

DESMATERIALIZACION DOCUMENTAL DE HISTORIAS CLINICAS

MANUELA GIRALDO JIMÉNEZ  
CAMILA MONTERO DELGADO  
LORENA HERNANDEZ DIAZ

UNIVERSIDAD CES  
FACULTAD DE DERECHO  
PROGRAMA PREGRADO DE DERECHO  
MEDELLÍN, COLOMBIA  
2024

## Resumen

La era digital exige la transformación de la historia clínica tradicional en formato electrónico (mensajes de datos). Este trabajo analiza las implicaciones legales de esta conversión, centrándose en la validez, efectos jurídicos y fuerza probatoria de la información médica digitalizada.

Mediante un análisis documental de normativa legal y jurisprudencia, se evalúa si la desmaterialización cumple con los requisitos para preservar la integridad y confiabilidad de la información médica. Se comparan las características de la historia clínica digital con el formato físico tradicional, y se ponderan los potenciales beneficios y riesgos de la desmaterialización.

La investigación, de tipo dogmática, positivista y hermenéutica, busca determinar si la desmaterialización documental de historias clínicas es una alternativa viable desde el punto de vista jurídico para la gestión de la información médica

**Palabras clave:** Desmaterialización documental, historias clínicas, validez, efectos jurídicos, fuerza probatoria, mensaje de datos, normativa legal, jurisprudencia.

## Abstract

The digital age requires the transformation of the traditional medical record into electronic format (data messages). This investigation analyzes the legal implications of this conversion, focusing on the validity, legal effects and evidentiary force of the digitized medical information.

A documentary analysis of legal regulations and case law assesses whether dematerialization meets the requirements to preserve the integrity and reliability of medical information. The characteristics of the digital medical history are compared with the traditional physical format, and the potential benefits and risks of dematerialization are weighed.

Dogmatic, positivist and hermeneutical research seeks to determine whether documentary dematerialization of medical records is a legally viable alternative for the management of medical information.

**Keywords:** Documentary dematerialization, medical records, validity, legal effects, evidentiary force, data message, legal regulation, jurisprudence.

## INTRODUCCIÓN

La transformación digital ha impactado significativamente en numerosos aspectos de la sociedad contemporánea, y el ámbito de la salud no ha sido ajeno a este fenómeno.

La historia clínica (HC) tradicional ha sido el pilar fundamental para la documentación del historial médico de un paciente durante décadas. Su implementación ha traído consigo que el registro sea de manera organizada y detallada, de tal manera que la atención médica, exámenes, diagnósticos, tratamientos y evolución clínica del paciente se encuentren detallados.

A pesar de su importancia y lo útil que es, la historia clínica tradicional presenta unas características que en esta era de transformación digital, se consideran limitaciones:

1. Fragmentación de la información: suele estar fragmentada en diferentes documentos físicos, dispersos en distintos centros de atención médica, lo que dificulta la accesibilidad e integración de la información completa del paciente, lo que puede afectar la calidad de la atención médica.
2. Interoperabilidad: los sistemas tradicionales de historias clínicas no se pueden compartir de manera fluida entre diferentes instituciones de salud, lo que genera barreras en la atención médica y dificulta el seguimiento del historial médico del paciente a lo largo de su vida.
3. Vulnerabilidad de datos: el almacenamiento físico los hace vulnerables a daños, pérdidas o robos. Además, la gestión manual de estos documentos aumenta el riesgo de errores y dificulta la trazabilidad de la información.
4. Inaccesibilidad para el paciente: Los pacientes tradicionalmente no tienen acceso directo a su HC lo que limita su participación en su propio cuidado y la toma de decisiones informadas sobre su salud.

En respuesta a estas limitaciones, la transformación digital ha impulsado el desarrollo de la historia clínica electrónica (HCE), la cual busca abordar las deficiencias del sistema tradicional y ofrecer una solución más eficiente, segura y accesible para la gestión de la información médica.

En este contexto, la desmaterialización documental de historias clínicas emerge como un tema crucial que plantea importantes interrogantes sobre su validez jurídica, efectos legales y fuerza probatoria.

En esta investigación, se abordará el impacto de la conversión de historias clínicas en mensajes de datos, con el objetivo de analizar detalladamente su repercusión en el ámbito legal.

Uno de los objetivos de la incorporación de las tecnologías de la información y de las comunicaciones en un sistema de salud, es mejorar la continuidad de la asistencia y

facilitar el acceso a esta información. De esta manera el paciente puede acceder desde cualquier lugar del mundo y en cualquier momento a su información, lo que con una historia clínica en medio físico no se logra, ya que, para acceder a esta, se debe contar al menos con un tiempo en desplazamiento y tiempo en el trámite para solicitarla.

Es por lo anterior, que la desmaterialización documental de historias clínicas implica un cambio positivo en los pacientes y en los administradores de salud, y de aquí la importancia en analizar si con la digitalización de estos documentos, se conserva la validez, efectos jurídicos y fuerza probatoria para que las entidades encargadas puedan realizar la transformación de este documento sin ningún tipo de barrera. Este es un proceso que plantea desafíos y oportunidades en términos de integridad, autenticidad y seguridad de la información médica.

La investigación que se propone es necesaria, entendiendo que en la normatividad vigente, no se evidencia ninguna regulación en cuanto a historia clínica digital, la forma de implementarlas y que estas a su vez gocen de validez jurídica, efectos jurídicos y fuerza probatoria, lo que tenemos son ciertas normas como la circular 02 de 1997 expedida por el Archivo General de la Nación en la que sólo enuncian que las entidades prestadoras de los servicios de salud, les está permitido utilizar medios físicos o técnicos para el registro y conservación de la historia clínica como computadoras y medios magneto ópticos o la Resolución 839 del 23 de marzo de 2017 que establece el manejo, custodia, tiempo de retención, conservación y disposición final de los expedientes de las historias clínicas, entre otras regulaciones.

Para abordar el tema en cuestión, se empleará un enfoque cualitativo analítico que permita examinar detenidamente la normativa legal y la jurisprudencia relacionada con la desmaterialización de historias clínicas. Además, se llevará a cabo una investigación exploratoria y descriptiva para comprender a fondo las implicaciones legales de este proceso. Se emplearán principalmente técnicas de análisis documental, incluyendo una revisión exhaustiva de normativas legales y jurisprudencia relevante.

Las variables de análisis incluirán la validez de la historia clínica, los efectos jurídicos de la desmaterialización y la fuerza probatoria de las historias clínicas digitales. Se comparará la confiabilidad y precisión de la información contenida en historias clínicas en formato digital versus el formato físico tradicional, teniendo en cuenta aspectos como accesibilidad, integridad y seguridad de la información.

Para comprender el marco legal y normativo que sustenta este proceso, nos basamos en la resolución 839 del 2017, que modificó la resolución 1995 de 1999 en Colombia, la cual define la historia clínica como un documento obligatorio y reservado que registra de manera cronológica la atención médica de un paciente. Exploramos las características que debe cumplir una historia clínica integral, secuencial, racional y

oportuna, destacando su disponibilidad como un aspecto crucial para la atención médica.

Además, consideramos la Circular 2 de 1997 del Archivo General de la Nación, que establece lineamientos para el registro y conservación de historias clínicas en medios físicos y técnicos, incluyendo computadoras y medios magneto ópticos.

Exploramos experiencias internacionales, como en Estados Unidos, Australia y Estonia, donde la historia clínica electrónica ha sido implementada con éxito, proporcionando eficiencia en la atención médica y facilitando el acceso a la información para pacientes y profesionales de la salud.

El trabajo se estructurará en los siguientes capítulos: Normativa legal y reglamentaria sobre digitalización de historias clínicas, experiencia internacional en la implementación, validez, efectos jurídicos y fuerza probatoria de la historia clínica en formato digital y comparativa entre formatos de historias clínicas.

## CAPÍTULO I

### NORMATIVA LEGAL Y REGLAMENTARIA SOBRE DIGITALIZACIÓN DE HISTORIAS CLÍNICAS EN COLOMBIA

La circular 2 de 1997 del Archivo General de la Nación, establece directrices para el registro y conservación de documentos en medios físicos y técnicos, incluyendo las historias clínicas, aquí se dice que es permitido la incorporación de tecnologías de punta en la administración de los archivos, pudiendo utilizar cualquier soporte documental por medio técnico, electrónico óptico, informático o telemático, pero siempre y cuando cumplan con estos requisitos

- Organización archivística previa de los documentos.
- Realizar estudios técnicos necesarios para una adecuada decisión y tener en cuenta aspectos como: conservación física, ambiental y operacional de los nuevos soportes.
- Justificar el uso e implementación de nuevas tecnologías de acuerdo con las necesidad y fines propias de cada una.
- Los documentos emitidos o reproducidos por los citados medios gozaran de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, integridad, inalterabilidad, perpetuidad y el cumplimiento de los requisitos exigidos por las leyes procesales.
- Los documentos originales que posean valores de carácter histórico, según lo registre la tabla de retención, no podrá ser destruido aún si es reproducido o almacenado por otro medio técnico, electrónico, óptico, informático o telemático.

Toda actuación administrativa que se desarrolle a partir de soportes de tecnología debe garantizar la conservación, operatividad, seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema de información.

Luego, la resolución 1995 de 1999 emitida por el Ministerio de Salud y Protección Social, define la historia clínica como un documento obligatorio y reservado que registra la información médica de un paciente de manera cronológica y sistemática. En su artículo 3, la resolución establece las características básicas que debe contener la historia clínica, que son las siguientes

1. Integralidad: la historia clínica de un usuario debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud en las fases de fomento, promoción de la salud, prevención específica, diagnóstico, tratamiento y rehabilitación de la enfermedad, abordándolo como un todo en sus aspectos biológico, psicológico y social, e interrelacionando con sus dimensiones personal, familiar y comunitaria.

2. Secuencialidad: los registros de la prestación del servicio de salud deben consignarse de manera cronológica en que ocurrió la atención.
3. Racionalidad científica: es la aplicación de criterios científicos en el diligenciamiento y registro de las acciones en salud brindadas a un usuario, de modo que evidencie en forma lógica, clara y completa, el procedimiento que se realizó en la investigación de las condiciones de salud del paciente, diagnóstico y plan de manejo.
4. Disponibilidad: es la posibilidad de utilizar la historia clínica en el momento que se necesita, con las limitaciones que impone la ley.
5. Oportunidad: es el diligenciamiento de los registros de atención de la historia clínica, simultánea o inmediatamente después de que ocurre la prestación del servicio.

Ahora bien, la misma circular en su artículo 18 habla de los medios técnicos de registro y conservación de la historia clínica, de la siguiente manera: “Los Prestadores de Servicios de Salud pueden utilizar medios físicos o técnicos como computadoras y medios magnetoópticos, cuando así lo consideren conveniente, atendiendo lo establecido en la circular 2 de 1997 expedida por el Archivo General de la Nación, o las normas que la modifiquen o adicionen”.

En conclusión, la normativa legal y reglamentaria sobre la digitalización de historias clínicas en Colombia ofrece directrices claras para la incorporación de tecnología en la administración de archivos médicos. La Circular 2 de 1997 del Archivo General de la Nación permite el uso de tecnologías avanzadas para el registro y conservación de documentos, siempre y cuando se cumplan ciertos requisitos, como la organización previa de los archivos, la realización de estudios técnicos y la garantía de autenticidad e integridad de los documentos digitales.

La Resolución 1995 de 1999 del Ministerio de Salud y Protección Social establece la historia clínica como un documento obligatorio y reservado, detallando las características básicas que debe contener, como integralidad, secuencialidad, racionalidad científica, disponibilidad y oportunidad.

En conjunto, estas normativas permiten a los prestadores de servicios de salud utilizar medios técnicos, como computadoras y medios magneto-ópticos, para el registro y conservación de historias clínicas, siempre y cuando se cumplan los lineamientos establecidos. Esto promueve una gestión más eficiente de la información médica, garantizando su integridad y disponibilidad para una atención de calidad al paciente.

Tenemos igualmente la ley 527 de 1999, la cual tiene varios artículos que debemos analizar con detenimiento, por lo que a continuación expondremos un cuadro anunciando el artículo y algunos aspectos para tener en cuenta:

| ARTÍCULO   | CONTENIDO  | ANÁLISIS  |
|--|--|---|
| ARTÍCULO 5.<br>RECONOCIMIENTO JURIDICO DE LOS MENSAJES DE DATOS. | No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.   | En este caso, queda claro que un mensaje de datos tiene plena validez, efectos jurídicos y fuerza obligatoria, siempre y cuando cumpla con los demás requisitos.  |
| ARTÍCULO ORIGINAL.<br>8o.  | <p>Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si:</p> <p>a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;</p> <p>b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar.</p> | En este caso, si la historia clínica pasa a ser un mensaje de datos, esta deberá conservar su integridad a partir del momento en que se generó por primera vez, es así que el prestador del servicio de salud, deberá garantizar a través de sistemas informáticos que la información expresada en mensaje de datos tenga una cadena de manipulación muy estricta, en caso de hacerse modificaciones, deberá guardar el registro de quien lo hizo y cual fue, además de tratar la información con todos los cuidados necesarios, así como se hace con una historia clínica en medios físicos. |
| ARTÍCULO 9o.<br>INTEGRIDAD DE UN MENSAJE DE DATOS.               | Se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y   | Es relacionado con el artículo anterior, y no hay dudas en que la historia clínica deberá permanecer completa y sin alteraciones, salvo algún cambio que se deba hacer por un proceso de comunicación.  |



|   |  |   |  |
|---|--|---|--|
|   |  | de todas las circunstancias relevantes del caso.  |  |
| ARTÍCULO 10.<br>ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS. |  |   | Estos artículos serán analizados en los capítulos posteriores.   |
| ARTICULO 11.<br>CRITERIO PARA VALORAR PROBATORIAMENTE UN MENSAJE DE DATOS.  |  |   |  |
| ARTÍCULO 12.<br>CONSERVACION DE LOS MENSAJES DE DATOS Y DOCUMENTOS.         |  | <p>Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:</p> <ol style="list-style-type: none"> <li>1. Que la información que contengan sea accesible para su posterior consulta.</li> <li>2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y</li> <li>3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.</li> </ol> | Este artículo es clave para los prestadores del servicio de salud, que deben conservar las historias clínicas según la resolución 839 de 2017, por un periodo mínimo de quince (15), contados a partir de la fecha de la última atención, deberán tener en cuenta la información de este artículo para cumplir con una correcta conservación del mensaje de datos. |

Ahora bien, en el 2020, se emitió la ley 2015 de 2020, que crea la Historia Clínica Electrónica Interoperable y se dictan otras disposiciones, igualmente que, en la anterior normativa, se hará un cuadro con la información de la ley y un pequeño análisis.

| ARTÍCULO   | CONTENIDO   | ANÁLISIS  |
|--|---|---|
| ARTÍCULO 10. Autenticidad.                                   | La Historia Clínica Electrónica se presumirá auténtica de acuerdo con la normatividad vigente.  | En este caso, la historia clínica electrónica será igual de auténtica que una historia clínica que este en formato físico.  |
| ARTÍCULO 13. Seguridad e la información y seguridad digital. | Deberán contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo mediante la adopción de los lineamientos para la administración de la seguridad de la información y la seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones o quien haga sus veces. Lo anterior, incluyendo lo señalado por la Ley 1581 de 2012 de Hábeas Data y Ley 527 de 1999 de Comercio Electrónico, o las normas que las modifiquen, sustituyan o complementen. | Es clave que los prestadores del servicio de salud tengan normas y procedimientos, entre otros, para garantizar una efectiva seguridad en la información y digital. |

La ley 527 de 1999 y la ley 2015 de 2020 proporcionan disposiciones adicionales que refuerzan la autenticidad, seguridad y conservación de la información en formato electrónico, incluyendo la Historia Clínica Electrónica, lo que implica la necesidad de implementar normas y procedimientos para garantizar la seguridad de la información y la adecuada gestión del riesgo digital por parte de los prestadores del servicio de salud.

## CAPITULO II

### EXPERIENCIA INTERNACIONAL EN LA IMPLEMENTACIÓN

En la era digital actual, la tecnología ha transformado radicalmente la forma en que se gestionan los registros médicos y se brinda atención sanitaria en todo el mundo. Uno de los avances más significativos en este ámbito es la implementación de historias clínicas electrónicas, que permiten la recopilación, almacenamiento y acceso seguro a la información de los pacientes de manera electrónica. En este contexto, el presente capítulo se enfoca en analizar la implementación de historias clínicas electrónicas en Estonia, el cual es conocida por ser líder en la digitalización de servicios gubernamentales y de salud, también mencionamos algunos aspectos de Estados Unidos y Australia.

#### 1. Estonia

La implementación de la digitalización de historias clínicas en este país se remonta a principios de la década de 2000, cuando implementaron un sistema de registro médico electrónico conocido como "e-Health", el cual es un sistema integral de salud electrónica que abarca una variedad de servicios y tecnologías para mejorar la atención médica, la gestión de datos de salud y la comunicación entre proveedores de atención médica y pacientes. Fue creado para ofrecer una atención médica más eficiente, segura y centrada en el paciente.

Para la implementación de este sistema Estonia invirtió en el desarrollo de una infraestructura de tecnología de la información robusta y segura, que proporciona la base necesaria para los servicios de salud electrónica. Esto incluye redes de comunicaciones confiables, sistemas de almacenamiento de datos seguros y protocolos de seguridad avanzados. A su vez, se establecieron estándares y protocolos para garantizar la interoperabilidad y la seguridad de los datos en todo el sistema e-Health, esto permitió que los diferentes componentes del sistema se comunicaran entre sí de manera efectiva y que los datos de salud se transmitieran de forma segura.

En la adopción de este nuevo sistema se fomentó la participación de los ciudadanos, permitiéndoles acceder a sus propios registros de salud a través de un portal de pacientes en línea. Esto les permite ver su historial médico, resultados de pruebas, medicamentos recetados y más, lo que promueve la participación y la toma de decisiones informadas en su atención médica.

##### 1.1. Normatividad en la implementación del sistema

Ahora bien, explicaremos cómo fue el proceso normativo de la implementación de este sistema en Estonia, para esto se debe tener en cuenta que la digitalización de

las historias clínicas fue posible gracias a una serie de normativas y políticas que establecieron un marco legal y regulatorio para la implementación de sistemas de salud electrónica. A continuación, se describen algunas de las leyes y regulaciones clave que permitieron la digitalización de las historias clínicas en Estonia:

1. Ley de Salud Electrónica: En 2005, Estonia promulgó una Ley de Salud Electrónica, la cual estableció los principios generales, requisitos y marcos legales para la implementación de sistemas de salud electrónica en el país. Esta ley tiene como objetivo principal promover la implementación de tecnologías de la información y la comunicación en el sector de la salud para mejorar la calidad, eficiencia y accesibilidad de los servicios de salud en Estonia, también busca facilitar el intercambio seguro de datos de salud entre los proveedores de atención médica y mejorar la coordinación de la atención médica.

Esta ley establece requisitos específicos para los sistemas de salud electrónica, incluyendo estándares técnicos, medidas de seguridad y privacidad, y procedimientos para el intercambio de datos de salud. Estos requisitos garantizan que los sistemas de salud electrónica cumplan con los estándares de calidad y seguridad necesarios para proteger la información de salud de los ciudadanos.

A su vez, también establece disposiciones específicas para proteger la privacidad y seguridad de los datos de salud de los ciudadanos estonios. Esto incluye medidas para garantizar el consentimiento informado de los pacientes para el uso y divulgación de su información de salud, así como medidas de seguridad para proteger los datos contra el acceso no autorizado.

A continuación, se describen algunas de las principales medidas de protección de datos personales contempladas en esta ley:

1.1. Consentimiento informado: La ley establece que el tratamiento de datos de salud requiere el consentimiento informado del paciente. Esto significa que los pacientes deben ser informados de manera clara y comprensible sobre cómo se recopilarán, almacenarán, procesarán y utilizarán sus datos de salud, y deben dar su consentimiento explícito para ello.

1.2. Confidencialidad: La ley establece que los proveedores de atención médica y otros profesionales de la salud tienen la obligación de mantener la confidencialidad de la información de salud de los pacientes. Esto incluye medidas para proteger la información de salud contra el acceso no autorizado, la divulgación y el uso indebido.

1.3. Acceso y control de los datos: La ley otorga a los pacientes el derecho de acceder a sus propios datos de salud y de controlar quién puede acceder a ellos. Esto incluye el derecho a solicitar una copia de sus registros médicos, el derecho a corregir información inexacta o incompleta, y el derecho a limitar o revocar el acceso a sus datos por parte de terceros.

1.4. Seguridad de la información: La ley establece requisitos específicos de seguridad para proteger la información de salud contra la pérdida, el robo, la manipulación y el acceso no autorizado. Esto incluye medidas técnicas y organizativas, como el cifrado de datos, la autenticación de usuarios, el control de acceso y la supervisión de la seguridad.

1.5. Notificación de violaciones de datos: La ley requiere que los proveedores de servicios de salud notifiquen a las autoridades de protección de datos y a los pacientes sobre cualquier violación de seguridad que pueda afectar la privacidad de sus datos de salud. Esto permite tomar medidas rápidas para mitigar el impacto de la violación y proteger los derechos de los pacientes.

En conclusión, la Ley de Salud Electrónica de Estonia establece una serie de medidas de protección de datos personales para garantizar la privacidad y seguridad de la información de salud de los ciudadanos. Estas medidas son fundamentales para promover la confianza en los sistemas de salud electrónica y proteger los derechos de los pacientes en el uso y tratamiento de sus datos de salud.

2. Ley de Protección de Datos Personales: Estonia cuenta con leyes sólidas de protección de datos personales que garantizan la privacidad y seguridad de la información de salud de los ciudadanos. Esta ley se basa en la Directiva de Protección de Datos Personales de la Unión Europea y en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Estas leyes establecen los derechos y obligaciones relacionados con la recopilación, almacenamiento y procesamiento de datos de salud. Algunos aspectos a tener en cuenta de esta ley son los siguientes:

2.1 Los Principios de protección de datos: La Ley de Protección de Datos Personales establece una serie de principios que deben seguirse al procesar datos personales, incluidos los datos de salud. Estos principios incluyen la legalidad, equidad y transparencia en el tratamiento de datos, la limitación de la finalidad, la minimización de datos, la exactitud, la integridad y la confidencialidad de los datos, así como la responsabilidad del controlador de datos.

2.2 Consentimiento del paciente: La ley requiere que el procesamiento de datos de salud, incluida la información contenida en la historia clínica electrónica, esté sujeto al consentimiento informado del paciente. Esto significa que los pacientes deben ser informados de manera clara y comprensible sobre cómo se utilizarán sus datos de salud y deben dar su consentimiento para ello. El consentimiento debe ser libremente otorgado, específico, informado e inequívoco.

2.3 Seguridad de los datos: La ley establece la obligación de implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos de salud. Esto incluye medidas como el cifrado de datos, la autenticación de usuarios, el

control de acceso, la supervisión de la seguridad y la notificación de violaciones de datos.

2.4 Derechos de los pacientes: La ley otorga a los pacientes una serie de derechos en relación con sus datos de salud, incluidos los datos contenidos en la historia clínica electrónica. Estos derechos incluyen el derecho de acceso a sus propios datos, el derecho a corregir información inexacta o incompleta, el derecho a solicitar la eliminación de datos en ciertas circunstancias, y el derecho a limitar o revocar el consentimiento para el procesamiento de datos.

2.5 Transferencia internacional de datos: La ley regula la transferencia de datos personales fuera del Espacio Económico Europeo (EEE) y establece requisitos específicos para garantizar la protección adecuada de los datos de salud en tales transferencias.

En resumen, la Ley de Protección de Datos Personales de Estonia proporciona un marco legal sólido para la protección de los datos de salud, incluidos los datos contenidos en la historia clínica electrónica. Esta ley garantiza que el procesamiento de datos de salud se realice de manera legal, equitativa, transparente y segura, y protege los derechos de los pacientes en relación con sus datos de salud.

3. Normativas de Seguridad de la Información: Se establecieron normativas específicas para garantizar la seguridad de la información de salud en los sistemas electrónicos. Estas normativas abordan aspectos como el acceso autorizado, la autenticación de usuarios, la encriptación de datos y la protección contra intrusiones cibernéticas.

4. Estándares de Interoperabilidad: Estonia adoptó estándares de interoperabilidad para garantizar que los diferentes sistemas de información de salud puedan comunicarse entre sí de manera efectiva. Esto facilitó el intercambio de datos entre proveedores de atención médica y sistemas de información de salud. Los aspectos a tener en cuenta de estos estándares son los siguientes:

4.1 Formatos de datos estandarizados: Estonia ha adoptado formatos de datos estandarizados para la representación de la información de salud en los sistemas de historia clínica electrónica. Estos formatos aseguran que los datos de salud sean comprensibles y accesibles para diferentes sistemas y aplicaciones de software.

4.2 Protocolos de comunicación: Se han establecido protocolos de comunicación estandarizados para facilitar el intercambio de datos de salud entre diferentes sistemas de información de salud.

Estos protocolos aseguran que los sistemas de historia clínica electrónica puedan comunicarse entre sí de manera efectiva y segura.

4.3 Identificadores únicos de pacientes: Estonia utiliza identificadores únicos de pacientes para garantizar la integridad y la identificación precisa de los datos de salud de los pacientes en los sistemas de historia clínica electrónica. Estos identificadores permiten vincular de manera única la información de salud de un paciente a lo largo del tiempo y en diferentes entornos de atención médica.

4.4 Estándares de seguridad: Se han establecido estándares de seguridad para proteger la confidencialidad, integridad y disponibilidad de los datos de salud en los sistemas de historia clínica electrónica. Estos estándares incluyen medidas de cifrado de datos, autenticación de usuarios, control de acceso y auditoría de seguridad.

4.5 Estándares de terminología médica: Estonia utiliza estándares de terminología médica estandarizados para garantizar la consistencia y la interoperabilidad de los términos utilizados para describir la información de salud en los sistemas de historia clínica electrónica. Esto facilita la comprensión y el intercambio de datos de salud entre diferentes sistemas y proveedores de atención médica.

Para concluir, los estándares de interoperabilidad de Estonia en la historia clínica electrónica están diseñados para facilitar el intercambio seguro y eficaz de datos de salud entre diferentes sistemas y proveedores de atención médica. Estos estándares aseguran que la información de salud sea comprensible, accesible y utilizable en diferentes entornos de atención médica, lo que contribuye a una atención médica más integrada y centrada en el paciente

5. Participación Ciudadana: Se promovió la participación de los ciudadanos en el proceso de digitalización de las historias clínicas. Los pacientes tienen derecho a acceder a sus propios registros de salud y a controlar quién puede acceder a su información de salud. Para la implementación del sistema “e – Health” en Estonia se tuvo en cuenta lo siguiente:

5.1 Acceso a los registros médicos electrónicos: Los ciudadanos estonios tienen derecho a acceder a sus propios registros médicos electrónicos a través de un portal en línea. Esto les permite ver su historial médico, resultados de pruebas, diagnósticos, tratamientos y otros datos relevantes sobre su salud.

5.2 Feedback y sugerencias: Los ciudadanos tienen aún la oportunidad de proporcionar retroalimentación y sugerencias sobre el diseño, funcionamiento y mejora continua del sistema de salud electrónica. Esto puede incluir comentarios sobre la usabilidad del portal de acceso a los registros médicos electrónicos, la calidad de la información proporcionada y cualquier otra área de interés para los usuarios.

5.3 Participación en grupos de interés y comités asesores: Se establecieron grupos de interés y comités asesores que incluyen representantes de la comunidad,

pacientes y otros grupos relevantes para proporcionar aportes y perspectivas sobre cuestiones relacionadas con la digitalización de las historias clínicas y el desarrollo de servicios de salud electrónica.

5.4 Educación y capacitación: Se llevaron a cabo actividades de educación y capacitación para informar a los ciudadanos sobre el sistema de salud electrónica, cómo acceder a sus registros médicos electrónicos y cómo utilizar la tecnología de la información para gestionar su salud. Esto incluye sesiones informativas, materiales educativos y recursos en línea.

Esto se puede concluir en que la participación de los ciudadanos en el proceso de digitalización de las historias clínicas en Estonia ha sido fundamental para garantizar que el sistema de salud electrónica sea centrado en el paciente, transparente, seguro y efectivo. La participación de los ciudadanos ha contribuido a mejorar la accesibilidad, calidad y usabilidad de los servicios de salud electrónica en el país.

6. Desarrollo de Infraestructura de TI: Estonia invirtió en el desarrollo de una infraestructura de tecnología de la información sólida y segura que proporciona la base necesaria para la implementación y operación exitosa del sistema de salud electrónica del país. A continuación, se describen algunos aspectos del desarrollo de la infraestructura de TI en este proceso:

6.1 Redes de comunicaciones confiables: Estonia ha invertido en el desarrollo y la expansión de redes de comunicaciones confiables y de alta velocidad que permiten la transmisión segura y eficiente de datos de salud entre diferentes sistemas y ubicaciones. Esto incluye redes de fibra óptica, redes de comunicaciones móviles y redes de área local (LAN) en entornos de atención médica.

6.2 Sistemas de almacenamiento de datos seguros: Se han implementado sistemas de almacenamiento de datos seguros y escalables para almacenar los registros médicos electrónicos y otros datos de salud de manera segura. Esto incluye centros de datos con medidas de seguridad física, protección contra incendios y sistemas de respaldo redundantes para garantizar la disponibilidad y la integridad de los datos.

6.3 Plataformas de software robustas: En su momento se desarrollaron y desplegaron plataformas de software robustas y escalables para la gestión de registros médicos electrónicos, intercambio de datos de salud, autenticación de usuarios, control de acceso y otras funciones relacionadas con la salud electrónica. Estas plataformas están diseñadas para ser seguras, interoperables y fáciles de usar.

6.4 Protocolos de seguridad avanzados: Se han implementado protocolos de seguridad avanzados para proteger la confidencialidad, integridad y disponibilidad de los datos de salud en la infraestructura de TI. Esto incluye medidas de cifrado de



datos, autenticación de usuarios, control de acceso basado en roles, monitoreo de seguridad y detección de intrusiones.

6.5 Integración con sistemas existentes: La infraestructura de TI para la digitalización de las historias clínicas se ha integrado con sistemas existentes en el sector de la salud, como sistemas de información hospitalaria, sistemas de gestión de laboratorios, sistemas de imágenes médicas y sistemas de facturación. Esto asegura una interoperabilidad efectiva y una transición suave al nuevo sistema de salud electrónica.

Para concluir este capítulo, el sistema e-Health en Estonia es un ejemplo de cómo la tecnología puede transformar la atención médica y mejorar la experiencia del paciente. Fue creado a través de una colaboración entre el gobierno, proveedores de atención médica y otros actores relevantes, con un enfoque en la infraestructura de Tecnologías de la Información sólida, estándares de interoperabilidad y participación ciudadana. Esto ha llevado al éxito del sistema e-Health en Estonia y ha establecido al país como un líder en salud electrónica a nivel mundial, esto también fue posible gracias a un marco legal y regulatorio claro, que estableció los principios, requisitos y estándares para la implementación de sistemas de salud electrónica.

## **2. Estados Unidos**

En el año 1996 el congreso de los Estados Unidos dictó la norma HIPAA<sup>1</sup> (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT), en la cual inician un camino para estandarizar las transacciones electrónicas del cuidado médico, como una vía para simplificar la administración del sector salud en su conjunto.

Actualmente, hay 3 sistemas que operan en estados unidos:

- PHR “personal health record”: se trata de un expediente médico personal, y es un sistema para almacenar el expediente, en el cual el paciente puede acceder a su historial clínico y añadir información, así en las visitas al médico, se pueden ver los resultados de los exámenes en solo unos minutos ya que se puede acceder de forma rápida al sistema.
- EMR “electronic medical record”: es un registro medico electrónico, que se utiliza en reemplazo de los ficheros en papel, así el medico introduce la información a una computadora y estos se guardan en el sistema informático del médico.

---

<sup>1</sup> La Ley de Responsabilidad y Transferibilidad de Seguros Médicos de 1996, y demás normas relacionadas en el título 45 del C.F.R. (Código de Normas Federales), partes 160 y 164, conocidas en su conjunto como HIPAA, establecen los criterios a seguir para la privacidad y seguridad de la información médica personal. Asimismo, establecen los criterios que regulan la protección de la información médica transmitida por vía electrónica.

- EHR “electronic health record”: es una historia clínica electrónica que se puede compartir con otros proveedores, por lo tanto, se pueden enviar tanto a especialistas del mismo proveedor como a otros.

En conclusión, estados unidos a pesar de que no tiene un sistema estandarizado y común para todos los estados, se manejan diferentes sistemas que ayudan con la coordinación de la atención, proporcionando a los prestadores del servicio de salud, información precisa y actualizada.

### **3. Australia**

La implementación de la HCE comenzó en la década de 1990, cuando Australia creó el Sistema Nacional de Historia Clínica Digital (llamado HealthConnect), el cual inicialmente duraría 10 años. Fue un concepto para estandarizar el formato de la información clínica en los puntos de atención médica, información que luego serviría para que profesionales de la salud y pacientes pudieran acceder a su HC de forma digital.

Luego en el 2004 se le incorporó otro sistema llamado inicialmente MediConnect que serviría para realizar las prescripciones de medicamentos de forma electrónica.

Según un informe realizado por Boston Consulting Group (BCG) llegó a la conclusión de que el principal problema que tuvo Australia en implementar el programa de eHealth fue la cantidad de iniciativas sin coordinación, que se presentaban a lo largo de los diferentes gobiernos territoriales. A causa de la falta de coordinación, interoperabilidad y escalabilidad, se necesitaba un órgano de aplicación nacional con colaboración de todos los estados territoriales. Por este motivo, entre otros, en Julio 2005 se creó una agencia nacional (National E-Health Transition Authority Ltd – NEHTA) con el objetivo de desarrollar e implementar las bases necesarias para ofrecer mejoras en la salud a través de Tecnologías de la Información y la Comunicación (TICs). Esta agencia incluyó representantes de los gobiernos nacionales, estatales y representantes de departamentos médicos de todo Australia.

Con esta nueva autoridad de aplicación, el programa de HealthConnect fue reexaminado con el objetivo de incluir todas las partes interesadas dado el escaso avance que tuvo anteriormente. NEHTA tiene como objetivos desarrollar la mejor forma de intercambiar los datos clínicos electrónicamente, establecer los estándares para la HCE a nivel nacional y asegurar la coordinación entre los distintos intervinientes de la salud. A partir de este nuevo enfoque del gobierno nacional, HealthConnect pasó a ser un proyecto colaborativo entre los diferentes actores involucrados con el objetivo de utilizar los sistemas e infraestructura existente y cumplir resultados de corto plazo. Además, se buscó estandarizar la información/arquitectura para buscar la interoperabilidad de la historia clínica electrónica, y una vez definidos los estándares se desarrolló un “mercado” donde

instituciones privadas/públicas o personas independientes tengan reglas claras para desarrollar el software y competir por mayor calidad de servicio, funcionalidad y precio

Con respecto a la privacidad y seguridad de los datos, Australia optó por un modelo de adhesión voluntario y sin discriminación. El registro es para todos los ciudadanos australianos y los residentes en Australia, pero de forma voluntaria tanto para los prestadores como para los pacientes. Por otro parte, la incorporación y el uso de la información está basada en el consentimiento personal y el estricto control sobre quien accede a dicha información. La información clínica se guardará en el sistema de cada prestador médico pero el resumen con los eventos fundamentales que se utilizará para la historia clínica digital será enviado a un repositorio nacional que conservará los datos para luego hacer las vistas y reportes estandarizados.

En 2015 el gobierno anunció el cambio de nombre del programa a My Health Record. Luego en mayo 2017 opto cambiar la forma de registrarse de los usuarios donde se pasó de un modelo voluntario para entrar, es decir que los usuarios deberían registrarse si querían entrar, a un modelo voluntario para salir, es decir que se los agrega al sistema de forma automática y el usuario decide si quiere salir del mismo.

Hasta el 2018, My Health Record contaba con 22,69 millones de personas y aproximadamente 13,2 millones de datos grabados. Por otro lado, 6,5 millones de personas contaban con la cartilla de vacunación actualizada. Por el lado de los proveedores de la salud, 70% de las farmacias y 73% de los profesionales generalistas estaban usando My Health Record. Se puede ver un gran incremento en la cantidad de usuarios del sistema dado el modelo elegido para que los ciudadanos tengan acceso al sistema de forma masiva y no se haga de forma voluntaria.

## **CAPÍTULO III**

### **VALIDEZ, EFECTOS JURÍDICOS Y FUERZA PROBATORIA DE LA HISTORIA CLÍNICA ELECTRÓNICA**

En Colombia, la adopción de la historia clínica electrónica (HCE) ha generado importantes interrogantes legales y jurídicos sobre su validez, efectos jurídicos y fuerza probatoria. Este texto examinará de cerca estos aspectos, explorando la normativa colombiana aplicable, analizando los criterios de validez de la HCE y evaluando su peso en procesos legales y litigios médicos. Al comprender la complejidad y el impacto de la HCE en el contexto colombiano, podemos avanzar hacia un mejor entendimiento de su papel en la atención médica y la administración de justicia.

#### **1. Validez de la Historia clínica electrónica**

Para este punto, nos vamos a referenciar por la ley 2015 del 2020, la cual crea la historia clínica electrónica interoperable y se dictan otras disposiciones, siendo así, es importante analizar la definición de HCE.

Historia clínica electrónica: es el registro integral y cronológico de las condiciones de salud del paciente, que se encuentra contenido en sistemas de información y aplicaciones de software con capacidad de comunicarse, intercambiar datos y brindar herramientas para la utilización de la información refrendada con firma digital del profesional tratante. Su almacenamiento, actualización y uso se efectúa en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad y acceso, de conformidad con la normatividad vigente.

De esta decisión podemos desprender varios aspectos:

- Al realizar el registro de los datos del paciente, es indispensable que se realice de forma completa y secuencial frente la atención brindada
- Se debe contar con un sistema de información y aplicación de software que tengan la capacidad de comunicarse, intercambiar datos y brindar herramientas para identificar correctamente el personal tratante, así evitar cualquier tipo de suplantación
- El almacenamiento, actualización y uso debe estar respaldado por condiciones óptimas de seguridad, integridad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad y acceso.

- Cualquier modificación que se le realice a la HCE deberá quedar registrada, aun en el caso de subsanar un error, para ello deberá tener fecha, hora, nombre e identificación de quien hizo la corrección.

El artículo 10 de la ley 2015 del 2020, le da la presunción de autenticidad a la HCE, de acuerdo con la normatividad vigente, por lo que en este caso nos remitimos a la resolución 1995 de 1999 del Ministerio de Salud y protección social, la cual establece las características, los requisitos y estándares para la custodia, manejo y conservación de la historia clínica en Colombia, que son los siguientes:

## 1. Características

-Integralidad: La historia clínica de un usuario debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud en las fases de fomento, promoción de la salud, prevención específica, diagnóstico, tratamiento y rehabilitación de la enfermedad, abordándolo como un todo en sus aspectos biológico, psicológico y social, e interrelacionado con sus dimensiones personal, familiar y comunitaria.

-Secuencialidad: Los registros de la prestación de los servicios en salud deben consignarse en la secuencia cronológica en que ocurrió la atención. Desde el punto de vista archivístico la historia clínica es un expediente que de manera cronológica debe acumular documentos relativos a la prestación de servicios de salud brindados al usuario.

-Racionalidad científica: Para los efectos de la presente resolución, es la aplicación de criterios científicos en el diligenciamiento y registro de las acciones en salud brindadas a un usuario, de modo que evidencie en forma lógica, clara y completa, el procedimiento que se realizó en la investigación de las condiciones de salud del paciente, diagnóstico y plan de manejo.

-Disponibilidad: Es la posibilidad de utilizar la historia clínica en el momento en que se necesita, con las limitaciones que impone la Ley.

-Oportunidad: Es el diligenciamiento de los registros de atención de la historia clínica, simultánea o inmediatamente después de que ocurre la prestación del servicio.

## 2. Componentes

-Identificación del usuario: datos personales de identificación del usuario, apellidos y nombres completos, estado civil, documento de identidad, fecha de nacimiento, edad, sexo, ocupación, dirección y teléfono del domicilio y lugar de residencia, nombre y teléfono del acompañante; nombre, teléfono y parentesco de la persona responsable del usuario, según el caso; aseguradora y tipo de vinculación.

-Registros específicos: debe ser de acuerdo con la naturaleza del servicio que presta y los contenidos mínimos deberán ser los contemplados en la resolución 2546 de 1998 y los generalmente aceptados en la práctica de las disciplinas del área de la salud.

-Anexos: Son todos aquellos documentos que sirven como sustento legal, técnico, científico y/o administrativo de las acciones realizadas al usuario en los procesos de atención, tales como: autorizaciones para intervenciones quirúrgicas (consentimiento informado), procedimientos, autorización para necropsia, declaración de retiro voluntario y demás documentos que las instituciones prestadoras consideren pertinentes.

En conclusión, la validez de la HCE es fundamental en el ámbito de la atención médica, especialmente porque se encuentra respaldada por la ley 2015 de 2020, que establece estándares claros para su creación, mantenimiento y uso interoperable. La definición detallada de la HCE nos lleva a considerar aspectos cruciales como la integridad y secuencialidad de los registros, la necesidad de sistemas de información seguros y la preservación de la autenticidad de los datos. Además, la legislación colombiana, en concordancia con resoluciones específicas, define los requisitos y componentes esenciales que garantizan la calidad y utilidad de la HCE, desde la identificación del usuario hasta la inclusión de los anexos relevantes. En este contexto, el cumplimiento riguroso de estas normativas fortalece la confiabilidad y eficacia de la historia clínica electrónica como una herramienta vital para la atención médica, asegurando la disponibilidad oportuna y el uso adecuado de la información en beneficio del paciente y del sistema de salud.

## **2. Efectos jurídicos de la Historia clínica electrónica**

La implementación de la historia clínica electrónica (HCE) en Colombia ha generado importantes debates en cuanto a sus efectos jurídicos, especialmente en términos de privacidad, confidencialidad, responsabilidad legal y validez probatoria.

En Colombia, la HCE está regulada principalmente por la Ley 2015 de 2020, que establece los lineamientos para su uso, almacenamiento y protección. Uno de los principales efectos jurídicos de la HCE es su impacto en la privacidad y confidencialidad de la información médica. La Ley 2015 garantiza el derecho a la intimidad y la protección de datos personales de los pacientes, y establece medidas de seguridad para prevenir el acceso no autorizado a la HCE. Sin embargo, existen preocupaciones sobre la vulnerabilidad de los datos ante posibles ataques cibernéticos o fallos en la seguridad informática.

Es por esto que garantizar la privacidad y confidencialidad en una HCE y asegurar el derecho a la intimidad y protección de datos personales implica la implementación de medidas integrales de seguridad y del cumplimiento de la ley, tales medidas podrían incluir los siguientes puntos:

1. Acceso restringido: limitar el acceso a la HCE solo para personal autorizado tales como médicos, enfermeras y personal administrativo con roles específicos. En este punto sería esencial contar con sistemas de autenticación, contraseñas seguras y controles de acceso.
2. Cifrado de datos: utilizar técnicas de cifrado para proteger los datos almacenados en la HCE, ya que garantizaría incluso si alguien obtiene acceso no autorizado a los datos, no podrá leerlos ni utilizar la información sin la clave de cifrado adecuada.
3. Auditoria de accesos: implementar un sistema de registro en el cual estén todas las actividades relacionadas con la HCE, incluidos los accesos, modificaciones y eliminaciones de datos, lo que ayudaría a identificar y rastrear cualquier actividad sospechosa o no autorizada.
4. Protección contra amenazas cibernéticas: implementar medidas de seguridad informática para proteger la infraestructura de la HCE contra amenazas como virus, malware, ataques de phishing y ataques de denegación de servicio, esto puede incluir firewalls, software antivirus, actualizaciones regulares de seguridad y capacitación del personal en prácticas seguras de navegación en línea.
5. Cumplimiento normativo: asegurarse de que la HCE cumpla con las regulaciones de privacidad y protección de datos. También implementar la aplicación de políticas y procedimientos que cumplan con los estándares legales y éticos en cuanto a la recopilación, almacenamiento, uso y divulgación de datos médicos personales.

Otro aspecto importante es la responsabilidad legal de los profesionales de la salud en relación con la HCE. Si bien la ley establece que los médicos son responsables de la veracidad y actualización de la información en la HCE, también plantea interrogantes sobre la responsabilidad en caso de errores o negligencia en su manejo. Por ejemplo, ¿quiénes son responsables en caso de pérdida o manipulación indebida de la información en la HCE?

En resumen, la historia clínica electrónica en Colombia tiene importantes implicaciones jurídicas que requieren una atención cuidadosa por parte de todas las partes involucradas.

Es fundamental garantizar la protección de la privacidad de los pacientes, establecer mecanismos efectivos de seguridad informática y definir claramente las responsabilidades legales de los profesionales de la salud.

### **3. Fuerza probatoria de la historia clínica en mensajes de datos**

Primero, es muy importante resaltar el papel que cumple la historia clínica en diferentes procesos, ya sea para obtener una pensión por invalidez o en los procesos de responsabilidad médica, entre otros, ya que es un documento fundamental y determinante para demostrar las pretensiones; la historia clínica es considerada como un medio probatorio esencial que proporciona en el caso de la pensión por invalidez, la existencia y la gravedad de la condición médica que justifica la invalidez y ayuda a evaluar la documentación médica para determinar si la condición médica del solicitante cumple con los requisitos establecidos para recibir la pensión por invalidez o en el caso de responsabilidad médica, sirve como evidencia para determinar si hubo una mala praxis médica o negligencia por parte del personal de salud, y a demostrar si se siguieron los estándares de atención médica adecuados, si se tomaron las medidas necesarias o si se proporcionaron los tratamientos adecuados.

Su utilización, en este caso, el de una historia clínica electrónica, se regularía por la ley 527 de 1999, la cual nos indica lo siguiente:

Ley 527 de 1999

Artículo 10. Admisibilidad y fuerza probatoria de los mensajes de datos. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o debido a no haber sido presentado en su forma original.

Artículo 11. Criterio para valorar probatoriamente un mensaje de datos. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

De lo anterior se infiere que:

- La historia clínica electrónica pasa a ser un medio de prueba documental, el cual está contenido en mensajes de datos y es un medio útil para la formación del convencimiento del juez.



- La validez como medio de prueba está amparada en las mismas disposiciones que expresamente dice cuáles son los medios de prueba, esto es el artículo 165 del código general del proceso y adicionalmente el artículo 10 y 11 de la ley 527 de 1999, la cual nos indica que no se negará valor probatorio a la información que este en forma de mensajes de datos por el solo hecho de estar así.
- Se tendrán en cuenta como en los demás medios de prueba:
  1. La confiabilidad de la forma que se generó, archivo o comunico el mensaje
  2. La confiabilidad en la forma de conservación de la información
  3. La forma en la que se identifique a su iniciador
  4. Cualquier otro factor que sea relevante.

En el contexto de la historia clínica, los mensajes de datos podrían incluir los registros electrónicos de consultas médicas, resultados de pruebas, diagnósticos, tratamientos, entre otros. La fuerza probatoria de estos mensajes dependerá de la evaluación de los criterios mencionados, así como de la normativa específica relacionada con la gestión de la información médica y la protección de datos de salud. Es importante que las instituciones médicas implementen medidas de seguridad y control de acceso adecuadas para garantizar la integridad y autenticidad de la información contenida en los mensajes de datos relacionados con la historia clínica de los pacientes.

## CAPITULO IV

### HISTORIA CLÍNICA TRADICIONAL VS. HISTORIA CLÍNICA ELECTRÓNICA

La historia clínica ha sido un elemento fundamental para la atención médica durante siglos. En ella se plasma el registro detallado del historial médico del paciente, incluyendo su diagnóstico, tratamiento, evolución y otra información relevante para su cuidado. Tradicionalmente, la historia clínica ha existido en formato físico, plasmada en papel y almacenada en expedientes. Sin embargo, como se ha mencionado en los capítulos anteriores, en las últimas décadas, la historia clínica electrónica (HCE) ha ganado terreno como una alternativa digital que ofrece diversas ventajas.

En este capítulo, se realizará una comparación profunda entre la historia clínica tradicional y la HCE, analizando sus características, ventajas y desventajas, con el objetivo de brindar una comprensión completa de las diferencias y similitudes entre ambos formatos.

| <b>Característica</b> | <b>Historia clínica digital</b>  | <b>Historia clínica tradicional</b>  |
|-----------------------|--|--|
| <b>Acceso</b>         | Su acceso es inmediato desde cualquier lugar con conexión a internet   | La historia clínica tradicional se elabora en papel, utilizando formularios preimpresos o registros manuscritos. Esto implica un mayor riesgo de pérdida o deterioro de la información, así como una dificultad para compartirla entre diferentes profesionales de la salud. |
| <b>Almacenamiento</b> | Base de datos segura en servidores   | Expedientes físicos en gabinetes o estanterías   |
| <b>Costos</b>         | Inversión inicial en software, hardware y capacitación, pero ahorro a largo plazo en almacenamiento, impresión y gestión de documentos | Menor costo inicial, pero mayores costos a largo plazo en almacenamiento, impresión y gestión de documentos.   |

|                                    |  |  |
|------------------------------------|--|--|
| <b>Dependencia a la tecnología</b> | Dependencia de sistemas informáticos que pueden presentar fallas o vulnerabilidades, necesidad de implementar medidas de seguridad adecuadas para proteger la información. | No requiere dependencia de sistemas informáticos, lo que la hace menos vulnerable a ataques cibernéticos.  |
| <b>Durabilidad</b>                 | Permanece inalterable en el tiempo para que su información pueda ser consultada.   | Sufre deterioro con el paso del tiempo, por su propio uso.   |
| <b>Desventajas</b>                 | Mayor riesgo de errores humanos en la transcripción, manejo de datos y registro de información.  | Imposibilidad de rastrear las acciones realizadas en la historia clínica.  |
| <b>Interoperabilidad</b>           | Facilita el intercambio de información entre diferentes instituciones de salud   | Dificulta el intercambio de información entre diferentes instituciones de salud.   |
| <b>Impacto ambiental</b>           | Se disminuye el consumo de papel y se promueven practicas sostenibles, contribuyendo a la protección del medio ambiente.   | Uso excesivo de papel lo que conlleva a un gasto innecesario con el cual se afecta gravemente el medio ambiente.   |
| <b>Legibilidad</b>                 | Presenta la información en formato digital legible y fácil de comprender, también permite la búsqueda rápida y eficiente de información mediante criterios específicos.    | Pueden llegar a ser poco legibles por la caligrafía del profesional de la salud que realiza las anotaciones, impactando esto directamente en la calidad de la atención médica y la seguridad del paciente, esto con lleva a que haya errores en los diagnósticos y tratamientos de los pacientes, que se dificulte la investigación en caso de presentarse un proceso legal.<br><br>Adicional a esto, su organización es manual, está basada en la |

|   |  |  |
|---|--|--|
|   |  | estructura de los formularios preimpresos o en la organización del personal a cargo.   |
| <b>Seguridad</b>                        | <p>Mayor control sobre el acceso a la información, menor riesgo de accesos no autorizados, trazabilidad de las acciones realizadas en la historia clínica, cumplimiento de regulaciones de privacidad de datos.</p> <p>A su vez, presenta dependencia de sistemas informáticos que pueden presentar fallas o vulnerabilidades, necesidad de implementar medidas de seguridad adecuadas para proteger la información.</p> | <p>No requiere dependencia de sistemas informáticos, lo que la hace menos vulnerable a ataques cibernéticos.</p> <p>A su vez, puede presentar dificultad para controlar el acceso físico a los expedientes, mayor riesgo de pérdida o robo de información, imposibilidad de rastrear las acciones realizadas en la historia clínica.</p> |
| <b>Secuencialidad de la información</b> | Garantizada por mecanismos de campos autonuméricos e inserción de hora y fecha automática.   | Es difícil, sino está previamente foliada, las evoluciones son consecutivas sobre un mismo papel.  |

Hemos logrado abarcar las diferencias entre la historia clínica física y la digital, destacando las ventajas significativas que ofrece la digitalización en términos de seguridad, eficiencia, accesibilidad, organización y costos, con ello llevándonos a concluir que la desmaterialización de las historias clínicas se presenta como un paso necesario para modernizar el sistema de salud y mejorar la calidad de la atención médica.

La historia clínica digital no solo representa un cambio tecnológico, sino también un cambio de paradigma en la forma en que se brinda y se recibe la atención médica. Es una oportunidad para repensar el sistema de salud y construir uno más eficiente, equitativo y centrado en las necesidades de los pacientes con ello damos un paso decisivo hacia un futuro más saludable para todos.

## CONCLUSIÓN

La desmaterialización documental de las historias clínicas es un proceso fundamental para la modernización y mejora del sistema de salud. Este trabajo ha explorado en profundidad los aspectos legales como la validez, efectos jurídicos y fuerza probatoria y prácticos de la transición hacia la historia clínica electrónica (HCE) en Colombia, destacando su importancia y los desafíos que conlleva.

El análisis normativo revela que Colombia cuenta con un marco legal sólido que respalda la implementación de la HCE. La ley 527 de 1999 y la Ley 2015 de 2020, entre otras regulaciones, establecen los requisitos y estándares para garantizar la validez, efectos jurídicos y fuerza probatoria de la HCE, al tiempo que se enfatiza la importancia de la seguridad, integridad y confidencialidad de los datos médicos.

La revisión de experiencias internacionales, como en Estonia, Estados Unidos y Australia, demuestra que la adopción exitosa de la HCE requiere una coordinación efectiva, el establecimiento de estándares de interoperabilidad, la participación ciudadana y el desarrollo de una infraestructura de tecnología de la información sólida y segura.

En cuanto a la validez, efectos jurídicos y fuerza probatoria de la HCE, se analizaron los criterios legales y jurisprudenciales aplicables. Se determinó que la HCE goza de la misma validez y fuerza probatoria que la historia clínica física, siempre y cuando se cumplan los requisitos establecidos en la normativa, como la integridad, autenticidad, inalterabilidad y trazabilidad de los datos.

Finalmente, se realizó una comparativa exhaustiva entre la historia clínica tradicional y la HCE, destacando las ventajas significativas que ofrece la digitalización en términos de accesibilidad, seguridad, eficiencia, organización y costos a largo plazo, así como su contribución a la sostenibilidad ambiental.

En conclusión, la desmaterialización documental de historias clínicas es un paso necesario para modernizar el sistema de salud colombiano y mejorar la calidad de la atención médica. Si bien implica desafíos técnicos, legales y de implementación, los beneficios potenciales son enormes, incluyendo una mejor gestión de la información, una atención más centrada en el paciente y una mayor eficiencia en todo el sistema de salud. Con la adopción adecuada de las tecnologías digitales y el cumplimiento de las regulaciones pertinentes, Colombia puede posicionarse a la vanguardia de la transformación digital en el sector de la salud.

## REFERENCIAS

Ley de protección de datos personales en Estonia-Isikuandmete kaitse seadus (lühend - IKS). Tomado de: <https://www.riigiteataja.ee/akt/104012019011>

Ley de organización de los servicios de atención sanitaria en Estonia-Tervishoiuteenuste korraldamise seadus (lühend - TTKS).  
Tomado de: <https://www.riigiteataja.ee/akt/115122023012>

Ley del seguro médico en Estonia-Ravikindlustuse seadus (lühend - RaKS).  
Tomado de: <https://www.riigiteataja.ee/akt/113032019136>

Historia de e-Estonia y bloques de construcción del estado electrónico.  
Tomado de: <https://e-estonia.com/solutions/>

Texas. Health and human services. La HIPAA y las leyes sobre la privacidad.  
Tomado de: <https://www.hhs.texas.gov/es/reglamentos/informacion-legal/la-hipaa-las-leyes-sobre-la-privacidad#:~:text=La%20ley%20sobre%20la%20privacidad,de%20procesamiento%20de%20informaci%C3%B3n%20m%C3%A9dica>

National Library of Medicine. Personal health record (PHR).  
Tomado de: <https://www.ncbi.nlm.nih.gov/books/NBK557757/>

HealthITBuzz The latest on health IT from onc. Diferencia entre EMR y EHR.  
Tomado de: <https://www.ncbi.nlm.nih.gov/books/NBK557757/>

Torres, Andrés. (2018). Estudio e implementación de la historia clínica electrónica a nivel nacional en Argentina, 34-45.  
Tomado de: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.utdt.edu/bitstream/handle/20.500.13098/11481/MBA\\_Torres\\_2020.pdf?sequence=1&isAllowed=y](https://repositorio.utdt.edu/bitstream/handle/20.500.13098/11481/MBA_Torres_2020.pdf?sequence=1&isAllowed=y)

ABECÉ. Interoperabilidad de datos de la historia clínica en Colombia.  
Tomado de: <https://www.minsalud.gov.co/ihc/Documentos%20compartidos/ABC-IHC.pdf>

Historia clínica electrónica vs historia clínica en papel.  
Tomado de: <https://medicalcloud.com.co/2015/09/30/historia-clinica-electronica-vs-papel/>