PROTECCIÓN DE DATOS UNA VISIÓN COMPARADA DESDE LA LEGISLACIÓN ESPAÑOLA Y COLOMBIANA

DATA PROTECTION A COMPARATIVE VISION FROM THE SPANISH AND COLOMBIAN LEGISLATION.

HAROL STIVEN GARZON FORERO

Hsgarzon@poligran.edu.co

MARELVIS DEL SOCORRO ARIAS MORENO

Mdariasm@poligran.edu.co

BLANCA NIDIA CASTRO HERRERA

Blcastro1@poligran.edu.co

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE SOCIEDAD CULTURA Y CREATIVIDAD

PROGRAMA DE DERECHO

BOGOTÁ D.C, NOVIEMBRE DE 2020

Agradecimientos

En primer lugar, nos permitimos agradecer a nuestra tutora, Doctora MONICA LUCIA FERNANDEZ MUÑOZ - DTC Investigador asociado de nuestra Institución Universitaria Politécnico Grancolombiano, quien con sus conocimientos nos guio permanentemente a través de cada una de las etapas de este proyecto para alcanzar los resultados que nos propusimos lograr.

Para nosotros es muy grato pertenecer a esta gran Institución Universitaria, que cuenta con un talento humano comprometido tanto sus directivas como sus docentes poseen una experticia para capacitar y liderar a sus alumnos, donde no solo quedan recuerdos académicos, sino de unión y fraternidad, siempre la llevaremos en nuestros corazones.

Agradecemos a nuestros compañeros con quienes realizamos la Misión Internacional para poder elaborar este trabajo de grado, a nuestras familias, por apoyarnos día a día, aun cuando los ánimos decaían. En especial, queremos mencionar a nuestros padres, que siempre estuvieron ahí para darnos palabras de apoyo y un abrazo reconfortante para renovar energías. No hubiésemos podido alcanzar estos resultados de no haber sido por sus apoyos incondicionales.

Muchas gracias a todos.

Resumen.

La historia clínica electrónica es la herramienta digital unificada y personal cuyo objetivo es el intercambio de la información sensible e importante de los pacientes, la cual integra todos los datos documentales que se utilizan en la práctica clínica, su motivación es dar celeridad a una oportuna prestación del servicio de salud. Igualmente, y por contener datos constitucionalmente sensibles de cada persona, y al haber un intercambio de la información el Estado debe asegurar que el método de transferencia cumpla con los estándares de interoperabilidad y protección de datos de acuerdo con la legislación gubernamental vigente. El presente artículo de investigación tiene como finalidad realizar un recorrido cronológico respecto a los avances en la protección de datos bajo una versión comparada entre España y Colombia, esto con el propósito de analizar de fondo la implementación de la historia clínica electrónica, los avances y ventajas que ello conlleva.

Abstract.

The electronic medical record is the unified and personal digital tool whose objective is the exchange of sensitive and important information of medical patients, which integrates all the documentary data that is used in clinical practice, its motivation is to speed up a timely provision of health service. Likewise, and because it contains constitutionally sensitive data of each person, and since there is an exchange of information, the state must ensure that the transfer method complies with the interoperability and data protection standards in accordance with current government legislation. The purpose of this research article is to carry out a chronological study regarding the advances in data protection under a comparative version between Spain and Colombia, this with the purpose of thoroughly analyzing the implementation of electronic medical records and the advances and advantages that this entails.

Palabras Clave: Protección de datos, historia clínica electrónica, intimidad, confidencialidad, paciente y salud.

Keywords: Data protection, electronic medical record, privacy, confidentiality, patient and health.

Introducción.

El presente artículo de investigación tiene como objetivo indicar al lector el tratamiento de datos personales que le da la legislación española a la historia clínica electrónica y se comparará frente a la implementación de la misma en Colombia, esto en consideración a que el Estado Colombiano mediante la ley 2015 del 31 de Enero de 2020, ordenó al Ministerio de Salud y Protección Social así como al Ministerio de Tecnologías de la Información y Comunicaciones la implementación del software que permita la interoperabilidad de la historia clínica electrónica en las entidades prestadoras de salud, lo cual se debe realizar en un término no mayor a cinco (5) años a partir de la promulgación de dicha ley.

Para cumplir con el objetivo principal realizaremos un análisis comparado basado en la legislación actual, para lo cual debemos antecedernos a la historia del nacimiento de la protección de datos, para tal fin analizaremos los avances que ha tenido el término protección de datos tanto en la legislación Colombiana como en la legislación Española, una vez analizada dicha situación examinaremos los mecanismos implementados por cada nación para ejecutar en forma correcta la historia clínica electrónica con la correspondiente protección de los datos sensibles de cada individuo.

Como es información de dominio público la protección de datos personales es un derecho de carácter constitucional, tales como los derechos a la intimidad y confidencialidad, teniendo en cuenta que en el presente artículo hablamos de protección de datos contenidos en la historia clínica electrónica los cuales son sensibles y deben tener una mayor custodia frente a su confidencialidad y no divulgación.

Con el desarrollo del presente trabajo se pretende dar respuesta a la pregunta ¿Cuál es la protección legal que brinda el Estado frente al uso y disposición de datos personales en la implementación de la historia clínica electrónica en Colombia?

I. Protección de datos una visión comparada entre Colombia y España.

IA. Antecedentes históricos y normativos de la protección de datos en España.

El 11 de enero de 1541 el emperador Carlos I de España, nombra por primera vez el derecho a la inviolabilidad de las cartas algo muy revolucionario para la época, pero poco se avanza en el derecho a la protección de datos en España, hasta que en 1869 se reforma la Constitución de 1812, en el sentido de establecer derechos para nacionales y extranjeros que habiten el territorio español, en cuanto a la protección al domicilio, el secreto a la correspondencia y los efectos personales, Igualmente el 17 de julio de 1945 el fuero de españoles crea los derechos fundamentales a la dignidad humana y libertad humana.

Con la reforma de la constitución española de 1978 si bien es cierto que no habla taxativamente de protección de datos, en su articulado estableció ‘’*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*’’(Padres de la Constitución, 1978), por lo que en cumplimiento a ello el legislador posteriormente crea la ley orgánica de protección civil 1/1982 del 5 de mayo, la cual crea el derecho al honor a la intimidad personal y familiar y a la propia imagen. Mediante la ley orgánica 16/1985 se nombra el derecho a la privacidad personal, mediante la ley orgánica 13/ 1986 establece las limitaciones de las autoridades respecto a la investigación científica y técnica en base a los datos de las personas. La ley Orgánica 12/ 1989 regula la función de estadística pública frente a la disposición de los datos personales, como se ha podido evidenciar durante el transcurso del tiempo, el avance normativo fue muy poco pero sustancioso, el gran avance se da con la creación de la Ley Orgánica 5/1992, del 29 de octubre, donde nace a la vida jurídica la Ley LORTAD o *ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal la cual estableció “*la implementación de mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información. A tal efecto se estructura en una parte general y otra especial’’ (Gobierno Español, 1992) lo que constituyó un momento revolucionario en la historia legislativa española, pues garantizaba la protección de los datos de carácter personal.

La ley LORTAD cumplió con los derechos que se debían proteger en el momento, pues garantizaba la protección de los datos personales almacenados en soportes

automatizados, pero tenía una falencia pues dejó a un lado la protección de datos de carácter personal tratados en papel. Con la finalidad de subsanar esta falencia el gobierno español mediante la creación de la ley Orgánica 15/1999 del 13 de diciembre, crea la Ley orgánica de Protección de Datos de Carácter Personal o ‘’LOPD’’ la cual regula las obligaciones que tienen las personas que intervienen en cualquier procedimiento del tratamiento de datos personales, igualmente con esta ley se garantiza la seguridad de los datos suministrados y regula los procedimientos sancionadores cuando haya una violación a los derechos personales entregados por los usuarios, por ello creó el delegado de protección de datos el cual es obligatorio para todas las compañías privadas o públicas.

El delegado de protección de datos se creó y tomó mayor importancia en el reglamento (UE), así como en la ley orgánica actual, puesto que indica que el mismo es de carácter obligatorio o voluntario dependiendo de la información que se recolecta, cabe resaltar que este cargo lo puede ejercer una persona jurídica o natural que haga o no parte de la compañía, en todo caso La Agencia Española de Protección de Datos deberá mantener una relación estrecha con cada compañía. Para que una compañía pueda recolectar datos deberá tener certificación emitida por la entidad que así lo permita.

Actualmente en España la interoperabilidad de datos se debe ajustar a lo establecido en los artículos 33 y 34 de la Ley Orgánica 15/1999, es decir la ley protección de datos personales y lo normado en el Título VI del Real Decreto 1720/2007, por la cual se desarrolló la Ley orgánica de protección de datos personales. La legislación actual ha tenido en cuenta las responsabilidades que se generan frente a la transferencia de datos con países que aún no tienen un gran avance normativo frente a la protección de datos, por lo que toda transferencia de datos internacionales debe ser autorizada por el director de la Agencia Española de Protección de Datos.

Teniendo en cuenta el uso y disposición de las nuevas tecnologías, lo que genera un reto frente al control de datos personales en internet, el gobierno español creó la ley orgánica 3/2018 o Ley Orgánica de Protección de Datos Personales y Garantía de Derechos

Digitales, en la cual se establecieron las garantía de protección de datos a personas fallecidas, así como la obligación de transparencia en las negociaciones contractuales frente al uso de los datos en internet, y lo más importante la protección de datos en redes sociales, lo que limitó el abuso de algunas páginas de redes sociales frente al uso y disposición de los datos de los usuarios. Con la finalidad de dar cumplimiento a lo establecido en esta ley, España dio la aplicación al reglamento General de protección de Datos ‘’RGPD’’, creado por el Parlamento Europeo, es así como, a partir del 25 de mayo de 2018, se asignan mayores funciones para los delegados de tratamiento de datos y se adicionan reformas al procedimiento sancionatorio por mal uso o disposición de los datos personales de los usuarios.

La historia clínica es el medio utilizado para garantizar una adecuada prestación del servicio de salud, por tanto, los profesionales de la salud son quienes realizan el diagnóstico y el tratamiento del paciente, y deben contar con acceso a la historia clínica electrónica.

Es así como en cumplimiento a la Ley General de Sanidad del 25 de abril de1986, el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, de manera que quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para su exposición. Igualmente, la ley establece que ‘’*Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Asimismo, se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso. Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, del 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la*

salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos. 4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones. 5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria. 6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto. 7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso". (Jefatura de estado, 2002).

IB. Antecedentes históricos y normativos de la protección de datos en Colombia.

Con la declaración Universal de los derechos humanos en 1948, se salvaguardó el derecho a la intimidad para cada individuo, puesto que indico a cada estado el deber de garantizar la protección de la vida privada, familia, domicilio o correspondencia. En aras de continuar con el desarrollo normativo, el Pacto Internacional de Derechos Civiles y Políticos, adoptado por la asamblea general de las naciones unidas el 16 de diciembre de 1966, En este sentido Colombia ratificó la convención el 28 de mayo de 1973.

Aunque en algunas ocasiones se había hablado del tema, solo hasta la Constitución Política del 1991, en su artículo 15, se definió El derecho a la intimidad y al tratamiento de los datos facultando al congreso de la República a legislar sobre las políticas de manejo, por lo que estableció:

> **"ARTÍCULO 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que

se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas''(Constitucion Politica, 1991).

Así mismo la honorable corte constitucional en Sentencia T-158 A de 2008 reiteró que '' El carácter reservado de la historia clínica se fundamenta en la necesidad de proteger el derecho a la intimidad del individuo sobre una información, que en principio, únicamente le concierne a él y que, por tanto, debe ser excluida del ámbito de conocimiento público''(Corte Constitucional, 2008)

Por lo que en desarrollo del precepto constitucional el congreso nacional de Colombia creó las dos leyes macro en protección de datos, las cuales constituyen el marco general de la protección de los datos personales:

Se creó la ley 1266 de 2008 y los Decretos reglamentarios1727 del 17 septiembre de 2009 y el Decreto 2952 del 18 de octubre de 2010 "Habeas Data", *'por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones* (Congreso de la Republica, 2008).

En el 2012 Colombia se unió al grupo de países que cuenta con una regulación general e integral sobre la protección de datos personales y el tratamiento de estos con el desarrollo de los derechos constitucionales a la intimidad y sus diversas manifestaciones y de acuerdo a la ley 1581 de 2012, reglamentada en el decreto 1377 del 27 de junio de 2013, que regula los datos y archivos, cuya esencia es: " desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política de Colombia; así como el derecho a la información consagrado en el artículo 20 de la misma''(Congreso de la Republica, 2012). Regulando en aspectos concernientes con la autorización del titular de la información para el tratamiento de sus datos personales, de acuerdo con las políticas de tratamiento y con autorización de los encargados del ejercicio de los derechos de los titulares de la información.

El derecho de habeas data también ha tenido un desarrollo en materia jurisprudencial como lo podemos identificar en la Sentencia T-414 de 1992, garantizando el derecho a la intimidad, pues en dicha sentencia estableció ‘’ Se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad. Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada’’(Corte Constitucional, 1992). En Sentencia SU-082 de 1995 se inició la reflexión sobre el derecho de habeas data como derecho autónomo, como el derecho a conocer la información, a actualizarla y a rectificarla en las bases de datos o archivos cuando no corresponda a la verdad.

Por otra parte, en Sentencia T-729 de 2002 define el habeas data como ‘’*El ámbito de acción o de operatividad del derecho al habeas data o derecho a la autodeterminación informática, está dado por el entorno en el cual se desarrollan los procesos de administración de bases de datos personales. De tal forma que integran el contexto material: el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos’’*(Corte Constitucional, 2002), el cual debe ir de la mano con el derecho al buen nombre y a la intimidad. En Sentencia C-1011 de 2008, se reitera la autonomía del derecho al habeas data, con el fin de evitar abusos en el trámite de la información y que las personas en pleno derecho de sus facultades puedan conocer la información recopilada en las bases de datos acerca de sus datos personales.

Como se ha podido observar los avances normativos en Colombia han sido bajos frente a la protección de datos, pues las obligaciones legales actuales para las personas naturales

y jurídicas que tratan y disponen de nuestros datos son menores a las protecciones que brinda el Estado Español a sus habitantes, aunado a ello es de resaltar la implementación del delegado de protección de datos en España.

Ahora bien, teniendo en cuenta la emergencia sanitaria actual causada por el Sarscov 2 (Covid 19), el cual ha afectado económica y salubremente al mundo entero, analizaremos desde un punto de vista normativo y sustancial, el avance en la implementación de la historia clínica electrónica en Colombia, frente a la implementación que ya le dio España a la misma.

II. Normativa e Implementación de la historia clínica electrónica en Colombia y España.

IIA. Normatividad vigente de historia clínica electrónica en España y Colombia.

En España la Historia es el documento donde queda plasmado la relación que se da entre el paciente y el profesional de la salud, quedando registrado sus características, valoraciones y hallazgos médicos que sirven de información histórica para otros profesionales y en posibles litigios, esto según la sentencia 529/2010, de 23 de julio, de la Audiencia Provincial de Pontevedra, Sección 6º de ahí que la historia clínica ha tenido gran relevancia en las diferentes ordenes jurisprudenciales basados en la prueba, la indemnización y el tiempo en diversos casos donde se protegen derechos e intereses jurídicamente protegidos del médico, del paciente, de la institución sanitaria tanto como pública como privada. Es así como en la jurisdicción civil se han desarrollado reclamaciones de índole de responsabilidad sanitaria en relación con la medicina privada, como lo fue en la sentencia del 31 de julio de 2012 de la Audiencia Provincial de Baleares Sección 4ª S 31-7-2012, No. 375/2012, Rec. 413/2011, en la jurisdicción contenciosa-administrativa, cuando se relacionan con el sistema nacional de la salud, en los casos donde se encuentre inmerso el profesional de la salud en un delito o falla se le aplicará la responsabilidad penal independiente del sector en que se genere (público. - privado). En España desde el año 2006 se inició con el proyecto de la historia clínica digital, siendo

pionera en Europa incluyendo de igual manera la firma electrónica y el certificado digital según la Ley 59/2003, del 19 de diciembre, en su artículo 8 que: “los datos firmados electrónicamente serán admisible como prueba documental en juicio. La firma electrónica debe brindar al ciudadano, Administraciones, un nivel de seguridad tal que sus datos no sean vulnerados, puesto que cuenta con criptografía de clave asimétrica aplicada a la firma electrónica de documentos”(Corte General de España, 2003).

Esto garantiza que únicamente el paciente pueda acceder a la información, evitando suplantaciones. Con la finalidad de obtener más seguridad cada vez que alguien consulta la misma el sistema refleja un rastro de su paso de acuerdo con lo consultado, así se sabe quién consultó cada documento, todo esto con la finalidad de precaver la prevalencia del derecho a la intimidad del documento.

La confidencialidad es un aspecto clave en la relación entre profesionales de la medicina y pacientes. Ya que según lo indica la sentencia "Los médicos valoran mucho la confidencialidad, pero incurren en conductas en las que, de modo inconsciente, ponen en peligro la intimidad del paciente"(Tribunal Supremo - Sala penal , 2001), Pues los pacientes tienen derecho a la reserva absoluta de sus datos médicos, teniendo en cuenta que son de carácter sensible por contener información privada.

Bajo ese entendido la historia clínica es el documento donde la relación con el paciente queda reflejada, razón por la cual está sujeta a la normativa general sobre protección de datos personales y a la regulación específica de la legislación sanitaria. Es por ello que cuando el profesional médico la elabora deberá conocer, mas no divulgar los aspectos básicos y la preexistencia de enfermedades del paciente.

La Constitución Española en concordancia con la Declaración Universal de los Derechos Humanos reitera la protección de datos pues establece ‘’1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad

personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos''(Padres de la Constitución, 1978).

En 1997, España suscribió el Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina, el cual reiteró a las personas el derecho al respeto de su vida privada en asuntos de salud.

Las normas que actualmente protegen los datos de los pacientes son la Ley 14/1986 General de Sanidad y la ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, la cual tuvo un gran avece normativo con la creación de la Ley 41/2002 de Autonomía del Paciente y en Navarra la Ley Foral 17/2010 de Derechos y Deberes de las Personas en Materia de Salud.

En la actualidad los códigos deontológicos de las organizaciones colegiales de medicina y enfermería recogen la obligación de guardar el secreto profesional, que es un deber moral de fidelidad que se debe guardar a los pacientes.

En España al igual que en Colombia, los pacientes tienen el derecho a que se le deje la constancia, de todos los procedimientos realizados a él, por los profesionales que operan en el sector sanitario en clínicas, hospitales, centros médicos, al momento de cualquier consulta o intervención con su salud, de manera escrita, en documento técnico, garantizando su derecho fundamental a la protección de datos personales de acuerdo a la Constitución Española en su artículo 18.4 y reglado en el Reglamento Europeo de protección de Datos (RGPD) y la ley orgánica de protección de datos (LOPDGDD), complementándose con la **Ley de Autonomía del Paciente 41/2002,** de 14 de noviembre, la cual se encarga de regular los derechos y las obligaciones en materia de información y documentación clínica del paciente.

Debemos mencionar que la historia clínica se compone de un conjunto de datos e información sobre la situación de salud física o mental y de la evolución clínica de un paciente a lo largo del tiempo, considerándose por el anterior RGPD, datos "*especialmente protegidos*" (Parlamento Europeo y Consejo de la Unión Europea, 2016).

Teniendo que cumplir por las entidades sanitarias la normatividad en la protección de los datos orientados a la dignidad de la persona humana y el respeto a la autonomía de su voluntad y de su intimidad; iniciando por el consentimiento del paciente regulado en el artículo 9 del RGPD, el cual deberá ser explícito y por escrito, con datos veraces y pertinentes, garantizando la calidad de los datos recolectados de manera leal y licita, respetando el carácter confidencial de los datos referentes a la salud con el fin de garantizar la asistencia adecuada al paciente. De igual manera se deberá informar al paciente de la existencia de la información, su trámite y manejo, el responsable del mantenimiento y protección de los datos contenidos en la historia clínica. Para los profesionales que tienen acceso a los datos del paciente, prevalece aun cuando haya terminado su tratamiento médico con el paciente debe guardar el secreto de confidencialidad.

Con el RGPD, se establece que los centros sanitarios, deben aplicar medidas para la protección de los datos de los pacientes por medio de diseños de medidas organizativas y de seguridad a la información, conservar la historia clínica en condiciones que garanticen su correcto mantenimiento y seguridad, como mínimo durante cinco años. De igual manera permitir al paciente acceder a su historia clínica y a los datos que figuren en ella.

En el año 2005, el gobierno español aprobó el *Plan Avanza*, y el programa sanidad en línea, teniendo en cuenta la interoperabilidad en todo el país, principalmente para intercambiar información administrativa y clínica, incluyendo entre otros temas la historia clínica electrónica contratada con la firma red.es.

En la actualidad se ha avanzado con la cita previa por Internet en todo el país, la receta electrónica, con interoperabilidad no en todas las comunidades autónomas, en cuanto a la Historia Clínica Electrónica (HCE), se encuentra en aplicación en todas las comunidades autónomas, mas no todos los sistemas de las comunidades son interoperables entre los distintos centros sanitarios, todas han interconectado de alguna medida sus sistemas con la historia clínica electrónica central del sistema Nacional de Salud y para su consulta se hará mediante un d**ocumento de seguridad, que deberá** estar siempre a disposición de

la Agencia Española de Protección de Datos para su consulta. Lo anterior con el fin de lograr la interoperabilidad de la información, permitiendo que la historia clínica pueda ser consultada en cualquier parte de las comunidades autónomas de manera sistematizada.

En la actualidad, en los centros de salud y hospitales, en todas las comunidades autónomas en España se encuentra implementada la historia clínica electrónica mediante software especializados permitiendo interoperabilidad clínica que contribuye a mejorar y optimizar en la atención de los pacientes, encontramos a la compañía Dedalus la cual es uno de los proveedores del software que se manejan en la actualidad en España.

Por lo que todos los programas informáticos que utilicen y diseñen para el manejo de las Historias Clínicas electrónicas, así como los soportes documentales y equipos de cómputo, deben estar provistos de mecanismos de seguridad, de tal forma que no puedan realizar modificaciones ni reproducciones a la misma, una vez se realice el registro y se guarden los datos. En todo caso debe protegerse la reserva de la historia clínica mediante mecanismos que impidan el acceso de personal no autorizado para conocerla y adoptar las medidas tendientes a evitar la destrucción de los registros en forma accidental o provocada.

IIB. Avances en la implementación de la historia clínica electrónica en Colombia.

Por el contrario, en Colombia la Resolución 1995 de 1999, en relación con los medios técnicos de registro y conservación de la historia clínica indica ‘’ Los profesionales, técnicos y auxiliares que intervienen directamente en la atención a un usuario, tienen la obligación de registrar sus observaciones, conceptos, decisiones y resultados de las acciones en salud desarrolladas, conforme a las características señaladas en la presente resolución’’(Ministerio de Salud, 1999), Así mismo la historia clínica deberá tener las siguientes características: Secuencialidad, Integralidad, Racionalidad científica, Disponibilidad y Oportunidad, aunado a ello establece que para el registro de la historia clínica los prestadores de servicios de salud pueden utilizar medios físicos o técnicos

como computadoras y medios magneto-ópticos, esto en cumplimiento a la circular 2 de 1997 expedida por el archivo general.

Teniendo en cuenta el avance tecnológico obligatorio, en Colombia se creó la ley 2015 del 31 de enero de 2020, por medio de la cual se reglamentó el uso de la historia clínica electrónica y cuya finalidad es agilizar y garantizar la debida prestación del servicio de salud, teniendo en cuenta que se obliga a las entidades prestadoras del servicio de salud, a hacer parte de la interoperabilidad de la historia clínica pues esto permite que la información esté disponible a través de un sistema de cómputo el cual permite al personal médico una oportuna información acerca de los antecedentes de salud de los paciente.

Una vez se implemente en un cien por ciento la interoperabilidad de la historia clínica servirá para que los médicos puedan consultar los antecedentes de salud de los pacientes desde cualquier lugar del país sin importar el sitio de atención del paciente, lo que permitiría que los profesionales de la salud tengan datos claros, reales y confiables de todas las enfermedades base con el fin de lograr mejores diagnósticos y una atención más segura.

Para dejar más claro el concepto de interoperabilidad al lector, indicamos que es el mecanismo de operación y colaboración que se usa entre varias entidades prestadoras del servicio de salud, con la única finalidad de intercambiar datos que permitan brindar un servicio de salud oportuno a los usuarios.

Actualmente se han realizado en Colombia varios pilotos en la implementación del Software que permitirá la interoperabilidad de la historia clínica electrónica. Estos pilotos han tenido resultados exitosos pues el Ministerio de Salud y Protección Social en asociación con el Ministerio de Tecnologías de la Información y Comunicaciones, se han encargado de proteger los datos de los usuarios, esto con el objetivo de dar cumplimiento a las normas, reglas internacionales, y lineamientos internos regulados por las TIC, en aras de crear un software capaz de cumplir con lo establecido en la ley.

Es así que para que la interoperabilidad de la historia clínica pueda realizarse en una forma legalmente segura para todos los pacientes, se debe cumplir con los siguientes estándares internacionales, así:

- ‘’Estándares de formato y estructura de mensajes y documentos
- Estándares de contenido de mensajes y documentos (incluyendo sistemas de codificación, terminología, y vocabulario)
- Estándares de seguridad del intercambio y el mensaje
- Estándares de transmisión
- Estándares de servicios de interoperabilidad, como identificadores únicos del usuario, prestador, aseguradora, y otros; servicios de localizador de información de usuarios de salud, de directorios de prestadores, de intercambio en forma “push” (empujar) y “pull” (halar), y acceso (“query”)’’ (RCN Radio.com, 2020).

Por otra parte, es importante relacionar la Resolución 839 de 2017, donde podemos evidenciar que el Ministerio de Salud y Protección Social. establece el manejo, custodia, tiempo, retención, conservación y disposición final de los expedientes de las historias clínicas y el manejo que le deben dar las entidades de salud en caso de liquidación.

El tiempo de retención y conservación de las historias clínicas es de quince (15) años, los cuales se cuentan a partir de la fecha de la última atención, por lo tanto, los primeros cinco (5) años se tendrán bajo custodia en el archivo de gestión de la entidad prestadora del servicio y los diez (10) años restantes en el archivo central.

En la eventualidad que existan pacientes víctimas de violaciones de derechos humanos o infracciones graves al Derecho Internacional Humanitario, el tiempo del tratamiento documental se duplicará.

Así mismo y para que las entidades prestadoras del servicio de salud puedan realizar el proceso de eliminación de la Historia Clínica, se debe haber cumplido el tiempo de retención y conservación al igual que se haya realizado el proceso de publicación a que se refiere la resolución 839 de 2017 y que se haya adelantado la valoración correspondiente.

Una vez se realice la eliminación se dejará constancia en un acta firmada por el representante legal o el revisor fiscal de la entidad. Para los profesionales independientes, una vez realizado el proceso de valoración, el acta será suscrita únicamente por dicho profesional.

Por todo lo anterior y con el fin de brindar la seguridad a la protección de los datos la implementación del mecanismo se deberá realizar de manera gradual, teniendo en cuenta que se llevará a cabo por servicios de red y deberá vincular a todas las instituciones que presten servicios de salud en el territorio. Aunado a esto la ley 2015 del 31 de enero de 2020, estableció '' En todo caso, el plazo máximo de implementación será de cinco (5) años contados a partir de la entrada en vigencia de la presente ley''(Congreso de la Republica, 2020)y deberá obedecer a criterios de interoperabilidad, protegiendo los datos, avances y sistemas existentes en los distintos prestadores de salud.

Conclusiones

Podemos evidenciar una vez realizado el trabajo de Protección de datos una visión comparada entre Colombia y España, que tanto en Colombia como en España, existen normativas vigentes para la implementación y puesta en marcha de las historias Clínicas electrónicas, actualmente en España ya se encuentra implementada y tiene control en la disponibilidad de la información sensible que se maneja de los pacientes, esto teniendo en cuenta que la seguridad está controlada por un responsable del tratamiento de los datos, el cual se debe encargar de que se cumplan las leyes a cabalidad.

Por otra parte, en Colombia aún no se encuentra implementada, toda vez que de acuerdo con la ley 2015 del 31 de enero de 2020, en el 2021 el Ministerio de Salud deberá determinar los aspectos técnicos que deben cumplir las EPS para implementar la Historia Cínica Electrónica y en máximo 5 años todo el país deberá contar con la Herramienta sistemática que permita la interacción de los datos.

Finalmente, poder contar con la Historia Clínica electrónica es un avance muy significativo en la medicina y prestación del servicios de salud, toda vez que les facilita a los profesionales de la medicina obtener la información detallada de cada paciente y poder realizar los tratamientos de forma segura y confiable, y es así como podremos obtener de forma inmediata los resultados de los antecedentes clínicos y tener la seguridad que en cada consulta podemos ser tratados con los medicamentos adecuados para cada tipología que se presente en cada instante de nuestras vidas, de otra forma con la situación actual que estamos viviendo a nivel mundial se hace necesario tener este tipo de herramientas para evitar las aglomeraciones que se presentan a diario en las clínicas y hospitales donde se corre el riesgo de contraer otro tipo de enfermedades que nos pueden agravar si tenemos patologías existentes.

Referencias

Congreso de la Republica. (2008). *Ley 1266 .* Bogota: Congreso de la republica.

Congreso de la Republica. (2012). *Ley 1581.* Bogota: Congreso de la republica.

Congreso de la Republica. (2020). *Ley 2015.* Bogota Colombia: Congreso de la Republica.

Constitucion Politica. (1991). *Constitucion Colombia.* Bogota D.C.: Estado Colombiano.

Corte Constitucional. (1992). *Setencia T- 414.* Bogota: Corte Constitucional.

Corte Constitucional. (2002). *T-729.* Bogota: Corte Constitucional.

Corte Constitucional. (2008). *Setencia T-158A .* Bogota Colombia: Corte Constitucional.

Corte General de España. (2003). *Ley 59 .* Madrid: Corte General de España.

Europa, C. d. (1997). *Convenio sobre Derechos Humanos y Biomedicina.* Oviedo: Consejo de Europa.

Gobierno de Navarra. (2010). *Ley Foral de 2010.* Navarra: Gobierno de Navarra.

Gobierno Español. (1992). *Boletin Oficial de estado 262.* Madrid.

Gobierno Nacional. (2008). *Ley 1266 de 2008.* Bogota D.C.: Estado Colombiano.

Jefatura de Estado. (1999). *Ley Orgánica de Protección de Datos de Carácter Personal.* Madrid España: Rey de españa.

Jefatura de Estado. (2002). *Ley 41 de 2002.* Madrid España: Rey de españa.

Jefatura de Estado. (2018). *Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales.* Madrid España: Rey de España.

Jefaturade Eestado. (1992). *Ley organica 5/1992.* Madrid España: Rey de España.

L.E., G. (1953). *The Florence Nightingale Pledge.* Detroit: Farrand Training School for Nurses.

La Asociación Médica Mundial preconiza . (1948). *2a Asamblea General de la A.M.M. .* Ginebra Suiza.

Ministerio de Salud. (1999). *Resolucion 1995.* Bogota D.C.: Ministerior de Salud.

Padres de la Constitución. (1978). *Constitucion español 1978.* Madrid España: Rey de España.

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento General de Protección de Datos.* España: Parlamento Europeo y Consejo de la Unión Europea.

RCNRadio.com. (10 de 02 de 2020). *Ministerio de Tecnologías de la Información y Comunicaciones*. Obtenido de https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/MinTIC-en-los-Medios/125903:Historia-clinica-electronica-empieza-a-implementarse-en-Colombia

Real Academia Española. (2014). *Real Academia Española*. Obtenido de https://www.rae.es/

Tribunal Supremo - Sala penal . (2001). *Sentencia 574/2001.* Madrid : Tribunal Supremo - Sala penal .