula, 12345678)
9                  && equal (subject/email,"email@email.com")
10                 && equal (subject/cel, 099999999)
11               policies:
12                 Rule readConfiguracionAccesoPaciente (permit
13                   target: equal ("Angela Techera", subject/tutorid)
14                 )
15     }
16 }
```

La política aplica a la HCEN de Luis (línea 2), aplicándose la acción READ y al resto de los atributos especificados (línea 7 a 10). Se define quién tiene permitido el acceso, es decir a Angela Techera (línea 12-13) en el marco de lo definido anteriormente.

5.1.2.2. Definición de datos de acceso

Los casos de pruebas en FACPL se presentan en Listing 5.4.

Listing 5.4: FACPL Casos de prueba: Requerimiento HB02.

```
1  Request:{ Request1 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/cedula, 12345678)
2  (subject/tutorid, "Angela Techera") (subject/email, "email@email.com") (subject/cel, 099999999)}
3  Request:{ Request2 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/cedula, 87654321)
4  (subject/tutorid, "Angela Techera") (subject/email, "email@email.com") (subject/cel, 099999999)}
5  Request:{ Request3 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/cedula, 12345678)
6  (subject/tutorid, "Pamela Sosa") (subject/email, "email@email.com") (subject/cel, 099999999)}
7  Request:{ Request4 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/cedula, 12345678)
8  (subject/tutorid, "Angela Techera") (subject/email, "email2@email.com") (subject/cel, 099999999)}
9  Request:{ Request5 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/cedula, 12345678)
10 (subject/tutorid, "Angela Techera") (subject/email, "email@email.com") (subject/cel, 099888888)}
```

Se definió un caso donde se permita el acceso a la HCEN de un paciente (línea 2) y varios casos donde se deniegue, variando los distintos atributos utilizados en la política (líneas 3 a 9).

Por ejemplo, en línea 3 se varió el atributo subject/cedula que corresponde a la cédula del tutor quien accederá a la HCEN de Luis (hce/pacienteid). En línea 7 se varió el atributo subject/email que corresponde al email del tutor quien accederá a la HCEN de Luis (hce/pacienteid).

5.1.2.3. Resultado Ejecución

La Figura 5.2 muestra la salida del proceso de ejecución correspondiente a los casos de prueba en FACPL, aplicados a la política definida en Listing 5.3, para este requerimiento.

```
--------------------------------------------------
Request: Request1

PDP Decision=
 Decision: PERMIT Obligations:

PEP Decision=
 PERMIT
--------------------------------------------------
--------------------------------------------------
Request: Request2

PDP Decision=
 Decision: DENY Obligations:

PEP Decision=
 DENY
--------------------------------------------------
--------------------------------------------------
Request: Request3

PDP Decision=
 Decision: DENY Obligations:

PEP Decision=
 DENY
--------------------------------------------------
--------------------------------------------------
Request: Request4

PDP Decision=
 Decision: DENY Obligations:

PEP Decision=
 DENY
--------------------------------------------------
--------------------------------------------------
Request: Request5

PDP Decision=
 Decision: DENY Obligations:

PEP Decision=
 DENY
--------------------------------------------------
```

Figura 5.2: Req. HB02: Resultado del proceso de evaluación

Como se puede observar para el Request1 el resultado fue PERMIT ya que en dicho request se definieron todos los datos de acceso para que al evaluar los atributos definidos, la regla devuelve el acceso permitido. Para los Request 2 al 5, el resultado fue DENY ya que se variaron los atributos con respecto al Request1 que fue el definido de acceso permitido.

5.1.3. Requerimiento: HB03

Como se vio en capítulos anteriores, este requerimiento refiere a que el tutor (persona de confianza del paciente) tome el control de la HCEN del paciente, en el momento posterior al fallecimiento de éste.

5.1.3.1. Definición de política

La política definida para este requerimiento se presenta en Listing 5.5.

Listing 5.5: FACPL Política: Req. HB03.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2    target: equal ("Luis", hce/pacienteid )
3    policies:
4      PolicySet readSpecialistHealth {deny-unless-permit
5          target: equal ("read", action/id)
6                  && equal (hce/isDead, true)
7                  && equal (subject/cedula, 12345678)
8                  && equal (subject/email,"email@email.com")
9                  && equal (subject/cel, 099999999)
10                policies:
11                    Rule readConfiguracionAccesoPaciente (permit
12                        target: equal ("Angela Techera", subject/tutorid)
13                        )
14     }
15 }
```

Se definió de la siguiente manera. La política aplica a la HCEN de Luis (línea 2), aplicándose la acción READ y al resto de los atributos especificados (línea 5 a 9). Se define quién tiene permitido el acceso, es decir Angela Techera (línea 11-12) en el marco de lo definido anteriormente.

5.1.3.2. Definición de datos de acceso

Los casos de pruebas en FACPL se presentan en Listing 5.6.

Listing 5.6: FACPL Datos de acceso: Requerimiento HB03.

```
1  Request:{ Request1 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
2  (subject/cedula, 12345678) (subject/tutorid, "Angela Techera") (subject/email, "email@email.com")
3  (subject/cel, 099999999)}
4  Request:{ Request2 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, false)
5  (subject/cedula, 12345678) (subject/tutorid, "Angela Techera") (subject/email, "email@email.com")
6  (subject/cel, 099999999)}
7  Request:{ Request3 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
8  (subject/cedula, 87654321) (subject/tutorid, "Angela Techera") (subject/email, "email@email.com")
9  (subject/cel, 099999999)}
10 Request:{ Request4 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
11 (subject/cedula, 12345678) (subject/tutorid, "Milton Gimenez") (subject/email, "email@email.com")
12 (subject/cel, 099999999)}
13 Request:{ Request5 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
14 (subject/cedula, 12345678) (subject/tutorid, "Angela Techera") (subject/email, "email2@email.com")
15 (subject/cel, 099999999)}
16 Request:{ Request6 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
17 (subject/cedula, 12345678) (subject/tutorid, "Angela Techera") (subject/email, "email@email.com")
18 (subject/cel, 099777777)}
```

Se definió un caso donde se permita el acceso a la HCEN de un paciente (línea 1) ya fallecido (hce/isDead) y varios casos donde se deniegue, variando los distintos atributos utilizados en la política (líneas 4 a 16).

Por ejemplo, en línea 4 se varió el atributo hce/isDead que permite saber si el paciente está fallecido o no. En línea 7 se varió el atributo subject/cedula que corresponde a la cédula del tutor quien accederá a la HCEN de Luis (hce/pacienteid) ya fallecido (hce/isDead), para su acceso.

5.1.3.3. Resultado Ejecución

La Figura 5.3 muestra la salida del proceso de ejecución correspondiente a los casos de prueba en FACPL, aplicados a la política definida en Listing 5.5, para este requerimiento.

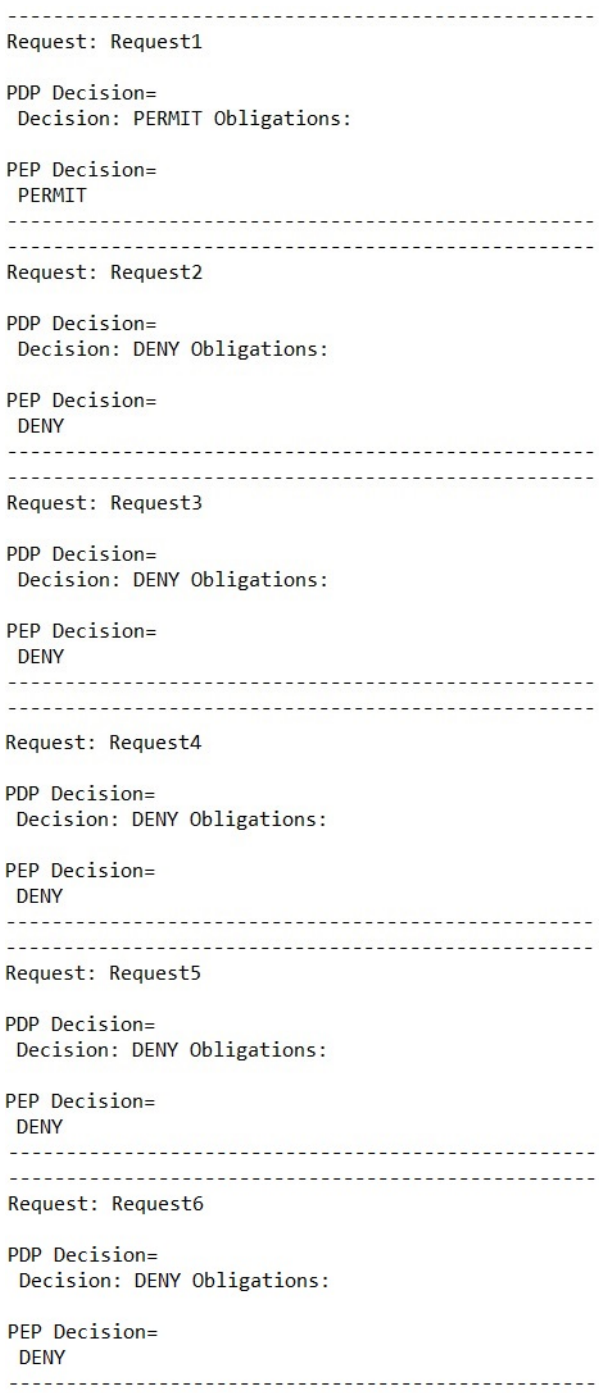

Figura 5.3: Req. HB03: Resultado del proceso de evaluación

Como se puede observar para el Request1 el resultado fue PERMIT ya que en dicho request se definieron todos los datos de acceso para que al evaluar los atributos definidos, la regla devuelve el acceso permitido. Para los Request 2 al 6, el resultado fue DENY ya que se variaron los atributos con respecto al

Request1 que fue el definido de acceso permitido.

5.1.4. Requerimiento: HB04

Como se vio en capítulos anteriores, este requerimiento refiere a que un Prestador de salud, de forma total o parcial, tenga acceso a la HCEN de un paciente, ya fallecido. Dicho acceso es por una determinada cantidad de años.

5.1.4.1. Definición de política

La política definida para este requerimiento se presenta en Listing 5.7.

Listing 5.7: FACPL Política: Req. HB04.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2
3    target: equal ("Luis", hce/pacienteid )
4    policies:
5      PolicySet readSpecialistHealth {deny-unless-permit
6          target: equal ("read", action/id)
7                  && equal (hce/isDead, true)
8                  && equal (subject/cantAnios, 8)
9                  && equal (subject/tipoActuacion, "Completa")
10                 policies:
11                     Rule readConfiguracionAccesoPaciente (permit
12                         target: equal ("SUMMUN", subject/id)
13                     )
14     }
15 }
```

Se definió de la siguiente manera. La política aplica a la HCEN de Luis (línea 3), aplicándose la acción READ y al resto de los atributos especificados (línea 6 a 9). Se define quién tiene permitido el acceso, es decir el Prestador de salud SUMMUN (línea 11-12) en el marco de lo definido anteriormente.

5.1.4.2. Definición de datos de acceso

Los casos de pruebas en FACPL se presentan en Listing 5.8.

Listing 5.8: FACPL Casos de prueba: Requerimiento HB04.

```
1 Request:{ Request1 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
2 (subject/id, "SUMMUN") (subject/cantAnios, 8) (subject/tipoActuacion, "Completa")}
3 Request:{ Request2 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
4 (subject/id, "Britanico") (subject/cantAnios, 8) (subject/tipoActuacion, "Completa")}
5 Request:{ Request3 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
6 (subject/id, "SUMMUN") (subject/cantAnios, 5) (subject/tipoActuacion, "Completa")}
7 Request:{ Request4 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isDead, true)
8 (subject/id, "SUMMUN") (subject/cantAnios, 8) (subject/tipoActuacion, "Parcial")}
```

Se definió un caso donde se permita el acceso a la HCEN de un paciente (línea 1) ya fallecido y varios casos donde se deniegue, variando los distintos atributos utilizados en la política (líneas 3 a 7).

Por ejemplo, en línea 3 se varió el atributo subject/id que corresponde al nombre del Prestador de salud, quien accederá a la HCEN de Luis (hce/pacienteid) ya fallecido (hce/isDead). En línea 5 se varió el atributo subject/cantAnios que corresponde a la cantidad de años que estará disponible la HCEN Luis (hce/pacienteid) ya fallecido (hce/isDead), para su acceso.

5.1.4.3. Resultado Ejecución

La Figura 5.4 muestra la salida del proceso de ejecución correspondiente a los casos de prueba en FACPL, aplicados a la política definida en Listing 5.7, para este requerimiento.

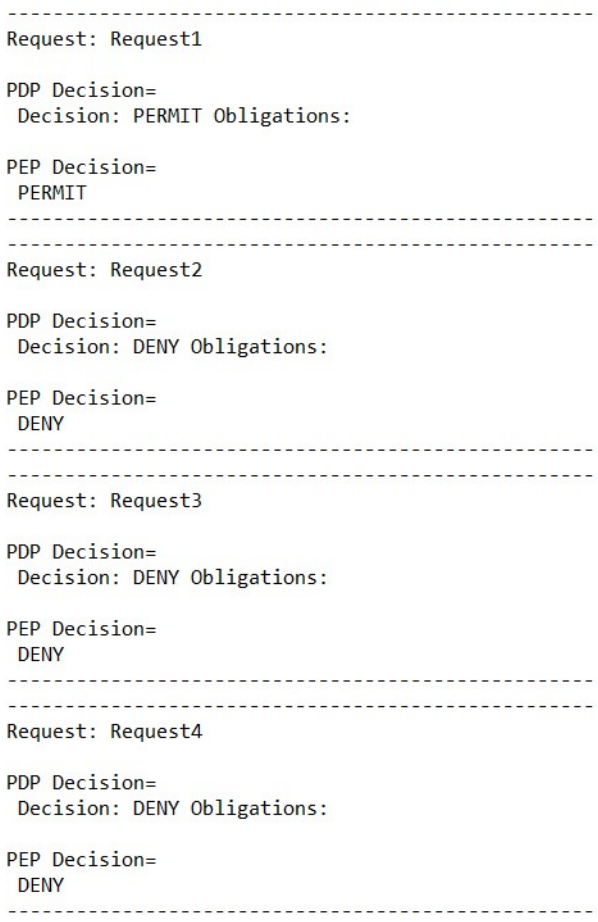

Figura 5.4: Req. HB04: Resultado del proceso de evaluación

Como se puede observar para el Request1 el resultado fue PERMIT ya que en dicho request se definieron todos los datos de acceso para que al evaluar los atributos definidos, la regla devuelve el acceso permitido. Para los Request 2 al 4, el resultado fue DENY ya que se variaron los atributos con respecto al Request1 que fue el definido de acceso permitido.

5.1.5. Requerimiento: HB05

Como se vio en capítulos anteriores, este requerimiento refiere a que un profesional de la salud, configura los permisos a otro profesional de la salud suplente para que acceda a la HCEN de un paciente, con su consentimiento previo.

5.1.5.1. Definición de política

La política definida para este requerimiento se presenta en Listing 5.9.

Listing 5.9: FACPL Política: Req. HB05.

```
1  PolicySet ConfiguracionAccesoPaciente {deny-unless-permit
2
3    target: equal ("Luis", hce/pacienteid )
4    policies:
5      PolicySet readSpecialistHealth {deny-unless-permit
6
7          target: equal ("read", action/id)
8                          && equal (4030740, subject/matricula)
9                          && equal ("Medicina General", hce/titleDocument)
10                         && ( greater-than(datetime/id, 2022/07/31)
11                         && less-than(datetime/id, 2022/08/16))
12                 policies:
13                     Rule readConfiguracionAccesoPaciente (permit
14                                 target: equal ("Pamela Diaz", subject/autorid)
15                         )
16     }
17 }
```

La política aplica a la HCEN de Luis (línea 3), aplicándose la acción READ y al resto de los atributos especificados (línea 7 a 11). Se define quién tiene permitido el acceso, es decir el profesional de la salud Pamela Díaz (línea 13-14) en el marco de lo definido anteriormente.

5.1.5.2. Definición de datos de acceso

Los casos de pruebas en FACPL se presentan en Listing 5.10.

Listing 5.10: FACPL Casos de prueba: Requerimiento HB05.

```
1  Request:{ Request1 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/matricula, 4030740)
2  (subject/autorid, "Pamela Diaz") (hce/titleDocument, "Medicina General") (datetime/id, 2022/08/01)}
3  Request:{ Request2 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/matricula, 4030741)
4  (subject/autorid, "Pamela Diaz") (hce/titleDocument, "Medicina General") (datetime/id, 2022/08/01)}
5  Request:{ Request3 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/matricula, 4030740)
6  (subject/autorid, "Carmelo Gomez") (hce/titleDocument, "Medicina General") (datetime/id, 2022/08/01)}
7  Request:{ Request4 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/matricula, 4030740)
8  (subject/autorid, "Pamela Diaz") (hce/titleDocument, "Deportologo") (datetime/id, 2022/08/01)}
9  Request:{ Request5 ( action/id , "read" ) (hce/pacienteid, "Luis") (subject/matricula, 4030740)
10 (subject/autorid, "Pamela Diaz") (hce/titleDocument, "Medicina General") (datetime/id, 2022/05/01)}
```

Se definió un caso donde se permita el acceso a la HCEN de un paciente (línea 1) y varios casos donde se deniegue, variando los distintos atributos

utilizados en la política (líneas 3 a 9).

Por ejemplo, en línea 3 se varió el atributo subject/matricula, que corresponde a la matrícula del profesional en salud suplente, quien accederá a la HCEN de Luis (hce/pacienteid). En línea 7 se varió el atributo hce/titleDocument, que corresponde a la especialidad Deportólogo del profesional en salud Pamela Díaz (subject/autorid), quien accederá a la HCEN de Luis (hce/pacienteid).

5.1.5.3. Resultado Ejecución

La Figura 5.5 muestra la salida del proceso de ejecución correspondiente a los casos de prueba en FACPL, aplicados a la política definida en Listing 5.9, para este requerimiento.

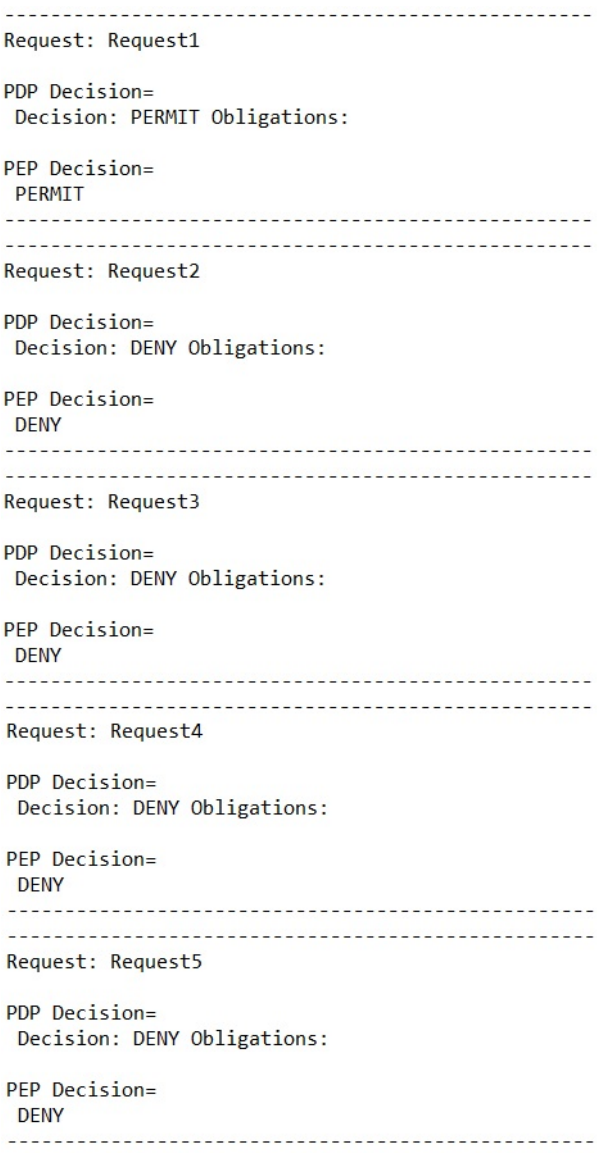

Figura 5.5: Req. HB05: Resultado del proceso de evaluación

Como se puede observar para el Request1 el resultado fue PERMIT ya que en dicho request se definieron todos los datos de acceso para que al evaluar los atributos definidos, la regla devuelve el acceso permitido. Para los Request 2 al 5, el resultado fue DENY ya que se variaron los atributos con respecto al Request1 que fue el definido de acceso permitido.

5.1.6. Requerimiento: HB06

Como se vio en capítulos anteriores, este requerimiento refiere a que un Especialista en Privacidad, configura las políticas de acceso para permitir a

los profesionales en salud, acceder a la HCEN de un paciente en situaciones *breaking the glass*.

5.1.6.1. Definición de política

La política definida para este requerimiento se presenta en Listing 5.11.

Listing 5.11: FACPL Política: Req. HB06.

```
1  PolicySet ConfiguracionBreakingTheGlass {deny-unless-permit
2
3    policies:
4      PolicySet readBreakingTheGlass {deny-unless-permit
5          target: equal ("read", action/id)
6            policies:
7              Rule readBreakingTheGlassPaciente (permit
8                  target: equal (true, hce/isBreakingTheGlass)
9                )
10     }
11 }
```

La política aplica a toda HCEN, por dicho motivo no se especifica un paciente en particular, como se vio en requerimientos anteriores. Se aplica la acción READ y al resto de los atributos especificados (línea 5-8) en el marco de lo definido anteriormente.

5.1.6.2. Definición de datos de acceso

La escritura de los casos de pruebas en FACPL se presentan en Listing 5.12.

Listing 5.12: FACPL Casos de prueba: Requerimiento HB06.

```
1  Request:{ Request1 ( action/id , "read" ) (hce/isBreakingTheGlass, true)}
2  Request:{ Request2 ( action/id , "read" ) (hce/isBreakingTheGlass, false)}
```

Se definió un caso donde se permita el acceso a una HCEN en situación BreakingTheGlass (hce/isBreakingTheGlass) (línea 1) y un caso donde se deniegue, variando el atributo utilizado en la política (línea 2).

5.1.6.3. Resultado Ejecución

La Figura 5.6 muestra la salida del proceso de ejecución correspondiente a los casos de prueba en FACPL, aplicados a la política definida en Listing 5.11, para este requerimiento.

```
--------------------------------------------------
Request: Request1

PDP Decision=
 Decision: PERMIT Obligations:

PEP Decision=
 PERMIT
--------------------------------------------------
--------------------------------------------------
Request: Request2

PDP Decision=
 Decision: DENY Obligations:

PEP Decision=
 DENY
--------------------------------------------------
```

Figura 5.6: Req. HB06: Resultado del proceso de evaluación

Como se puede observar para el Request1 el resultado fue PERMIT ya que en dicho request se definió el acceso para que al evaluar el atributo definido, la regla devuelve el acceso permitido. Para el Request2, el resultado fue DENY ya que se varió el atributo con respecto al Request1 que fue el definido de acceso permitido.

5.1.7. Requerimiento: AD01

Como se vio en capítulos anteriores, este requerimiento refiere a que un paciente, puede configurar la auditoría para conocer quién y cuándo se accedió a su HCEN y a qué parte precisamente. Cuando este acceso ocurre, se debe generar una notificación relacionada.

5.1.7.1. Definición de política

La política definida para este requerimiento se presenta en Listing 5.13.

Listing 5.13: FACPL Política: Req. AD01.

```
1  PolicySet ConfiguracionAccesoPaciente {deny−unless−permit
2
3    target: equal ("Luis", hce/pacienteid)
4    policies:
5      PolicySet readSpecialistHealth {deny−unless−permit
6          target: equal ("read", action/id)
7                  policies:
8                  Rule readConfiguracionAccesoPaciente (permit
9                    target: equal (true, hce/isConfigured)
10                 )
11     }
12     obl−p: [O mailTo('usuario@correo.com', subject/autorid, datetime/id, subject/cedula, subject/id)]
13 }
```

La política aplica a la HCEN de Luis (línea 3), aplicándose la acción READ y al resto de los atributos especificados (línea 6-9). Se define la configuración de envío de emails (hce/isConfigured) en el marco de lo definido anteriormente. Se configuran los atributos para recibir el email de la notificación (línea 12).

5.1.7.2. Definición de datos de acceso

Los casos de pruebas en FACPL se presentan en Listing 5.14.

Listing 5.14: FACPL Casos de prueba: Requerimiento AD01.

```
1  Request:{ Request1 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isConfigured, true)
2  (subject/autorid, "Marcio Leal") (datetime/id, 2022/08/01) (subject/cedula, 12345678)
3  (subject/id, "Britanico")}
4  Request:{ Request2 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isConfigured, false)
5  (subject/autorid, "Marcio Leal") (datetime/id, 2022/08/01) (subject/cedula, 12345678)
6  (subject/id, "Britanico")}
7  Request:{ Request3 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isConfigured, true)
8  (subject/autorid, "German Lorenzo") (datetime/id, 2022/08/01) (subject/cedula, 12345678)
9  (subject/id, "Britanico")}
10 Request:{ Request4 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isConfigured, true)
11 (subject/autorid, "Marcio Leal") (datetime/id, 2022/09/01) (subject/cedula, 12345678)
12 (subject/id, "Britanico")}
13 Request:{ Request5 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isConfigured, true)
14 (subject/autorid, "Marcio Leal") (datetime/id, 2022/08/01) (subject/cedula, 99999999)
15 (subject/id, "Britanico")}
16 Request:{ Request6 ( action/id , "read" ) (hce/pacienteid, "Luis") (hce/isConfigured, true)
17 (subject/autorid, "Marcio Leal") (datetime/id, 2022/08/01) (subject/cedula, 12345678)
18 (subject/id, "SUMMUN")}
```

Se definió un caso donde se configura el envío de la notificación según acceso a la HCEN de un paciente (línea 1) y varios casos donde se deniegue, variando

los distintos atributos utilizados en la política (líneas 4 a 16).

Por ejemplo, en línea 4 se varió el atributo hce/isConfigured, que corresponde a la configuración del envío de email cuando se accede a la HCEN de Luis (hce/pacienteid). En línea 10 se varió el atributo datetime/id, que corresponde a la fecha de acceso del profesional en salud Marcio Leal (subject/autorid), quien accederá a la HCEN de Luis (hce/pacienteid).

En dicha configuración, al paciente Luis (hce/pacienteid) le interesa recibir el nombre del especialista que accedió (subject/autorid), su número de cédula de identidad (subject/cedula), la fecha cuando accedió (datetime/id) y de qué Prestador de salud (subject/id) accede. Esa información se le notificará al email que haya configurado ('usuario@correo.com' visto en Listing 5.13).

5.1.7.3. Resultado Ejecución

La Figura 5.7 muestra la salida del proceso de ejecución correspondiente a los casos de prueba en FACPL, aplicados a la política definida en Listing 5.13, para este requerimiento.

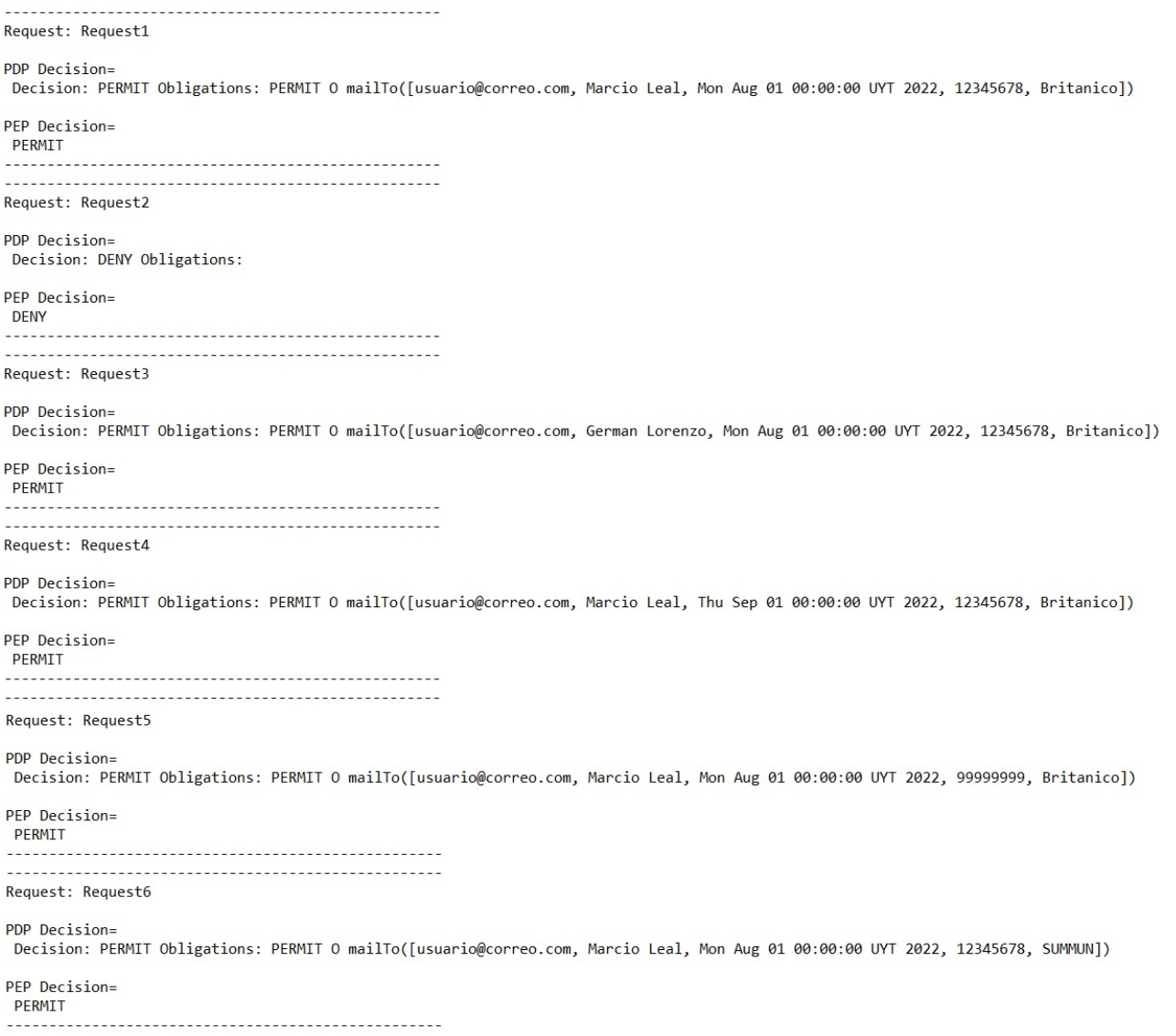

Figura 5.7: Req. AD01: Resultado del proceso de evaluación

Como se puede observar para el Request1 el resultado fue PERMIT ya que en dicho request se definieron todos los datos de acceso para que al evaluar los atributos definidos, la regla devuelve el acceso permitido al enviar el email. Para los Request 2 al 6, el resultado fue DENY ya que se variaron los atributos con respecto al Request1 que fue el definido de acceso permitido.

5.2. Encuesta preliminar a usuarios

A continuación se desarrolla la encuesta preliminar a usuarios. Los objetivos de la misma fueron: indagar qué tanto se conoce a nivel general la actual aplicación **Mi Historia Clínica Digital** de Salud.uy, y como parte de validación de algunos requerimientos identificados y previo a la propuesta de solución, visto en el Capítulo 3 del presente documento.

Para la implementación de la encuesta se utilizó GoogleForms de forma de facilitar su envío, análisis, respuesta y generación de resultados. Todas las preguntas tienen una única respuesta posible y son todas de carácter obligatorio. La encuesta preeliminar es anónima y fueron seleccionadas personas allegadas a la autora de la presente tesis, todas mayores de edad, pertenecientes al sistema de salud (público o privado) y se incluyó personas pertenecientes a algún servicio de emergencia médico móvil. Esta selección totalizó 74 personas, las cuales todas realizaron la encuesta preeliminar. La encuesta preeliminar está disponible en línea a través del servicio de GoogleForms.

La misma inicia con una breve introducción al tema para contextualizar al encuestado, luego se tiene un total de 8 preguntas obligatorias de múltiple opción y finalmente un espacio de respuesta libre, no obligatoria.

A continuación, se describe la encuesta punto por punto.

5.2.1. Detalles de la encuesta

5.2.1.1. Introducción

Hoy en día el Estado brinda un servicio en línea para acceder a **Mi Historia Clínica Digital**, donde el usuario puede restringir el acceso a la información y acceder a los documentos realizados por el médico en cada consulta. Esta aplicación por el momento no permite acceder a la totalidad de la historia clínica digital, es decir a ver estudios, análisis, pero lo que permite hacer es:

- Ver quiénes accedieron a Mis Documentos
- El paciente tiene tres tipos de opciones para restringir el acceso de forma general a su información clínica: restringiendo “solo con fines asistenciales”, habilitando “parcialmente” durante un tiempo o “no habilita”, no permitiendo el acceso a nadie. En casos de emergencias, por normativa del Estado, el prestador de salud puede ingresar sin necesidad de permiso

alguno.

5.2.1.2. Preguntas

A continuación, se desarrollan las preguntas que componen la encuesta preliminar:

1. ¿Conoces este servicio en línea propuesto por el Estado? SI / NO
2. ¿Consideras de importancia poder acceder a tu historia clínica en formato digital y así poder visualizar las actuaciones de los médicos y/o análisis realizados? SI / NO
3. Teniendo en cuenta la introducción ofrecida al principio, ¿consideras que lo ofrecido es suficiente para tener control sobre tu historia clínica electrónica? SUFICIENTE / NO SUFICIENTE
4. Considerando lo que permite hacer la plataforma de accesos, indique qué otras funcionalidades entiende sería deseable tener y qué grado de prioridad le correspondería:
   - Conocer cuando un profesional de la salud accede a tu historial médico sin que tengas agendada una visita, ¿crees de utilidad que un sistema informático te notifique de dicha visualización? Marque una prioridad: ALTA / MEDIA / BAJA
   - Especificar el acceso a tu historia clínica digital, por el tiempo que tu desees, a un especialista médico determinado. Marque una prioridad: ALTA / MEDIA / BAJA
   - Otorgar permisos a ciertas partes de la historia clínica digital, por ejemplo: estudios (resonancias, rayosX, tomografías, entre otros), exámenes de laboratorios, etc, a determinada especialidad médica. Marque una prioridad: ALTA / MEDIA / BAJA
   - Definir a una persona de tu confianza a tomar el control de tu historia clínica digital en caso de que tú te veas imposibilitado por la razón que fuese. ¿Consideras que sería de utilidad? Marque una prioridad: ALTA / MEDIA / BAJA
5. Si pudieras agregar otras funcionalidades no consideradas anteriormente

en la plataforma de accesos, como ser alguna de las siguientes, marque la prioridad de interés para cada una de ellas.

Previo a realizar un viaje, habilitar tu historia clínica digital a instituciones médicas ofrecidas por tu seguro de viajero. Marque una prioridad: ALTA / MEDIA / BAJA

6. Brindar acceso al área académica a tu historial médico permitiendo, si fuese el caso, análisis de enfermedades raras/complicaciones, etc., y así permitir estudiar soluciones de salud alternativas. Marque una prioridad: ALTA / MEDIA / BAJA

7. Si existiese a nivel país una plataforma informática que permita que todas las instituciones de salud, públicas o privadas y emergencias médicas móviles, fueran miembros de esta plataforma y así tener acceso a la historia clínica digital de una persona, ¿consideras que sería de utilidad informatizar a nivel nacional dicho acceso y así permitir actuar sobre una única versión de la historia clínica digital? ALTA / MEDIA / BAJA

8. Espacio para comentarios. Es texto libre, no obligatorio.

5.2.2. Resultados

A continuación, se presentan los resultados ordenados por pregunta, en base a las 74 respuestas obtenidas.

La Figura 5.8 muestra el resultado de la pregunta 1. El 78 % de los encuestados no conoce el servicio en línea del Estado.

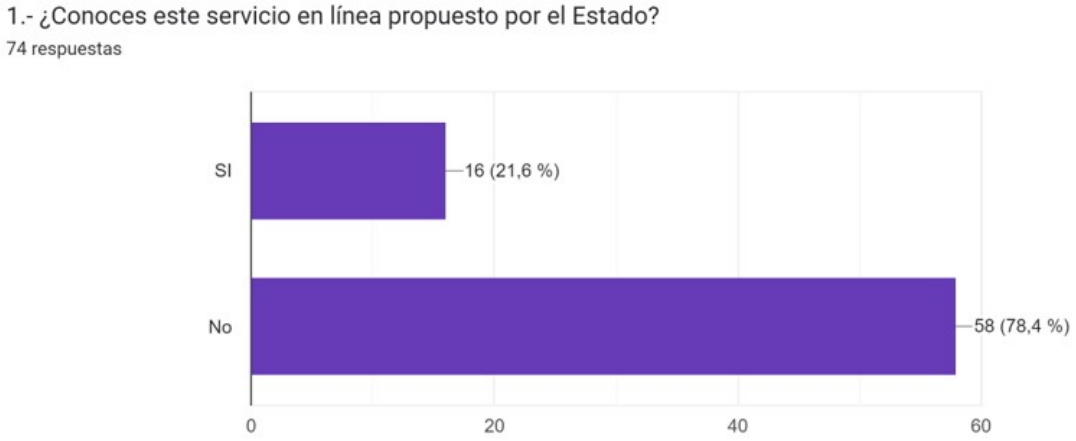

Figura 5.8: Respuesta a pregunta 1

La Figura 5.9 muestra el resultado de la pregunta 2. El 100 % de los encuestados considera de importancia acceder a su HCEN.

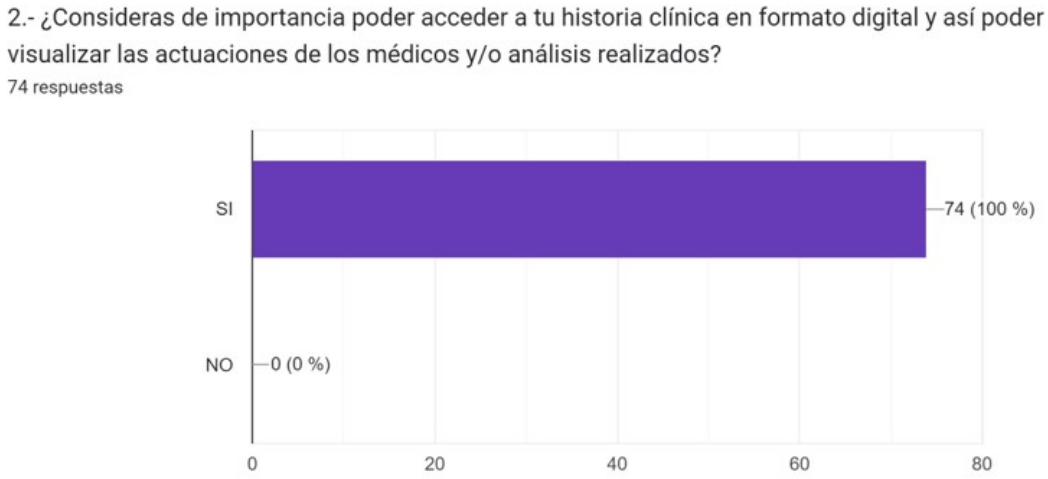

Figura 5.9: Respuesta a pregunta 2

La Figura 5.10 muestra el resultado de la pregunta 3. El 54 % de los encuestados considera que lo mencionado es suficiente para tener control sobre su HCEN.

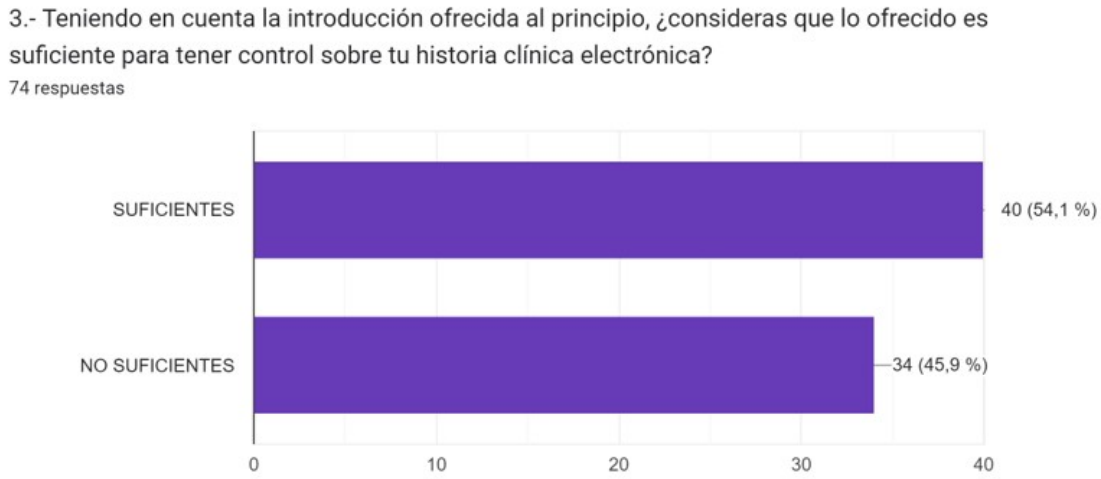

Figura 5.10: Respuesta a pregunta 3

La Figura 5.11 muestra el resultado de la pregunta 4.a. La mayoría de los encuestados (casi el 65 %) respondieron la opción de prioridad ALTA. Con este porcentaje se entiende que desean tener la posibilidad de conocer cuando un profesional de la salud accede a su historial médico, en los casos que no se tiene cita agendada.

Figura 5.11: Respuesta a pregunta 4.a

La Figura 5.12 muestra el resultado de la pregunta 4.b. La mayoría, den-

tro de las dos prioridades media/alta consideran que es bueno especificar por tiempo determinado el acceso a un profesional de salud acceder a su HCEN.

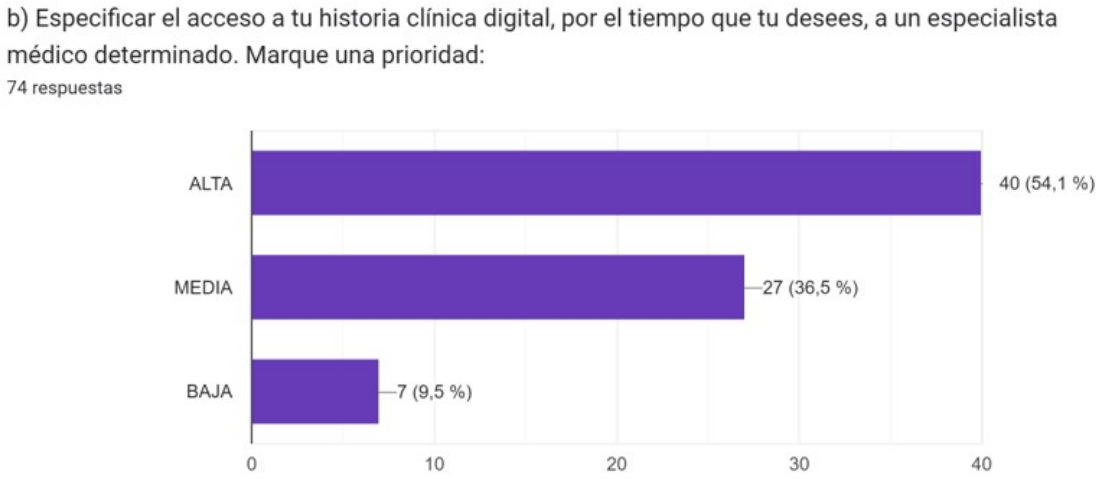

Figura 5.12: Respuesta a pregunta 4.b

La Figura 5.13 muestra el resultado de la pregunta 4.c. En este caso, también la mayoría dentro de las dos prioridades media/alta consideran que es bueno especificar acceso a determinadas partes de su HCEN a un profesional de salud. Esto hace pensar que la mayoría de los encuestados ven positivo tener más control granular sobre sus datos médicos.

Figura 5.13: Respuesta a pregunta 4.c

La Figura 5.14 muestra el resultado de la pregunta 4.d. Se puede observar que la mayoría de los encuestados, casi el 80 % ven de alta prioridad tener la posibilidad de designar a un tutor para tener control sobre su HCEN.

Figura 5.14: Respuesta a pregunta 4.d

La Figura 5.15 muestra el resultado de la pregunta 5. Si bien los seguros de cobertura de viajero cubren la salud de cada usuario, se puede observar que la mayoría de las respuestas brindadas entre la prioridad media/alta, consideran que sería bueno tener la posibilidad de habilitar su HCEN a la Institución de salud que brinda cobertura mediante el uso del seguro de viajero contratado.

Figura 5.15: Respuesta 5

La Figura 5.16 muestra el resultado de la pregunta 6. La gran mayoría consideran de interés disponibilizar su historial médico para la ayuda de otros, en base a estudios académicos y quizás así, encontrar respuestas más acertadas a determinados casos de enfermedades que se descubren.

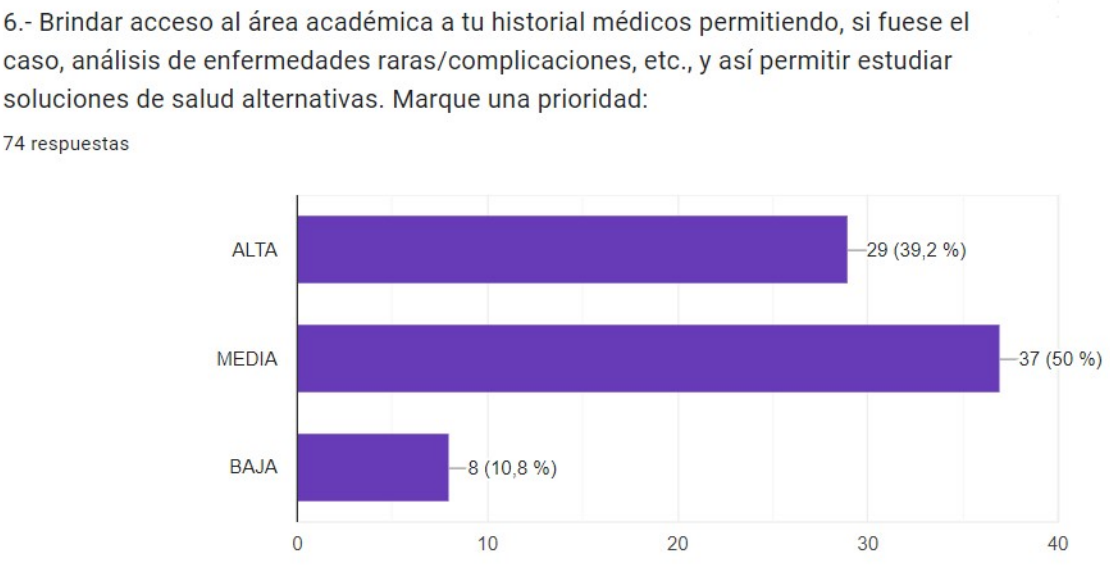

Figura 5.16: Respuesta a pregunta 6

La Figura 5.17 muestra el resultado de la pregunta 7. Casi el 100 % de los encuestados ven positivo y necesario que la historia clínica esté informatizada y sea única a nivel nacional sin depender de la Institución de salud a la cual pertenecen.

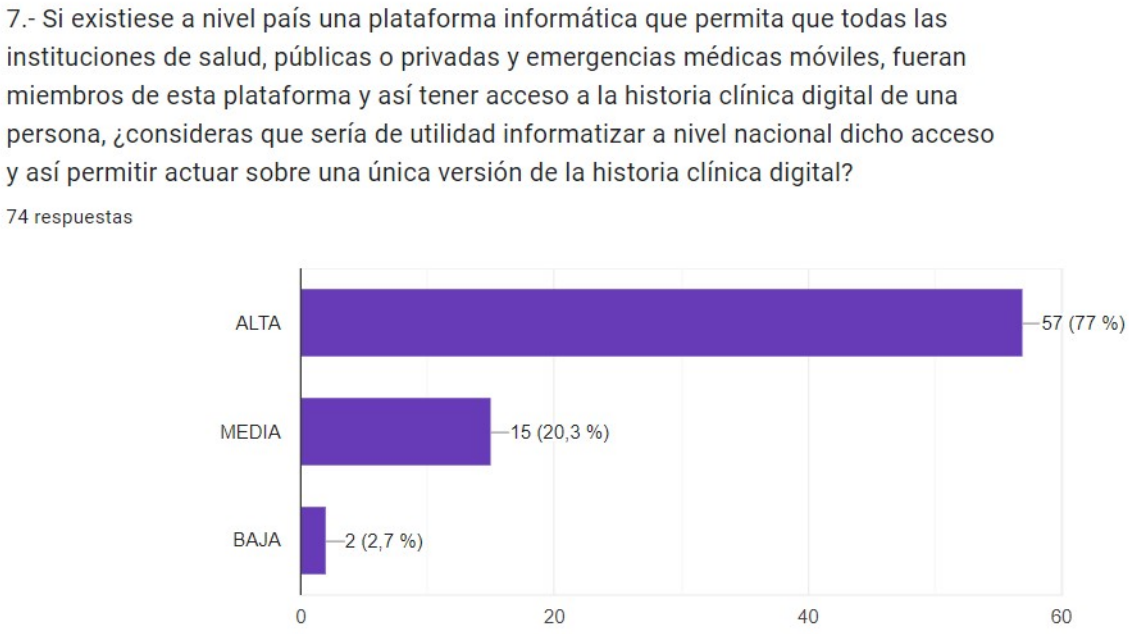

Figura 5.17: Respuesta a pregunta 7

5.2.2.1. Comentarios adicionales de las respuestas

A continuación se comparten los comentarios adicionales realizados en la pregunta abierta (numerada como 8).

1. Conocer el nivel de los actuantes de mis legajos o historial de salud.

2. Poder acceder sin restricciones de nivel a toda mi historia clínica y exámenes clínicos.

3. Me interesa que se pueda unificar toda historia clínica, pero siempre que el usuario sea el que tiene el control de lo que quiere mostrar, salvo en caso de emergencia o riesgo de vida. En ese caso la institución podría acceder a la historia clínica en su totalidad.

4. Tengo conocimiento que una empresa privada estaba ofreciendo este servicio en algún momento, pero luego tuvieron problemas con las habilitaciones gubernamentales.

5. Cuanto mayor acceso se tenga, siempre y cuando respetando determinadas privacidades del paciente, será de mayor provecho para su salud, así como estudios y controles actuales como para la prevención de posibles enfermedades y así mismo para el estudio de determinados casos específicos que sean de utilidad para futuros pacientes.

6. Es muy importante tener la posibilidad de acceder a tu historia clínica. Lo digo porque fui una de las perjudicadas por el cierre de Casa Galicia y al día de hoy mi mutualista actual no cuenta con datos de importancia.

7. Interesante el proyecto. ¡Saludos!

8. Muy interesante. No tenía conocimiento de la existencia. Gracias

5.2.3. Análisis de resultados

Los resultados de la encuesta permiten ver que el aplicativo del Estado **Mi Historia Clínica Digital** es poco conocido entre los usuarios encuestados (casi el 79 %). Independientemente de ello, el 100 % de los encuestados consideran que es de suma importancia poder acceder a su historia clínica.

Además la encuesta permitió conocer que la mayor parte de los encuestados consideran que lo que brinda dicho aplicativo es suficiente. Se entiende entonces que si su difusión fuese más amplia, su uso sería altamente mayor a lo que puede estar siendo hoy en día. De todas formas, complementando con la visión general de la encuesta y las funcionalidades agregadas, potenciar la herramienta sería muy bienvenido por los encuestados.

La mayor parte de los encuestados consideran que es muy importante tener control para permitir el acceso a un determinado especialista a sus datos clínicos, como también acceso para visualizar determinados estudios y actuaciones médicas de su HCEN. Esta respuesta permite ver que los usuarios efectivamente quieren tener acceso y control sobre su información clínica, teniendo la posibilidad para gestionar estos accesos.

La mayor parte de los encuestados desearían contar con la posibilidad de poder otorgar permisos sobre su historial clínico a una persona de su confianza,

como también controlar el acceso cuando se trata de un seguro de viajero. Esto aporta información valiosa en cuanto a la solución propuesta a la plataforma actual. A nivel usuarios, sería muy positivo tenerlo.

Como comentario adicional, luego de haber hablado personalmente con algunos de los encuestados, se detectó que ven como muy necesario el poder acceder a su historia clínica en todo momento. Las respuestas abiertas permiten ver algo clave que ha sucedido a nivel país (el de la mutualista Casa de Galicia). En este caso los usuarios se vieron fuertemente afectados, no solo por el cierre en si mismo de su Institución de salud, sino los problemas que surgieron para que se puedan hacer de su propia historia clínica.

5.3. Reunión con Salud.Uy

Esta sección describe la reunión que se realizó con Salud.uy que permitió presentar este trabajo de tesis sobre Privacidad de Datos en la HCEN para su validación e interés, con el fin de obtener retroalimentación sobre la propuesta.

5.3.1. Datos Generales de la Reunión

Por AGESIC/Salud.uy: Mauricio Bouza, Sabrilla Sellanes, Arianne Palau
Por Maestría CPAP: Dra Laura González
Estudiante: Ing. Silvanna Chakeyian
Fecha: Viernes 27 de Agosto, 2021 – 9:30 a 11:00hrs
Modalidad: Zoom

La reunión se dividió en dos partes principales: presentación del trabajo de tesis y consultas e intercambio.

5.3.2. Presentación del Trabajo de Tesis

En la primera parte de la reunión se presenta el trabajo de tesis a Salud.uy, realizando consultas enfocadas en:

- Validar lo que se tiene analizado y construido hasta el momento
- Entender la situación actual en Uruguay sobre la HCEN
- Ver si son de interés las propuestas del trabajo de tesis
- Existe una hoja de ruta para los temas que identificamos como principales

Al presentar el trabajo, Salud.uy realiza algunas acotaciones:

- En el diagrama donde se mostaron los distintos actores (p. ej. pacientes, médicos), se sugirió que quede explícita la figura del tutor de la HCE.
- Se sugiere aclarar que las funcionalidades que se brindan por la solución son para personas mayores a 18 años de edad y que no son dependientes de un mayor a cargo.
- En la unidad de URGENCIAS de cualquier Institución médica, sea que la historia clínica sea digital o en papel, en caso de requerir, se utiliza el *Breaking the Glass* (ver Sección 3.3).

5.3.3. Consultas e intercambio

Se comenta que, en el contexto que un médico quiera acceder a una HCEN y esté restringido por el usuario, el médico puede acceder pero generando una petición al usuario para otorgarle permisos sobre la HCEN y que él pueda observar lo que necesite para posterior atención al paciente.

También se manifestó que han analizado la posibilidad que el consentimiento sea a nivel de Institución de salud, no a nivel del médico, pero se identificaron varios temas a resolver por lo que aún no se ha abordado.

Se manifestó también que existen muchos desafíos para el inicio de sesión en la plataforma de accesos, por lo que se sigue estudiando el tema.

Se consulta al equipo de Salud.uy si se puede iniciar sesión con la CI al portal, ¿se puede acceder a toda la HCEN?

Salud.uy menciona que si, pero no es completa, puede no estar completamente digitalizada. Sobre el año 2018 se comenzó a digitalizar y por ley, pueden tener la historia clínica guardada en papel y es un respaldo también, no están obligados a digitalizar en su totalidad. También sucede que hojas de la historia clínica de hace mucho tiempo, estén ilegibles. Además, la digitalización es un trabajo manual y pueden introducirse errores.

Se maneja la idea sobre las recetas médicas, poder generar un código QR para despachar los medicamentos.

Se comentó también los tres niveles de permisos en la plataforma de accesos, descriptos en la Sección 2.2.3.1.

Habilitar permisos por médico: es todo un tema a analizar y profundizar, ya que no es un tema sencillo e involucra datos sensibles.

Habilitar permisos por estudio clínico: Pueden existir problemas tecnológicos para dar solución a esto, pero no es imposible, es cuestión de análisis. Se ha estudiado mucho esto y se han formado grandes debates al respecto. Puede quedar como un trabajo a futuro, hoy la mecánica de usuario no podría ser viable implementarlo, pero es bueno dejarlo planteado.

Acceso granular de una especialidad: se ha conversado mucho el tema, puede ser que llegue a generarse fragmentación de la HCEN. Pero es cuestión de volverlo a estudiar y analizar alternativas.

Se consulta al equipo de Salud.uy, ¿qué estándar están manejando para la definición?

El equipo de Salud.uy comentan que en cuanto a estánderes de control de acceso, se utilizaba XACML. De BPPC y APPC se tomaron como referencia lo mejor de ellos dos, pero solo de base, el fuerte es el XACML.

En cuanto a comunicación transfronteriza, el equipo de Salud.uy mencionan que no hay nada implementado, si bien se ha hablado. Uno de los participantes comenta que estuvo participando en el proyecto de RACSEL, sobre el año 2018.

Existen complejidades al respecto: Estándares - semántica, leyes, normas. Terminología - arquitectura, accesos de integración.

Piensan que se puede lograr accediendo cada Institución de salud de cada país integrante de la plataforma con una URL + token 24hrs. Pero es una posibilidad, no la solución definitiva.

Hoy en día si una persona recibe atención médica en el exterior, trae la información de la atención recibida, si quiere le puede solicitar a la Institución de salud que la adjunte a su historia clínica.

También se mencionó que otros terceros que hoy acceden a la HCEN es el Fondo Nacional de Recursos[1] y el Banco de Seguros del Estado[2]. Se conectan a la plataforma con link + token 24hrs. El Hospital de Clínicas[3] está conectado a la plataforma, de igual manera que se mencionó anteriormente, pero su parte clínica solamente, no la parte de trasplantes y otras áreas del hospital. La

[1] https://www.fnr.gub.uy/
[2] https://www.bse.com.uy/portal-comercial
[3] https://www.hc.edu.uy/

sección de quemados del hospital está conectado, pero no el Centro Nacional del Quemado[4]. Se expone el tema del Juez, AGESIC indica que de implementarlo, sería de gran interes.

Todo estos puntos se analizaron pero no se han implementado aún, se expusieron como aportes de tesis de la presente maestría. Se entiende que el equipo de Salud.uy ha mostrado interés en los temas tratados, pero para su implementación real se considera que cada tema es una tesis de por sí. El equipo de la presente tesis es consciente de eso, pero esta tesis tiene el aporte del análisis, no hace foco en la implementación profunda, por eso mismo, son temas complejos que llevan mucho análisis junto a un equipo multidisciplinario en las distintas áreas.

[4] https://www.cenaque.org.uy/

Capítulo 6

Conclusiones y Trabajo futuro

En este capítulo se presentan las conclusiones de la tesis y posibles trabajos a futuro. En primer lugar, en la Sección 6.1 se presenta el resumen del trabajo realizado y sus principales contribuciones. Luego, en la Sección 6.2 se describen algunas problemáticas y desafíos identificados a lo largo del trabajo. Por último, en la Sección 6.3 se comentan posibles trabajos a futuro.

6.1. Resumen y Contribuciones

En la actualidad, en Uruguay, existe la Plataforma Salud.uy que permite a los usuarios de servicios de salud acceder a su historia clínica, consultar accesos a dicha historia y realizar una configuración básica de privacidad.

Esta tesis propone una extensión a dicha Plataforma permitiendo un nivel mayor de granularidad en las configuraciones de privacidad. Para esto, en primer lugar se realizó un relevamiento y análisis del conocimiento existente vinculado a la privacidad de datos en una HCE.

La presente tesis ha profundizado en un estudio nacional e internacional sobre el control de acceso granular en la historia clínica electrónica, tanto en la Unión Europea (UE) como en otros países de América Latina, para conocer la realidad actual y así, tener una idea aproximada de cómo está posicionado Uruguay al respecto.

Sobre el estudio en la UE, se describieron técnicas en el intercambio transfronterizo que se entiende pueden ser muy útiles su implementación en Uruguay, para aplicar en principio, con sus países limítrofes y así extender funcionalidades de la Plataforma de Salud.uy.

Sobre el estudio en países de América Latina, se observó que el avance de la HCE es heterogéneo pero sin mucho soporte en privacidad. Se destaca Uruguay en la disponibilidad de información pública vinculada a la HCEN.

Este relevamiento, tanto en UE como en los países de América Latina, aportó a este trabajo de tesis un mayor entendimiento de la temática, pero no se identificaron soluciones que se pudieran aprovechar para este trabajo.

En segundo lugar, se identificaron cinco requerimientos de privacidad de datos en el contexto de la Plataforma Salud.uy. Por otro lado, se identificaron dos requerimientos adicionales, en el contexto de notificaciones y acceso a la HCEN en situaciones de emergencia.

En base a estos requerimientos, se proponen soluciones que extienden las que actualmente se brindan en la HCEN de Uruguay, a nivel de la Plataforma Salud.uy. Estas soluciones propuestas comprenden el diseño tanto de interfaces gráficas como de políticas de control de acceso, más concretas para que el paciente pueda tener más control granular sobre su privacidad. Las políticas están basadas en el estándar eXtensible Access Control Markup Language (XACML), utilizando el lenguaje Formal Access Control Policy Language (FACPL). Estas políticas constituyen la extensión de la Plataforma Saluy.uy. A nivel de la aplicación web actual **Mi Historia Clínica Digital** de Salud.uy, estas nuevas interfaces gráficas dan soporte a nuevas funcionalidades que permiten extender dicha aplicación web.

Las soluciones se evaluaron mediante la ejecución de casos de prueba en base a FACPL, encuesta preliminar a usuarios, y reunión con Salud.uy. Los casos de prueba se generaron con el fin de verificar que las políticas retornan la evaluación esperada. Sobre la encuesta preliminar a usuarios, los objetivos de la misma fueron: indagar qué tanto se conoce a nivel general la actual aplicación **Mi Historia Clínica Digital** de Salud.uy, y como parte de validación de algunos requerimientos identificados, previo a la propuesta de solución. Sobre la reunión con el equipo de Salud.uy, se mostraron interesados con los temas que se tratan en la presente tesis, los desafíos y los posibles trabajos a futuros a realizar.

6.2. Algunas problemáticas y Desafíos Identificados

El trabajo realizado permitió reflexionar acerca de algunos aspectos que se consideran clave en cuanto a aspectos de privacidad de datos en el área de la salud.

De acuerdo a los trabajos seleccionado, analizados en el estudio de la HCE en otros países, Uruguay refleja un gran avance al respecto. Se entiende así porque es el que tiene más información pública disponible y eso permite hacer esta valoración. No se ha encontrado información relevante de los otros países para poder destacar o mencionar más fehacientemente que incorporaron los cambios y procesos para lograr un avance tal de la HCE como se ha visto en Uruguay.

Una problemática encontrada en el estudio realizado, fue que tanto Uruguay como Argentina han sido los países que más detallaron de forma pública la normativa aplicada a las HCE. De los demás países que conformaron el estudio, no se ha encontrado información que pueda valorarse. Puede especularse que no todo fue expuesto en los trabajos recogidos para el desarrollo del presente estudio, pero fueron lo suficiente para dar una noción sobre las normas que se utilizan. En líneas generales todos los países tienen claro que deben tratar fuertemente la privacidad apoyándose no solo en la normativa vigente y establecida en su país, sino también en las TIC's para lograr tal fin, estableciendo mecanismos para facilitarlo.

El estudio realizado para la presente tesis, permitió conocer sobre políticas de accesos, protección de datos, legislación y terminología en común, junto con una serie de pasos que cumplen al momento de compartir de forma transfronteriza la HCE, siendo válidas las intervenciones médicas en otros países como si sucediera directamente en el país origen. Respecto a la semántica, debe ser interpretada de igual manera en todos los países que participen ya que está fuertemente ligada con la protección de datos, legal y normativo de cada país. Estos son grandes desafíos a tratar.

Otro desafío que se encontró, es que en base a los trabajos seleccionados, los países que componen el estudio contemplan hacia dónde deben apuntar con el intercambio de HCE entre prestadores de salud, teniendo en cuenta que es

crucial para brindar un servicio completo a nivel país a sus ciudadanos, siendo un gran desafío la estandarización e interoperabilidad.

Como se pudo observar según el estudio realizado, el avance en los países analizados es heterogéneo pero sin mucho soporte en privacidad. Se destaca Uruguay en la disponibilidad de información pública vinculada a la HCEN. El relevamiento aportó a este trabajo de tesis un mayor entendimiento de la temática, pero no se identificaron soluciones que se pudieran aprovechar para este trabajo. En el marco jurídico, se entiende que Uruguay en comparación con otros países analizados, está muy bien posicionado, basándose en un marco jurídico amplio. En cuanto a la conexión a Internet, se ha podido observar que es un problema muy común que tienen los países estudiados, este punto es una ventaja en Uruguay, si bien el servicio de Internet se entiende no está aún instalado en el 100 % del territorio nacional, es un servicio que está creciendo y expandiéndose a todos los puntos del país, de forma acelerada.

Un tema que se considera muy útil y es todo un desafío para desarrollar e implementar es la creación de capacitaciones tanto para personal de la salud como para pacientes. Entendemos que es fundamental brindar capacitaciones de forma nacional mediante una plataforma de conocimientos, sobre la HCEN, su funcionamiento y lo que implica la gestión de los permisos.

Si bien en el presente trabajo de tesis no se ha ahondado sobre el desarrollo de la solución técnica de las extensiones propuestas para la Plataforma, se entiende que tienen un tenor importante sobre los desafíos que puede presentar, principalmente sobre la complejidad técnica de estas extensiones propuestas, no solo para usuarios finales, sino también para el equipo técnico de la Plataforma.

6.3. Trabajo Futuro

A partir del trabajo realizado, se identificaron algunas líneas de trabajo a futuro.

En Uruguay hoy en día, no se han encontrado trabajos académicos o científicos que permitan conocer si actualmente se han realizado primeras experiencias sobre la comunicación transfronteriza entre países, como tampoco un caso de éxito al respecto. En este contexto, una línea de trabajo a futuro sería que la Plataforma Salud.uy brindara la posibilidad del soporte para la comunicación

transfronteriza, entre Uruguay y países limítrofes, como primer avance.

Otra línea de trabajo a futuro se generó a partir de una entrevista informal con una persona profesional en leyes, quien explicó la situación de los jueces frente a casos que surgen de temas relacionados con la HCEN de una persona: el Juez actualmente no tiene forma de visualizar online la HCEN. En este contexto sería de interés que la Plataforma Salud.uy brindara la posibilidad del soporte para la comunicación entre el Poder Judicial y las Instituciones de salud del país, como primer avance.

Un tema que se considera muy útil para desarrollar como trabajo a futuro es la creación de capacitaciones tanto para personal de la salud como para pacientes. Éstos podrían recibir una formación sobre la gestión de la privacidad de datos y así entender qué implica cuando un paciente configura sus accesos, lo que transcurre detrás de ese proceso y el impacto que tiene en líneas generales. A su vez, brindar capacitaciones de forma nacional mediante una plataforma de conocimientos, sobre la HCEN, su funcionamiento y lo que implica la gestión de los permisos.

Un tema que se considera útil desarrollar como otra línea de trabajo a futuro sería poder generar otras instancias de validaciones con el equipo de Salud.uy y usuarios finales del sistema de salud, sea público o privado. Para evaluar desde otra óptica el desarrollo de la solución propuesta para la Plataforma Salud.uy, más completa de como se realizó al inicio del trabajo de tesis.

Sumado a esta línea de trabajo, sería de aporte realizar más pruebas sobre las políticas desarrolladas específicamente para los requerimientos destacados, generando más casos de prueba y a su vez, combinando políticas de varios requerimientos. También sería de aporte analizar el comportamiento y perfeccionamiento de las mismas, así como el poder implementar un prototipo de las soluciones propuestas vinculado con la actual Plataforma Salud.uy.

A su vez, otras líneas de trabajo a futuro identificadas para la Plataforma Salud.uy, son: disponibilidad en varios idiomas (al menos en inglés y español), como también proporcionar un chatbot para guiar al paciente en el uso de la Plataforma.

Referencias bibliográficas

[1] IMPO, *Ley Nº 18335. Derechos y Obligaciones de pacientes y usuarios de los servicios de salud.* Fecha consulta: 12 de junio, 2021, ago. de 2008. dirección: https://www.impo.com.uy/bases/leyes/18335-2008.

[2] AGESIC, «Agencia Digital Uruguay 2011-2015,» abr. de 2017.

[3] J. Abin, H. Nemeth e I. Friedmann, «Systems architecture for a nationwide healthcare system. In MEDINFO 2015: eHealth-enabled Health - Proceedings of the 15th World Congress on Health and Biomedical Informatics,» São Paulo, Brazil, ago. de 2015, págs. 12-16.

[4] S. Pidre, L. González, R. Mendoza y col., «A data quality aware enterprise service bus for e-Health integration platforms,» en *2017 XLIII Latin American Computer Conference (CLEI)*, IEEE, 2017, págs. 1-10.

[5] J. Fernandez-Aleman, I. C. Señor, P. Oliver Lozoya y A. Toval, «Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics,» 2013, 46(3):541-562.

[6] O. Heinze, M. Birkle, L. Köster y B. Bergh, «Architecture of a Consent Management suite and Integration Into IHE-Based regional health information networks. BMC Medical Informatics and Decision Making,» oct. de 2011, 11(1):58.

[7] C.-Y. Yang, C.-T. Liu y T.-W. Tseng, «Design and implementation of a privacy aware framework for sharing electronic health records,» en *2015 International Conference on Healthcare Informatics*, IEEE, 2015, págs. 504-508.

[8] T.-W. Tseng, C.-Y. Yang y C.-T. Liu, «Designing privacy information protection of electronic medical records,» en *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, 2016, págs. 75-80.

[9] M. Jayabalan y T. O'Daniel, «Access control and privilege management in electronic health record: a systematic literature review,» *Journal of medical systems*, vol. 40, n.º 12, págs. 1-9, 2016.

[10] A. Zhang, A. Bacchus y X. Lin, «Consent-based access control for secure and privacy-preserving health information exchange,» *Security and Communication Networks*, vol. 9, n.º 16, págs. 3496-3508, 2016.

[11] Salud.uy, *Accesos Salud.uy*, 2018. dirección: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/accesos-salud-uy.

[12] «Historia Clínica Electrónica en América Latina. 5G Américas.,» Fecha consulta: 23 de mayo, 2020, jul. de 2019. dirección: https://brechacero.com/wp-content/uploads/2019/07/HCE-America-Latina-ESP.pdf.

[13] J. Salvador, *Historia Clínica Electrónica*. Fecha consulta: 01 de diciembre, 2022. dirección: https://www.gestion-sanitaria.com/1-historia-clinica-electronica.html.

[14] K. Häyrinen, K. Saranto y P. Nykänen, «Definition, structure, content, use and impacts of electronic health records: a review of the research literature,» *International journal of medical informatics*, vol. 77, n.º 5, págs. 291-304, 2008.

[15] L. Alarcon, C. Rubio y M. Chumán, «Interoperabilidad de Historias Clínicas Electrónicas en el Perú. Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática.,» Lima, Perú., inf. téc., 2019, Fecha consulta: 28 de abril, 2020. dirección: https://revistasinvestigacion.unmsm.edu.pe/index.php/rpcsis/article/download/16359/14137/.

[16] A. Shabo (Shvo), «Clinical Document Architecture,» en *Encyclopedia of Database Systems*. Boston, MA: Springer US, 2009, págs. 353-354, ISBN: 978-0-387-39940-9. DOI: 10.1007/978-0-387-39940-9_59. dirección: https://doi.org/10.1007/978-0-387-39940-9_59.

[17] H. Standard, *CDA – Clinical Document Architecture*, 2013. dirección: https://www.hl7.org.uk/standards/hl7-standards/cda-clinical-document-architecture/.

[18] J. Gil Yacobazzo y M. Viega Rodríguez, «Historia clínica electrónica: confidencialidad y privacidad de los datos clínicos. Rev. Méd. Urug. Vol. 34, nro 4.,» dic. de 2018. dirección: http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S1688-03902018000400102.

[19] E. P. Forum, *The new EU Regulation on the protection of personal data: what does it mean for patients?*. 2014-2020. dirección: https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf.

[20] D. Sign, *Control de acceso: qué es y cómo ayuda a proteger nuestros datos*, Fecha consulta: 12 de julio, 2022, oct. de 2021. dirección: https://www.docusign.mx/blog/datos-sensibles.

[21] U. R. de control de datos personales, «Protección de datos en salud,» AGESIC, inf. téc., dic. de 2018.

[22] S. D. C. d. Vimercati, S. Foresti y P. Samarati, «Recent Advances in Access Control,» en *Handbook of Database Security: Applications and Trends*, M. Gertz y S. Jajodia, eds. Boston, MA: Springer US, 2008, págs. 1-26, ISBN: 978-0-387-48533-1. DOI: 10.1007/978-0-387-48533-1_1. dirección: https://doi.org/10.1007/978-0-387-48533-1_1.

[23] Microsoft, «Control de Acceso Definido,» inf. téc., Fecha consulta: 30 de noviembre, 2022. dirección: https://www.microsoft.com/es-es/security/business/security-101/what-is-access-control.

[24] GrupoAtico34, «Control de Acceso. Definición, objetivos y tipos,» inf. téc., Fecha consulta: 30 de noviembre, 2022. dirección: https://protecciondatos-lopd.com/empresas/control-de-acceso/.

[25] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo y J. Voas, «Attribute-based access control,» *Computer*, vol. 48, n.º 2, págs. 85-88, 2015.

[26] O. Standard, *extensible access control markup language (xacml) version 3.0*, 2013.

[27] L. González, «A Comprehensive and Policy-based Approach to Compliance Management within Inter-organizational Service Integration Platforms,» Doctorado en Informática - PEDECIBA, Facultad de Ingeniería, Universidad de la República, Uruguay, abr. de 2019.

[28] T. rep. Organization for the Advancement of Structured Information Standards, *OASIS. eXtensible Access Control Markup Language (XACML) version 3.0.* 2013. dirección: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[29] A. Margheri, M. Masi, R. Pugliese y F. Tiezzi, «A Rigorous Framework for Specification, Analysis and Enforcement of Access Control Policies,» *IEEE Transactions on Software Engineering*, págs. 1-1, 2017. DOI: 10.1109/tse.2017.2765640.

[30] A. Appenzeller, E. Kempler, E. Rode y J. Beyerer, «Enabling Data Sovereignty for Patients through Digital Consent Enforcement. In The 13th Pervasive Technologies Related to Assistive Environments Conference (PETRA '20).,» ACM, New York, NY, USA., jul. de 2020. dirección: https://dl.acm.org/doi/10.1145/3389189.3393745.

[31] I. I. I. (ITI), «Technical Framework. Volumen 1 (ITI TF-1) Integration Profiles,» inf. téc., jul. de 2020. dirección: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf.

[32] I. I. T. Committee, «IHE IT Infraestructure Technical Framework Supplement. Advanced Patient Privacy Consents (APPC).,» inf. téc., jul. de 2019. dirección: https://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf.

[33] H. Standard, *HL7 - FHIR*, 2022. dirección: http://www.hl7.org/fhir/.

[34] D. Jodi, M. Goldstein y A. Rein, «Consumer consent options for electronic health information exchange: policy considerations and analisys.,» mar. de 2010. dirección: https://www.healthit.gov/sites/default/files/choicemodelfinal032610.pdf.

[35] R. H. Q., «Patient Privacy, Consent, and Identity Management in Health Information Exchange.,» inf. téc., jun. de 2013. dirección: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4945174/.

[36] E. M. Meslin, S. A. Alpert, A. E. Carroll, J. D. Odell, W. M. Tierney y P. H. Schwartz, «Giving patients granular control of personal health information: using an ethics 'Points to Consider'to inform informatics system designers,» *International journal of medical informatics*, vol. 82, n.º 12, págs. 1136-1143, dic. de 2013. dirección: https://www.sciencedirect.com/science/article/pii/S1386505613001895.

[37] P. Altamirano, «Bioética. El principio de autonomía.,» abr. de 2006, Fecha consulta: 01 de mayo, 2021. dirección: http://www.colmed9.com.ar/Bioetica/PRINCIPIO_DE_AUTONOM%5C%C3%5C%8DA.pdf.

[38] AGESIC, *Arquitectura de referencia HCEN*, 2018. dirección: https://centroderecursos.agesic.gub.uy/web/arquitectura-salud.uy/.

[39] M. de Salud Pública - Dirección General del Sistema Nacional de Salud, «Configurar Acceso a Mi Historia Clínica Digital. GubUy.,» Fecha consulta: 16 de noviembre, 2020, mar. de 2020. dirección: https://www.gub.uy/tramites/configurar-accesos-mi-historia-clinica-digital.

[40] Racsel, *Modelo Institucional y Normativo para implementar salud electrónica*, Fecha consulta: 25 de febrero, 2020, abr. de 2018.

[41] M. Tonso, «E-Salud: La historia clínica electrónica en el mundo y en Argentina.,» 2014, Fecha consulta: 06 de abril, 2020. dirección: http://www.gecsi.unlp.edu.ar/documentos/tonso2.pdf.

[42] J. Lezcano y N. Olivera, «La Historia Clínica Electrónica: Entre la e-Salud y la Privacidad.,» 2010, Fecha consulta: 06 de abril, 2020. dirección: http://www.gecsi.unlp.edu.ar/documentos/HCE_entre_la_e-salud_y_la_privacidad.pdf.

[43] H. Usuaria, «Seguridad en la Historia Clínica Electrónica (HCE).,» Fecha consulta: 08 de abril, 2020. dirección: https://www1.hospitalitaliano.org.ar/#!/home/infomed/noticia/22842.

[44] A. Folgarait, *La historia clínica, última frontera de la privacidad.* Fecha consulta: 12 de abril, 2020, mar. de 2015. dirección: https://www.lanacion.com.ar/opinion/la-historia-clinica-ultima-frontera-de-la-privacidad-nid1779455.

[45] B. Donato, «La Historia Clínica Electrónica centrada en el paciente como componente fundamental para la gestión de un Sistema de Información de Salud.,» 2013, Fecha consulta: 20 de mayo, 2020. dirección: https://repositorio.udesa.edu.ar/jspui/bitstream/10908/934/1/%5C%5bP%5C%5d%5C%5bW%5C%5d%5C%20M.%5C%20Ges.%5C%20Donato.pdf.

[46] G. Hospitalaria, «Argentina: Implementar Historia Clínica Electrónica sería un cambio radical para el sistema de salud.,» 2016, Fecha consulta: 20 de mayo, 2020. dirección: https://clustersalud.americaeconomia.com/argentina-implementar-historia-clinica-electronica-seria-cambio-radical-sistema-salud.

[47] M. Loewy, «Argentina formaliza su Red Nacional de Interoperabilidad en Salud. E-Health Reporter,» dirección: https://ehealthreporter.com/es/noticia/argentina-formaliza-su-red-nacional-de-interoperabilidad-en-salud/.

[48] G. C. Ministerio de Salud, *Chile ingresa a la Red para el Desarrollo de la Historia Clínica Electrónica Regional.* Fecha consulta: 22 de abril, 2020, oct. de 2014. dirección: http://www.salud-e.cl/destacados-home/chile-participara-en-la-presentacion-de-la-red-para-el-desarrollo-de-la-historia-clinica-electronica/.

[49] C. Salud, *El avance de la ficha clínica electrónica en Chile*, Fecha consulta: 22 de abril, 2020, ago. de 2016. dirección: https://clustersalud.americaeconomia.com/avance-la-ficha-clinica-electronica-chile.

[50] E.-H. Reporter, «Registro Clínico Electrónico: Requerimientos para la acreditación de calidad.,» inf. téc. dirección: https://ehealthreporter.com/es/noticia/registro-clinico-electronico-requerimientos-para-la-acreditacion-de-calidad/.

[51] J. Godoy Olave y J. Barraza Mesquida, «La ficha clínica mirada desde la legislación chilena actual.,» Fecha consulta: 24 de abril, 2020. dirección: https://scielo.conicyt.cl/pdf/abioeth/v24n2/1726-569X-abioeth-24-2-00181.pdf.

[52] M. de Salud, *Sistema de Informatización de la Red Asistencial: Ficha médica electrónica. Subsecretaría de Redes Asistenciales, Ministerio de Salud.* Fecha consulta: 25 de abril, 2020. dirección: http://www.agendadigital.gob.cl/#/seguimiento/medida/Sistema-de-Informatizacion-de-la-Red-Asistencial:-Ficha-medica-electronica.

[53] G. Muñoz, «La ficha clínica y la protección de datos de salud en Chile: Jurisprudencia. Superintendencia de Salud, Facultad de Derecho, Universidad de Chile.,» inf. téc., Fecha consulta: 26 de abril, 2020. dirección: https://adnz.uchile.cl/index.php/RCSP/article/download/47665/50037.

[54] C. Mansilla, *Del papel a la pantalla: cómo funciona la salud digital en Chile.* Fecha consulta: 26 de abril, 2020, ene. de 2019. dirección: https://www.latercera.com/pulso/noticia/del-papel-la-pantalla-funciona-la-salud-digital-chile/500421/.

[55] J. Carnicero e I. Abad, «Intercambio internacional de información clínica,» *En: Manual de salud electrónica para directivos de servicios y sistemas de salud. Santiago: CEPAL, 2012. p. 237-252. LC/L. 3446*, 2012, Fecha consulta: 05 de mayo, 2020.

[56] TrendTic, *Servicio de salud del país avanzan en iniciativas de interoperabilidad entre sus sistemas de información sanitaria.* Fecha consulta: 21 de mayo, 2020. dirección: https://www.trendtic.cl/2020/03/servicios-de-salud-del-pais-avanzan-en-iniciativas-de-interoperabilidad-entre-sus-sistemas-de-informacion-sanitaria/.

[57] C. de Colombia, *Ley Nº 201531ENE2020. Congreso de Colombia.* Fecha consulta: 17 de abril, 2020, ene. de 2020.

[58] C. Motoa, *Alcances de nueva ley sobre la Historia Clínica Electrónica. Congreso de la República de Colombia.* Fecha consulta: 19 de abril, 2020, feb. de 2020. dirección: http://www.senado.gov.co/index.php/prensa/lista-de-noticias/715-estos-son-alcances-de-nueva-ley-sobre-la-historia-clinica-electronica.

[59] Minsalud, *Interoperabilidad de Datos de la Historia Clínica en Colombia*, jul. de 2018. dirección: https://www.minsalud.gov.co/ihc/Documentos%5C%20compartidos/ABC-IHC.pdf.

[60] Redacción, «Con la historia clínica electrónica se modernizará sistema de salud en Colombia,» feb. de 2020. dirección: https://www.periodicolacampana.com/con-la-historia-clinica-electronica-se-modernizara-sistema-de-salud-en-colombia/.

[61] M. Benedetti Arzuza, *Análisis de las barreras para la unificación de una Historia Clínica Electrónica -HCE- en Colombia.* Fecha consulta: 21 de abril, 2020, 2016. dirección: https://repository.urosario.edu.co/bitstream/handle/10336/12122/BenedettiArzuza-Mario-2016.pdf?sequence=1&isAllowed=y.

[62] K. C. Jiménez, *Costa Rica alista su Estrategia Nacional de Privacidad.* Fecha consulta: 21 de abril, 2020, sep. de 2019. dirección: https://www.elfinancierocr.com/tecnologia/costa-rica-alista-su-estrategia-nacional-de/CJEUGVPUCVAU5B3JQTK335RGDY/story/.

[63] L. E. (2019), *Seguro Social de Costa Rica*, Fecha consulta: 29 de marzo, 2020, 2019. dirección: https://www.ccss.sa.cr/edus/informacion-edus.html.

[64] EFE, *Costa Rica implementa expediente médico digital en todos sus hospitales.* Fecha consulta: 21 de mayo, 2020, sep. de 2018. dirección: https://www.elpais.cr/2018/09/28/costa-rica-implementa-expediente-medico-digital-en-todos-sus-hospitales/.

[65] L. Sánchez, *Autoridades compartirán datos de expediente de salud y Sinirube para simplificar trámites.* Fecha consulta: 24 de mayo, 2020, ene. de 2020. dirección: https://observador.cr/noticia/autoridades-compartiran-datos-de-expediente-de-salud-y-sinirube-para-simplificar-tramites/.

[66] E. de Transformación Digital, *Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0. 2018 - 2022.* Fecha consulta: 24 de mayo, 2020, 2018. dirección: https://www.micit.go.cr/sites/default/files/estrategia-tdhcrb.pdf.

[67] M. de Salud, *Resolución Ministerial Nº 618-2019—MINSA. Ministerio de Salud, República del Perú.* Fecha consulta: 26 de abril, 2020, 2019. dirección: https://repositorio.udesa.edu.ar/jspui/bitstream/10908/934/1/%5C%5bP%5C%5d%5C%5bW%5C%5d%5C%20M.%5C%20Ges.%5C%20Donato.pdf.

[68] G. PanelG., *Se contará con el 70 por ciento de las historias clínicas electrónicas en el 2021.* Fecha consulta: 29 de abril, 2020, 2017. dirección: https://archivo.gestion.pe/panelg/se-contara-70-historias-clinicas-electronicas-2021-2197856.

[69] K. Sánchez, «Recuperación de Historias Clínicas Electrónicas a partir de un Repositorio Digital usando una Arquitectura Orientada a Servicios.,» Tesis de Grado. dirección: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/6315/SANCHEZ%5C_KATTY%5C_RECUPERACION%5C_HISTORIAS%5C_CLINICAS%5C_ELECTRONICAS.pdf%5C?sequence=1%5C&isAllowed=y.

[70] P. Legislativo, *Ley Nº 30024 Congreso de la República, Poder Legislativo*, Fecha consulta: 27 de abril, 2020, 2013. dirección: ftp://ftp2.minsa.gob.pe/normaslegales/2013/Ley30024.pdf.

[71] C. de la República, *Ley Nº 26842 Congreso de la República, Poder Legislativo*, Fecha consulta: 27 de abril, 2020. dirección: http://www.essalud.gob.pe/transparencia/pdf/publicacion/ley26842.pdf.

[72] E. Sánchez, *Aprobado el dictamen promovido por la Región para la creación de una historia clínica electrónica europea. Onda Regional.* Fecha consulta: 04 de mayo, 2020, feb. de 2019. dirección: https://www.orm.es/informativos/aprobado-el-dictamen-para-la-creacion-de-una-historia-clinica-electronica-europea/.

[73] I. Nova, *Los médicos españoles accederán a la historia de cualquier europeo en 2020.* Fecha consulta: 04 de mayo, 2020, abr. de 2019. dirección: https://www.redaccionmedica.com/secciones/ministerio-sanidad/los-medicos-espanoles-accederan-a-la-historia-de-cualquier-europeo-en-2020-6745.

[74] E. Global, *La e-receta interoperable se estrena en la UE.* Fecha consulta: 14 de mayo, 2020, ene. de 2019. dirección: https://elglobal.es/politica/la-e-receta-interoperable-se-estrena-en-la-ue-hf1887458/.

[75] FRA, *Manual de legislación europea en materia de protección de datos.* Fecha consulta: 23 de mayo, 2020, 2018. dirección: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf.

[76] H. Balanta, «Retos en la protección de datos personales en a Historia Clínica Electrónica. Escuela de Privacidad.,» inf. téc., Fecha consulta: 24 de mayo, 2020. dirección: https://escueladeprivacidad.com/

retos-en-la-proteccion-de-datos-personales-en-la-historia-clinica-electronica/.

[77] Y.-Y. Ke y D.-M. Liou, «Design and Implement an Electronic Health Records Platform Based on the Management of the Personal Consent,» HL7, 2010.

[78] Y. Kim y D. Baik, «Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System. IEEE Access.,» inf. téc., 2018. dirección: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8281074.

[79] J. Heurix, «Guía de Integración a la HCEN,» inf. téc., Fecha consulta: 10 de mayo, 2020. dirección: https://publications.sba-research.org/publications/Heurix_trustbus_2011.pdf.

[80] M. Yelen, «Control de acceso a la Historia Clínica Electrónica.,» Proyecto de grado, Facultad de Ingeniería, Universidad de la República, Uruguay, 2011.

[81] P. Ardanaz, R. Arocena y R. Delgado, «Plataforma de Integración de Servicios en el Área de la Salud.,» Proyecto de grado, Facultad de Ingeniería, Universidad de la República, Uruguay, 2013.

[82] G. Dr. Adriasola, *Protocolo. Ingreso y mantenimiento a lista de trasplante renal y reno – páncreas.* Ver. 001, Fecha consulta: 11 de junio, 2021, sep. de 2015. dirección: https://www.enfermeria.hc.edu.uy/images/pdf/formato_iso_protocolo_pre_trasplante.pdf.

[83] IMPO, *Ley Nº 14.005 (1971). Donación para uso con fines científicos y terapeúticos del cuerpo u órganos y tejidos. Registro Nacional de Donantes de órganos y tejidos.* Fecha consulta: 12 de junio, 2021, ago. de 1971. dirección: https://www.impo.com.uy/bases/leyes/14005-1971.

[84] G. Dr. Adriasola, *La inviolabilidad de la clínica médica: custodia de la intimidad del paciente y su historia.* Fecha consulta: 11 de junio, 2021, jul. de 2012. dirección: http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S1688-03902012000200007.

[85] IMPO, *Reglamentación de la ley Nº 18.335 sobre derechos y obligaciones de pacientes y usuarios de los servicios de salud.* Fecha consulta: 10 de junio, 2021, sep. de 2010. dirección: https://www.impo.com.uy/bases/decretos/274-2010.

APÉNDICES

Apéndice 1

RACSEL

En este apéndice se describe la iniciativa Red Americana de Cooperación sobre Salud Electrónica (RACSEL) en base a [40].

1.1. Descripción General

América Latina tuvo la necesidad de crear un espacio para la reflexión y compartir las experiencias de las HCE, generando las primeras recomendaciones de gobierno para apoyar el desarrollo, como también discutir sobre los principios de una integración regional. Es así como RACSEL ha logrado consolidar la experiencia, facilitando el desarrollo de la salud electrónica en la región, con énfasis en la HCE. Al momento de realizar este estudio en base a [40], sus miembros eran: Colombia, Costa Rica, Chile, Perú y Uruguay. Se desarrolla en el contexto de un bien público regional para el avance de la HCE en América Latina y el Caribe, con el apoyo del Banco Interamericano de Desarrollo (BID)[1]. Los principales temas en los que RACSEL ha trabajado, relacionados con la recopilación técnica, y ha dejado a disposición son: marco institucional y normativo para la HCE, arquitectura de sistemas de información de HCE, estándares de interoperabilidad en salud, terminologías farmacéuticas, receta electrónica y lineamientos de medición de TIC en salud. RACSEL ha iniciado un esfuerzo en que ha logrado reunir los fundamentos para que los países y la región avancen en los desarrollos de HCE, contando con una referencia fiel para sus propias iniciativas [40].

[1] https://www.iadb.org/es

1.2. Conceptos Fundamentales

La HCE comprende una serie de procesos y cambios estructurales en las organizaciones de la salud en cada país. No sólo se trata de una transformación tecnológica sino de un cambio de paradigma en la atención médica, generando un cambio radical en la forma de trabajo del personal de salud. Además de los cambios tecnológicos que implica, es necesario gestionar correctamente los factores de tipo humano para llevar a cabo una correcta implementación del proyecto [40].

La creación de determinados elementos como ser: un único Índice Maestro de Pacientes, disponibilidad de infraestructura, disponer de un servidor terminológico y de una plataforma de integración de aplicaciones en salud o promover cambios de orden legislativo, son compartidos por los países de la red, sea cual sea su tamaño o particularidades en sus sistemas de salud [40].

En el plano de las TIC, si bien buena parte de los países latinoamericanos disponen de iniciativas en marcha para mejorar dicha infraestructura, aún es amplio el margen de mejora. En este sentido, los planes estratégicos que permitan que todas las Instituciones de salud dispongan de un acceso adecuado, deben estar alineados con los proyectos de HCE, sin TIC no sería posible extender la HCE [40].

Cualquier proyecto de salud electrónica, plantea varias cuestiones sobre temas legales, éticos e institucionales. El desarrollo de marcos regulatorios en el ámbito de la seguridad de la información y la protección de datos ha seguido diferentes caminos en los distintos países. En algunos existen regulaciones específicas y en otros, regulaciones generales que incluyen aspectos relacionados con la salud [40].

Cual sea el caso, hay algunos aspectos fundamentales compartidos por diferentes regulaciones. Como regla general, la legislación sobre privacidad y seguridad debe considerar [40]:

- La identificación y el consentimiento del paciente.
- Deber de información al ciudadano, con conocimiento previo de la finalidad para la cual se le recogen sus datos.
- Medidas de seguridad en autenticación y validación de los profesionales que intervienen en todo el proceso.

Otro aspecto que no puede dejarse de lado es promoción y divulgación de

estándares HL7[1], DICOM[2] o los que adoptan las guías Integrating the Healthcare Enterprise[3] (IHE). A su vez, se hace imprescindible gestionar los vocabularios controlados, es decir, el *Servidor Terminológico*, para que los sistemas de información puedan identificar, comparar y operar con la información que se almacena en ellos. Este tipo de vocabularios es un lenguaje normalizado para representar conceptos, ya que el lenguaje médico es de difícil dominio [40].

1.3. Marco Normativo

El puntapié inicial de la regulación de la HCE, debe ser el paciente o el titular de la historia clínica y los derechos que sobre ésta corresponden, velando así por la protección de su información personal, tanto en su correcto uso y tratamiento. A su vez, es importante establecer una normativa que avale y respalde la validez de los documentos en papel con firmas ológrafas junto a los documentos y firmas electrónicas, estableciendo una equivalencia válida entre ambos [40].

En base a que la historia clínica, sea en formato papel o electrónico, contiene datos clínicos de personas, existe la necesidad de protección de sus datos personales. La protección de la privacidad e intimidad de las personas, se contemplan en las principales herramientas internacionales de derechos humanos, como ser *Pacto Internacional de los Derechos Civiles y Políticos*[1], *Pacto de San José de Costa Rica*[2] y la *Declaración Universal de los Derechos del Hombre*[3]. A pesar de esto, algunos países aplican una regulación específica para regular los datos personales de salud como datos sensible, que requieren el consentimiento del individuo para su tratamiento [40].

Es por ello que la protección de información de salud implica habilitaciones legales respecto a su comunicación o transferencia a terceros, incluso lo que se considera transferencia internacional de datos. Es indispensable, para que un sistema de historia clínica funcione a nivel nacional, que intercambie

[1] https://www.hl7.org.uk/

[2] https://www.dicomstandard.org/

[3] https://centroderecursos.agesic.gub.uy/web/arquitectura-salud.uy/inicio/-/wiki/Arquitectura+para+Salud/Marco+Normativo/pop_up?_com_liferay_wiki_web_portlet_WikiPortlet_viewMode=print

[1] https://www.coe.int/es/web/compass/the-international-covenant-on-civil-and-political-rig

[2] https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

[3] https://www.un.org/es/about-us/universal-declaration-of-human-rights

información clínica entre diferentes organizaciones de salud en cada país, por lo que es necesario dichas habilitaciones. Este intercambio debe cumplir con los principios de disponibilidad, integridad y confidencialidad de la información [40].

En la HCE pueden intervenir múltiples actores, por ello es necesario establecer mecanismos de identificación electrónica de éstos, asignando roles para gestionar los accesos tanto a los profesionales de la salud como a los pacientes. Para la red regional, se deben incluir métodos de autenticación e identificación, garantizar la compatibilidad entre otros sistemas tanto a nivel nacional como internacional, al menos con los países que forman parte de la red [40].

Para que sea posible la transferencia de la HCE entre los países que integran la Red, se deberá establecer una metodología o proceso para determinar la información mínima de intercambio. Será necesario regular legalmente esta necesidad y de instrumentación a través de la aplicación de estándares internacionales. La propia normativa de cada país establece particularidades en cuanto a transferencia de datos, exigiendo que el país que envíe datos de salud a otro, debe garantizar que el país destino dispone de las mismas medidas de seguridad o equivalentes en cuanto a protección de datos del país origen [40].

Apéndice 2

Detalles de BPPC y APPC

Este apéndice brinda detalles y casos de uso de los perfiles BPPC y APPC.

2.1. Consentimiento Básico de Privacidad del Paciente (BPPC)

2.1.1. Consentimiento implícito versus consentimiento explícito

Este perfil admite entornos de consentimiento implícito y explícito. En un entorno implícito, es normal que un consumidor de documentos no encuentre ninguna aceptación específica del paciente de una política de consentimiento de privacidad. Esto también puede ser cierto en un entorno de consentimiento explícito, donde la obtención del reconocimiento se retrasa debido a razones médicas (p. ej. emergencia) [31].

2.1.2. Limitaciones de BPPC

Pueden existir políticas jurisdiccionales u organizativas que requieren soporte para el consentimiento de privacidad del paciente más complejas. Estas políticas de privacidad pueden requerir que un paciente consienta explícitamente la divulgación de su información de salud protegida o sensible a entidades específicas. El perfil BPPC proporciona un punto de partida para implementar estos tipos de políticas de consentimiento de privacidad, pero no especifica explícitamente cómo se transmite la información necesaria para hacer cumplir

la política. En estos casos, la capacidad de BPPC puede no ser suficiente para soportar todo tipo de necesidades. Un ejemplo de consentimiento avanzado de privacidad del paciente sería cuando este quiere nombrar personas que puedan acceder a sus documentos [31].

2.2. Consentimiento Avanzado de Privacidad del Paciente (APPC)

Esta sección menciona algunos casos de uso que ilustran las capacidades de este perfil. No pretenden ser una lista exhaustiva de los esquemas de control de acceso/consentimiento del paciente admitido, ni pretenden ser una implementación particular. Todos los casos de uso comparten un nivel de complejidad que sería difícil de implementar con BPPC, por lo tanto, se ajusta mejor a este perfil [32].

2.2.1. Caso 1: Acceso específico en un proveedor de salud.

El paciente otorga acceso a sus datos al personal de un proveedor de salud específico. El alcance del acceso y las restricciones que lo acompañan se condensan en un patrón de acceso que el paciente selecciona para este proveedor.

Condición previa: Este caso de uso tiene lugar en un dominio específico, donde el acceso a la información de la historia clínica solo se otorga si el paciente acuerda explícitamente compartir documentos [32].

Flujo principal abreviado: Un paciente visita un proveedor de salud A porque necesita una intervención. Luego del procedimiento, el proveedor A desea organizar la atención posterior a la intervención, pero en otro proveedor B. El proveedor A cargó todos los datos relevantes sobre el procedimiento, un miembro del personal le pide al paciente que firme un formulario de consentimiento que autoriza al proveedor A a otorgar acceso a los datos de salud del paciente al proveedor B. El paciente puede elegir entre tres patrones de acceso, que se enumeran en el formulario: acceso *solo resumen*, *acceso general* y *acceso completo*. El paciente selecciona el *acceso general*, que incluye la mayoría de los análisis de laboratorio e imágenes, pero excluye documentos particularmente sensibles (p. ej. evaluaciones psiquiátricas). El paciente firma el formulario. El

miembro del personal selecciona al paciente en el sistema, busca al proveedor B en el directorio de proveedores de atención médica conectado, selecciona el centro y luego selecciona el patrón de *acceso general*. El sistema crea un documento de consentimiento de privacidad y lo transmite al repositorio central de documentos. Después del alta del proveedor A, se utiliza una política de consentimiento para decidir otorgar acceso al registro de pacientes del proveedor B. Los demás que no estén autorizados, no pueden acceder a los registros del paciente [32].

2.2.2. Caso 2: Retener el consentimiento para información relacionada a un pedido específico

Un paciente desea restringir la divulgación sobre un pedido específico que realizó, así como cualquier información resultante de dicho pedido.

Condición previa: Un paciente se dirige hacia un laboratorio central donde se guardan todos los pedidos y resultados de laboratorio. Utiliza un modelo de consentimiento implícito para la solicitud de información, lo que significa que el documento sería visible por defecto [32].

Flujo principal abreviado: El paciente acude a su prestador de salud para la detección de enfermedades de transmisión sexual. Dicho paciente es enfermero en un hospital local y le preocupa que sus colegas puedan tener acceso a la orden y a los resultados de las pruebas. El médico tratante solicita una serie de análisis clínicos para confirmar el diagnóstico. El paciente indica que le gustaría negar su consentimiento para la divulgación del pedido de análisis y los resultados posteriores. El médico ingresa el pedido en el formulario de pedido en línea de su laboratorio e indica que el paciente ha retenido su consentimiento para la divulgación. El repositorio de información del laboratorio genera una orden de laboratorio y un documento de consentimiento que especifica que el paciente desea denegar el acceso a la orden, excepto al médico que realiza el pedido. Si un colega intentara visualizar el registro del paciente, no podrá realizarlo ya que dicho pedido fue eliminado de los registros de búsqueda por el consentimiento solicitado. Este consentimiento permite que el médico tratante tenga acceso a la orden de laboratorio y al resultado. Otros prestadores de salud no tienen acceso a la orden y al resultado de laboratorio específico, pero pueden tener acceso a otras órdenes y resultados de laboratorio del paciente [32].

2.3. Condiciones de Privacidad y Seguridad

Los documentos de consentimiento se rigen por las políticas de privacidad al igual que los documentos clínicos de los pacientes. Un documento de consentimiento de privacidad puede contener información confidencial, por ejemplo, un paciente con enfermedad terminal puede decidir que su pronóstico no debe compartirse con sus familiares, sin embargo, otra información puede ser que si. Por lo tanto, el código de confidencialidad colocado en los documentos de consentimiento de privacidad debe asignarse adecuadamente. Otra opción es incluir reglas de acceso en dicho documento que regulen específicamente el acceso al documento de consentimiento en sí. Una estrategia de mitigación que a menudo se adopta en la atención médica es proporcionar responsabilidad a través de controles de auditoría. Se confía en que los proveedores de salud no abusen de su capacidad de acceder a la información privada del paciente, pero eso está respaldado por una política de monitoreo del acceso del proveedor para detectar si ha ocurrido un abuso [32].

Apéndice 3

Detalles adicionales del Enfoque PIPE

En este Apéndice se describe este trabajo relacionado [79], el cual fue estudiado al inicio del presente trabajo de tesis y resultó interesante por las temáticas tratadas. De acuerdo a [79] para la aplicación de la HCE es requerida la aplicación de TIC para respaldar los flujos de trabajos médicos, pero no solo esto, sino para mejorar la comunicación entre las diferentes Instituciones de salud. Las TIC proporcionan la infraestructura técnica para facilitar el intercambio de información y documentos al estar disponibles de forma digital al implementar la HCE, produciendo un nivel elevado en la calidad de la atención médica. Si bien existe un marco legal para la protección y divulgación de datos no autorizados, se requieren soluciones técnicas para evitar la divulgación de registros médicos a personas no autorizadas. Así mismo, el gran caudal de información digital que se genera en este contexto debe estar disponible para el uso, el análisis e investigación en el área de la salud.

3.1. Fundamentos

En esta Sección se describen los conceptos de anonimización, encriptación y pseudoanonimización, en base a [79], dado que son fundamentales para comprender el enfoque.

3.1.1. Anonimización

El anonimato y el cifrado son dos técnicas que se mencionan cuando se requiere confidencialidad y privacidad. La anonimización se refiere a eliminar el identificador de los datos médicos de manera que los registros no puedan rastrearse hasta el paciente correspondiente. Esta técnica se puede lograr mediante la eliminación de cualquier información que identifique al paciente de dichos registros. Esta desvinculación de manera "perfecta" no se puede lograr, donde el dueño de los datos no sea identificable en todos los escenarios. Una desventaja de esta técnica es que no se puede revertir, lo que significa que los datos de salud anonimizados no se pueden utilizar en la atención directa, donde el vínculo entre los datos de salud y el paciente correspondiente claramente debe conocerse por el profesional de la salud [79].

3.1.2. Encriptación

El cifrado de datos, es otra técnica que se emplea generalmente cuando se requiere la confidencialidad de datos. Al cifrarlos completamente con una clave secreta que solo el paciente conoce, se garantiza su privacidad. A diferencia del anonimato, el cifrado completo de datos es reversible, pero el principal problema es que el uso de los registros en una investigación está totalmente impedido, al menos que el paciente descifre explícitamente sus datos revelando así, su identidad [79].

3.1.3. Pseudonimización

La pseudonimización combina la potencia de la anonimización y el cifrado completo, logrando la desvinculación mediante la introducción de especificadores (llamados seudónimos) que no pueden asociarse con el paciente sin conocer un determinado secreto, el anonimato simple es reversible. De esta forma, con la previa despersonalización de los registros permite almacenar los registros en un estado anonimizado, mientras que este anonimato puede ser revertido por personas que conozcan la clave secreta. Si bien la pseudonimización se basa también en la criptografía, solo es necesario cifrar los metadatos para que la carga criptográfica sea menor [79].

La Figura 3.1 muestra la compensación existente entre privacidad y transparencia en cada técnica mencionada, representando la dificultad de mantener

la privacidad del paciente y la usabilidad de los datos [79].

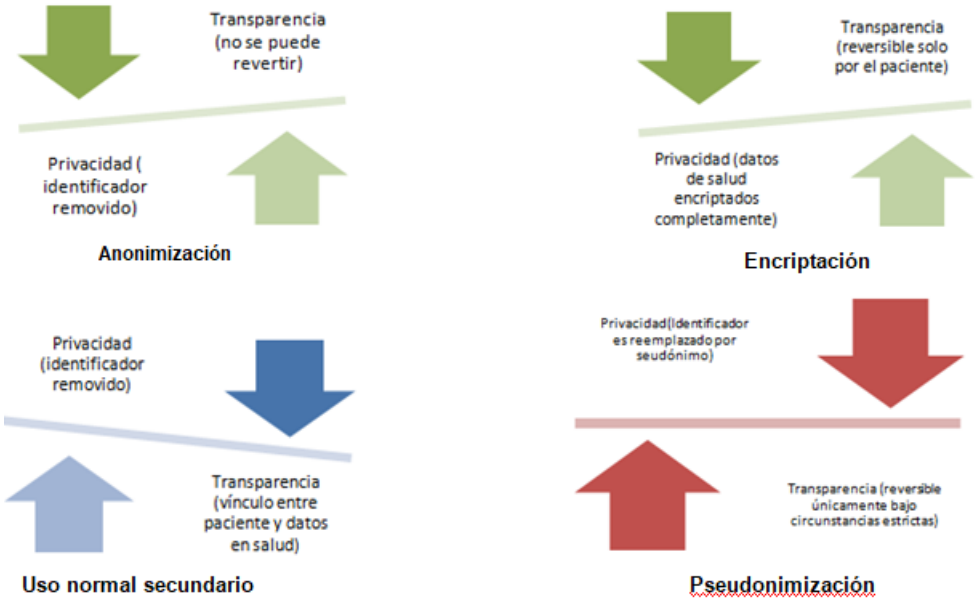

Figura 3.1: Pseudonimización – Equilibrio de conceptos [79].

3.2. Enfoque PIPE

Llamado PIPE por sus siglas en inglés (Pseudonymization of Information for Privacy in e-Health – seudonimización de la información para la privacidad en salud electrónica-) proporciona un almacenamiento y recuperación seguros preservando la privacidad de los datos médicos confidenciales. Básicamente muchos registros médicos por sí solos (p. ej. una tomografía), son insuficientes para identificar de forma unívoca la identidad del paciente después de la desvinculación. Pues entonces, esta información médica se separa de la información del identificador (nombre de paciente, identificador, etc.) y a ambos registros se le asigna un seudónimo de identificación y de salud al azar, formando una relación 1:1. Estos seudónimos funcionan como token de acceso y están protegidos por cifrado con clave secreta específica del usuario [79].

La estructura de datos seudonimizados PIPE proporciona dos "vistas" diferentes según las autorizaciones concedidas. Observando la Figura 3.2, en su lado izquierdo, representa la vista de datos para administradores y usuarios secundarios (no autorizados en términos de confidencialidad y privacidad de datos) o usuarios maliciosos. Si bien la identificación y los registros de salud

son claramente visibles para ellos, no pueden asociar los vínculos correctos entre los datos de salud pseudonimizados y los registros de identificación. Del lado derecho, están los usuarios autorizados (pacientes, Instituciones de salud y tutores) que pueden ver "a través" de la seudonimización y establecer los enlaces correctos (carpetas resaltadas) [79].

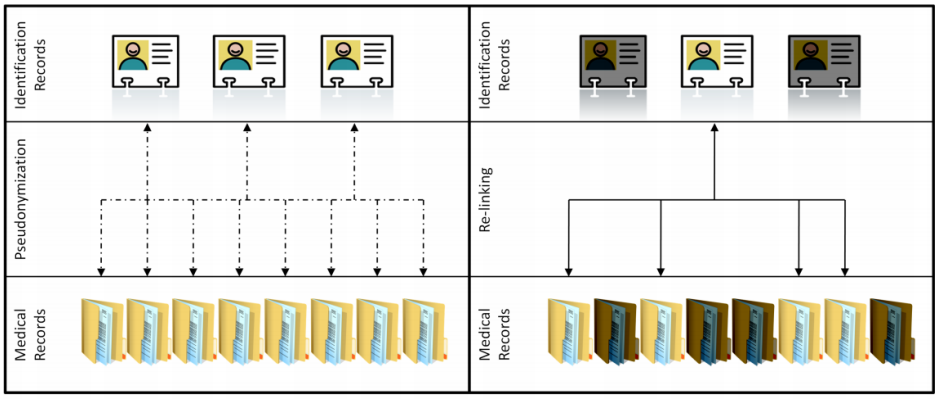

Figura 3.2: Vista pseudonimizada para personas autorizadas y no autorizadas [79].

Apéndice 4

Otras líneas de trabajo. Detalles adicionales

En esta sección se describen otras posibles líneas de trabajo, como ser que Uruguay se comunique de forma transfronteriza con sus países limítrofes en cuanto a disponibilizar la HCEN de sus pacientes. Si bien estas líneas se analizaron, quedaron por fuera del alcance de este trabajo de tesis.

4.1. Comunicación transfronteriza

Surge principalmente de los trabajos relacionados [55] [72] [73] y análisis con la tutora.

4.1.1. Contexto

Un número elevado de personas suele viajar de un país a otro, sea por temas laborales, vacaciones, estudio, tratamientos médicos, humanitarios, entre otros. El incremento de la movilidad en el país destino puede generar que se incremente la atención médica, en un país en el cual la persona no es residente. De requerirlo, la persona se atiende en un servicio de salud local, pero lo que el médico tratante genere en un archivo clínico, sea papel o electrónico, quizás no podrá adjuntarlo a su actual HCE.

Para que Uruguay establezca en el futuro una comunicación transfronteriza entre países limítrofes, se sugiere considerar una transmisión semántica equivalente como ser los marcos legales en la protección de datos, la identificación de los pacientes, de los productos farmacéuticos, entre otros [55] [72] [73].

4.1.2. Marco legal

Cada país es responsable de su sistema de salud y de garantizar la atención médica de sus ciudadanos, en base a leyes y regulaciones locales específicas para cumplir con la asistencia médica y esto varía de un país a otro. A pesar de esto, es de público conocimiento que los datos médicos son datos sensibles y si bien acceder a ellos permite una mejor calidad en la atención médica, hay que asegurar que dicho acceso sea efectuado por personas autorizadas para tal fin [55] [72] [73].

4.1.3. Algunas sugerencias

Se sugiere conocer las leyes nacionales e internacionales, con el fin de identificar barreras legales para la interoperabilidad de HCE compartidas a nivel transfronterizo. Se sugiere evaluar el nivel de informatización de la HCE que tiene la Institución de salud que quiera ser parte del sistema nacional transfronterizo [55] [72] [73].

Este análisis permitiría conocer el escenario donde pueda ser viable dicha implementación. A su vez identificar barreras legales posibles para el desarrollo de la comunicación transfronteriza de datos en la HCE, desde el Uruguay hacia países limítrofes. Se sugiere atender la regularización de la información de cada uno de los países que deseen ser parte del sistema, estudiando si han adoptado una legislación al respecto o no, teniendo en cuenta [55] [72] [73]:

1. Si los países proporcionan una definición legal específica de HCE o no;
2. Los diferentes enfoques legales sobre el contenido de la HCE;
3. Si la legislación nacional de cada país requiere que las HCE incluyan información más allá de los datos de salud, de ser así, se debe detallar;
4. Si la legislación nacional de cada país se refiere a terminología común o utilizan códigos de sistemas, ya sea para terminología médica como para medicamentos y afines;
5. Las fechas de vencimiento de las inmunizaciones del paciente extranjero deben estar disponibles en su HCE;
6. Marco legal específico para regular el consentimiento del paciente sobre su HCE. La falta de ello, no debería perjudicar la asistencia del paciente.

7. En el extranjero, se sugiere que cada vez que un paciente uruguayo requiera la atención de un profesional de la salud, debe dar su consentimiento para que el profesional acceda a su HCE brindando una "contraseña en presencia" que documente que el paciente está en la Institución médica extranjera y acepta dicho acceso. Si la situación es de emergencia y el paciente no está en facultades para eso, el profesional accederá al registro, pero igualmente, se grabará su actuación.

4.1.4. Cobertura de Salud Internacional

Esta sección tiene como finalidad conocer brevemente cómo es el mecanismo para obtener una cobertura médica en el exterior, basándose en Universal Assistance S.A.[1].

Este análisis será independiente de la empresa de seguro contratante, suponiendo que todas dan la misma cobertura, características de topes de coberturas, tarjetas de crédito o cualquier otra característica comercial. Solo se hará foco en lo que compete a la duración del seguro y características afines a la posibilidad de utilizar un servicio médico fuera del país. La empresa de seguro se asocia a Universal Assitance para extender el seguro hacia afuera del país, permitiendo dar cobertura en el país donde el usuario, necesite viajar.

En Uruguay, la asistencia de viaje se presta por períodos no mayores a 90 días corridos por cada viaje, quedando expresamente excluidos los períodos de residencia permanente en el extranjero.

Un seguro de viajero expedido por una empresa de seguros, está asociado a empresas como Universal Assistance S.A. la cual regirá los servicios asistenciales para los beneficiarios del seguro contratado.

En el presente estudio, no se encontró información que pueda sugerir que existe actualmente una comunicación transfronteriza entre Uruguay y otros países que establezcan compartir la HCEN. Se observó que si bien la cobertura de asistencia médica es internacional y se habilita la HCEN al personal médico de Universal Assistance, no se pudo conocer si dicha habilitación se realiza también a Instituciones de salud de los países destino.

[1] https://www.universal-assistance.com/uy-la/home.html

4.2. Juzgado, Donación y Trasplantes de Órganos

Se abordarán las siguientes áreas, desde una perspectiva legal, cómo es la situación actual y cómo se sugiere su incorporación a la Plataforma Salud.uy.

- Instituto Nacional de Donación y Trasplantes de Célula, Tejidos y Órganos (INDT).
- Solicitud de una historia clínica por parte de un Juez.

La presente sección cuenta con el apoyo de la Licenciada en Relaciones Internacionales y Doctora en Ciencias Jurídicas Sandra Dene, que muy amablemente asesoró en el análisis de los artículos de las leyes utilizadas para el desarrollo, mediante la realización de una reunión presencial con la autora de la presente tesis.

4.2.1. Marco legal

Se menciona el marco legal para cada área de abordaje.

Donación de órganos y Trasplantes de Células, Tejidos y Órganos

Interpretación de la ley Nº 14005 (1971) – 18968 [83]

La donación puede darse de dos formas:

- Entre vivos.
- Post mortem (total y sin elección, queda a disposición de quien necesite, a no ser que el fallecido así lo haya declarado en vida o directamente no haya revocado la donación de sus órganos).

El artículo 11 de la presente ley declara textual:

"Toda persona mayor de veintiún años de edad podrá consentir en la remoción, en vida, de órganos o tejidos de su cuerpo para ser trasplantados o injertados a otros seres humanos. Previamente, un médico deberá dejar constancia escrita de su advertencia al donante, firmada, también, por éste acerca de los riesgos de la operación y de la disminución física que habrá de sobrevenirle. Dicha constancia quedará archivada en el establecimiento donde se realizó la intervención.".

El artículo 13 declara textual: *"Solamente se admitirá la donación en vida o para después de la muerte de órganos o tejidos a favor de una persona determinada, cuando ésta sea pariente del disponente por consanguinidad o afinidad en línea recta o en la colateral hasta el segundo grado."*.

Estos dos artículos brindan una clara visión del marco legal para ambos casos posibles de donación.

Poder Judicial - Juez Letrado – Juez de Oficio - Justicia Penal

El abordaje será:

- Existe una investigación penal sobre un paciente de una Institución médica (excluye al personal de la Institución de salud);
- En la historia clínica hay datos que pueden incriminar penalmente al paciente, la justicia solicita el original de esa historia clínica;
- Un Juez solicita la historia clínica por una sentencia en el caso que un menor sea un donante de órganos.

El artículo 18 literal d) de la ley Nº 18.335 establece que la historia clínica será reservada y que *"el revelar su contenido, sin que fuera necesario para el tratamiento o mediare orden judicial... hará pasible de delito previsto en el artículo 302 del Código Penal"*. En base a que solamente, medie una orden judicial, la historia clínica debe ser otorgada a la Justicia [1].

El secreto profesional médico puede ser revelado por un Juez en lo penal sin el consentimiento expreso del paciente, por lo tanto una norma que autorice a la Justicia Penal a revelar el secreto profesional médico y en consecuencia, violar la intimidad del paciente en cuanto al contenido de su historia clínica, debe ser bajo los siguientes requisitos:

- Determinar la autoridad juridicial facultada por la ley a violar la intimidad (Juez en lo penal, en lo laboral, etc);
- Determinar la naturaleza del proceso en que puede emitir ese mandato (proceso penal, familiar, laboral, etc);
- Indicar las razones por las cuales la Justicia necesite revelar el secreto profesional.

Interpretando la ley Nº 18.335 la cual hace referencia a una orden judicial, no la transforma en una norma intrusiva en la esfera de la privacidad, pues no identifica en qué casos la Justicia puede pedir la historia clínica; tampoco identifica si es la Justicia penal, civil o de familia, ni tampoco enumera los requisitos que debería observar un Juez para ordenar tal requerimiento. De todas formas, tal cual está la ley hoy, es improbable interpretar que el Artículo Nº 18 (literal d) de la presente ley, faculta a la Justicia a requerir a las Instituciones de salud las historias clínicas con independencia del consentimiento del titular del secreto profesional [84].

Con este análisis se observa que se debe partir de una orden judicial para obtener una historia clínica y así ser enviada a la Justicia para su análisis. El formato en el cual hoy predomina su transporte, es copia de la misma en formato papel.

4.2.2. Análisis de situación actual

Donación y trasplante de órganos

Este apartado se basa en el intercambio de información que surgió con una pareja allegada a la autora de la presente tesis, sobre el trasplante de riñón que se sometería uno de ellos. A partir de aquí, se generó un pequeño estudio para conocer el procedimiento para trasplantes y donaciones de órganos.

La persona necesita un trasplante de riñón. Se presenta en el 4to piso del Hospital de Clínicas[1] y se le entrega una serie de formularios para completar, a su vez debe entregar una copia de su historia clínica a dicha Institución de salud. Se le solicita un resumen de la misma con un lapso no mayor a seis meses, junto a otra documentación vigente [82].

Si el paciente ingresa a lista de espera de donantes, se realiza una apertura de historia clínica pre-trasplante conteniendo: formularios, hojas check list, exámenes y estudios necesarios para la cirugía, datos del paciente y familiares, consentimiento informado, evolución médica y de enfermería [82].

De lo anteriormente expuesto se puede deducir que la historia clínica que se abre para trasplantes de órganos, se realiza en el Hospital de Clínicas. No se tiene información que pueda confirmar si dicha historia clínica se sincroniza con la historia clínica del paciente de su Institución de salud.

[1] https://www.hc.edu.uy/

Por lo expuesto en el Artículo N° 11 de la ley 14005 *"...Dicha constancia quedará archivada en el establecimiento donde se realizó la intervención."*. Se sugiere que esa constancia pueda adjuntarse directamente a la HCEN del paciente, siendo así una forma de nuclear toda su información médica, como también de fácil acceso por todos los actores intervinientes para tal caso [83].

Poder Judicial - Juez Letrado – Juez de Oficio - Justicia Penal

Con foco en dos casos diferentes tratados por ley, se analiza:

- Investigación del Juez a efectos de comprobación.
- Donación de órganos.

Investigación del Juez a efectos de comprobación: el Juez requiere de una historia clínica para actuar. La solicita a la Institución de salud por medio de una copia en formato papel para su posterior estudio. Éste, trabaja sobre ella, y su análisis y actuación, genera una constancia de ese avistamiento, el cual lo deja por escrito.

Donación de Órganos: En estos casos se requiere una sentencia judicial previa, aquí se requiere registrar la misma por el Juez.

De lo anteriormente expuesto se sugiere que pueda existir una forma de compartir de forma electrónica la HCE de un paciente entre el Poder Judicial[1] y la Institución de salud que posee la historia clínica. De esta forma se podría establecer un registro único que permita tener acceso a toda la información cuando el Juez requiera, sin necesidad de solicitar copia de la misma en formato papel. Partiendo del supuesto que la historia clínica en cuestión se encuentra en formato electrónico, el Juez puede dejar adjunto la constancia del avistamiento y/o la sentencia judicial previa en la historia clínica, manteniéndose actualizada en línea y accesible desde los diferentes puntos los cuales se requiera para su intervención.

Con foco en el Artículo Nº 19 del Decreto 274/010, que se basa en el proceso de intercambio de información clínica, cada evento clínico o asistencial de una persona, debe registrarse en un documento clínico electrónico [85].

Este Decreto implica:

[1] https://www.poderjudicial.gub.uy/

- Obligatoriedad de conexión a la plataforma HCEN
- Intercambiar información con finalidad asistencial
- Seguir lineamientos determinados por el Ministerio de Salud Pública (MSP)[1]

A su vez, el Instituto Nacional De Trasplantes (INDT)[2] entrega un formulario para dar de alta/revocación de donación. Aquí se sugiere que en la carátula del formulario sea visible la mención a la donación de órganos y este formulario se envíe de forma electrónica a la Institución de salud de la persona [85].

[1] https://www.gub.uy/ministerio-salud-publica/
[2] https://www.indt.gub.uy/

Apéndice 5

Glosario

A

ABAC: Attribute Based Access Control (Control de Acceso Basado en Atributos)

AGESIC: Agencia para el Gobierno Electrónico y la Sociedad de la Información y Conocimiento

APPC: Advanced Patient Privacy Consents (Consentimiento Avanzado de Privacidad del Paciente)

B

BID: Banco Interamericano de Desarrollo

BPPC: Basic Patient Privacy Consents (Consentimiento Básico de Privacidad del Paciente)

C

CDe: Certificado de Defunción Electrónico

CNVe: Certificado de Nacidos Vivo Electrónico

CTI: Centro de Tratamientos Intensivos

F

FACPL: Formal Access Control Policy Lenguaje (Lenguaje de política de

control de acceso formal)

FHIR: Fast Healthcare Interoperability Resources (Recursos de Interoperabilidad de Atención Médica Rápida)

H

HCE: Historia Clínica Electrónica

HCEN: Historia Clínica Electrónica Nacional

HCEO: Historia Clínica Electrónica Oncológica

HCPe: Historia Clínica Perinatal Electrónica

HIPAA: Health Insurance Portability and Accountbaility Act (Ley de Portabilidad y Responsabilidad del Seguro Médico)

HIS: Health Information System (Sistemas de Información en Salud)

I

IHE: Integrating the Healthcare Enterprise

INUS: Índice Nacional de Usuarios de Salud

M

MEF: Ministerio de Economía y Finanzas

MSP: Ministerio de Salud Pública

NCI: National Cancer Institute (Instituto Nacional de Cáncer)

O

OMS: Organización Mundial de la Salud

OPS: Organización Panamericana de la Salud

P

PAP: Policy Administration Point (Punto de Administración de Políticas)

PDP: Policy Decision Point (Punto de Decisión de Políticas)

PEP: Policy Enforcement Point (Punto de Aplicación de Políticas)

PIP: Policy Information Point (Punto de Información de Políticas)

PIPE: Pseudonymization of Information for Privacy in e-Health (Seudonimización de la Información para la Privacidad en Salud Electrónica)

PNS: Plataforma Nacional de Salud

PR: Policy Repository (Repositorio de Políticas)

PRP: Policy Recuperation Point (Punto de Recuperación de Políticas)

R

RACSEL: Red Americana de Cooperación sobre Salud Electrónica

RBAC: Role Based Access Control (Control de Acceso Basado en Roles)

RIDI: Red Integrada de Diagnóstico por Imagen

RUCAF: Registro Único de Cobertura de Asistencia Formal

S

SEVEN: Sistema de Estadística Vitales, Embarazo y Niñez

SNIS: Sistema Nacional Integrado de Salud

T

TI: Tecnología de la Información

TIC: Tecnologías de la Información y Comunicación

X

XACML: eXtensible Access Control Markup Language

XML: eXtensible Markup Language