MEDIDAS DE PROTECCION DE LOS DATOS MEDICOS CONTENIDOS EN LA HISTORIA CLINICA DE LOS PACIENTES DEL SECTOR SALUD EN COLOMBIA

Nicole Julieth Alfonso Nieto[1]

Universidad Pontificia Bolivariana
Bucaramanga, Colombia
nimidi@hotmail.com

Resumen

El desarrollo de la tecnología y la implementación de la misma en las diferentes áreas, ha permitido un mayor avance en campos como la ciencia y la medicina; sin embargo, así como el avance genera desarrollo y este a su vez innovación, también aparecen nuevas brechas en el ámbito de seguridad que antes no se habían percibido. Siempre se ha procurado buscar la confidencialidad de cierto tipo de datos, su cuidado y sobre todo la integridad de los mismos, por lo cual a este ritmo de crecimiento acelerado de la tecnología es imposible no incluir los datos médicos de los pacientes en este nuevo avance. El objeto de este documento es realizar un análisis profundo sobre las regulaciones actuales en Colombia con respecto al trato de los datos médicos contenidos en la historia clínica, y las regulaciones existentes en otros países, con el fin de presentar las recomendaciones necesarias para alcanzar la confidencialidad, integridad y disponibilidad de los datos de la historia clínica.

Palabras claves

Datos Médicos, Regulación Datos Médicos, Historia Clínica Electrónica, Seguridad, Protección de Datos.

[1] N. Alfonso, Esp. En Gestión y Regulación de las Telecomunicaciones, Universidad Externado de Colombia

Abstract

The Technology development and implementation of the same in different areas, has allowed further progress in fields like science and medicine, however, the development and technological progress generates turn this innovation, including new listing gaps in the security field had not previously perceived. Always has been searched the confidentiality of certain types of data, care and above all their integrity, so this rapid growth of technology is impossible not to include medical data of patients in this new development . The purpose of this paper is a detailed analysis on current regulations in Colombia regarding the treatment of medical data contained in medical records, and regulations in other countries, in order to make the necessary recommendations to achieve confidentiality, integrity and availability of data from medical records.

Keywords:
Medical Information, Regulatory Medical Information, Electronic Record of Health, Security, Data Protection.

1. Introducción

Con el constante crecimiento de la tecnología y el desarrollo de la misma, surge en la sociedad un bien imprescindible, permanentemente comercializado y un insumo diario para los sistemas informáticos del mundo entero, la información, el bien más consumido, perseguido, robado e incluso asegurado, por la sociedad. Los datos personales son una clase de información que circula libremente por la red, a lo cual cientos de personas pueden tener acceso, pues estos datos viajan sin restricción, traspasan las fronteras, y pueden ser fácilmente recolectados y almacenados por quienes estén interesados. Bajo este pretexto si los datos que circulan libremente por la red hacen referencia a datos de carácter personal es necesario que estos sean sometidos a regulaciones, restricciones y controles que garanticen la seguridad y protección para no violar los derechos de los individuos que se vean directamente afectados.

Lo anterior en cuanto a datos de carácter personal sin embargo, cuando la tecnología ha alcanzado aéreas como la ciencia y la medicina, y se maneja información sobre la salud de los individuos, asistencia sanitaria e historia clínica, tanto la regulación aplicable como las medidas de protección y control sobre este tipo de datos deben ser más rigurosas, garantizando su confidencialidad, integridad y disponibilidad de los mismos.

Esta investigación surge con el fin de mostrar cuáles son las falencias en el manejo de los datos médicos de los pacientes en especial con aquellos datos que están contenidos en la historia clínica, cómo se garantiza su confidencialidad y cuáles son las regulaciones o normatividades en Colombia que obligan a todos aquellos que tienen acceso a este tipo de datos a garantizar la confidencialidad del paciente. En igual proporción se pretende realizar una comparación con países como Estados Unidos y España los cuales han innovado en esta área en torno a la creación de leyes y normas logrando alcanzar en algunos aspectos la confidencialidad, integridad y autenticidad de estos datos.

2. Datos Personales

Para poder entrar a analizar cómo debe ser el tratamiento de los datos médicos en Colombia en especial la historia clínica, se hace necesario comprender los conceptos de dato personal, dato medico e historia clínica; igualmente conocer los conceptos de los mismos en la normatividad de los países de España y Estados Unidos los cuales ya tienen una regulación vigente con respecto al tratamiento y protección de los datos personales y más especialmente los datos médicos.

El concepto de dato personal y su normatividad, nace como respuesta del avance tecnológico al que se ve enfrentado la sociedad, ya que resulta innegable el hecho que la información era recopilada, almacenada, tratada y difundida de un lugar a otro sin restricciones, sin controles y sin mecanismos que le permitieran a los usuarios dueños de esta información garantizar el cumplimiento de sus derechos fundamentales.

En respuesta a lo anterior y conscientes que la tecnología avanza en todos los campos, nace el concepto de dato personal inicialmente en la Comunidad Europea donde el Parlamento Europeo y el Consejo de la Unión Europea dictan la Directiva 95/46/CE del 24 de Octubre de 1995 en la cual se estable el concepto de Dato personal como: “Toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos, específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural y social.” [1].

Sin embargo teniendo en cuenta el rápido crecimiento de las redes y la premura por la protección de los datos que en ellas se encuentran, la Comunidad Europea expide la Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa, en la cual se concientiza que tanto la recogida u obtención de los datos médicos así como también el procesamiento de los mismos, debe ser regulado y que debe primar la confidencialidad y la seguridad de los datos personales, garantizando como aspecto primordial que estos se emplean de acuerdo con los derechos y libertades fundamentales del individuo y en particular el derecho a la intimidad.

Según la Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa se nombra la definición de dato personal, “Los datos personales abarcan cualquier información relativa a un individuo identificado o identificable. Un individuo no se considerará "identificable" si la identificación requiere una cantidad de tiempo y de medios no razonables. En los casos en que el individuo no sea identificable, los datos son denominados anónimos.”[2]. Con base en la Directiva y en la Recomendación anterior España a través de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) 15/1999 del 13 de Diciembre, en el Articulo 3, numeral a. Define los datos de carácter personal como “Cualquier información concerniente a personas físicas identificadas o identificables.” [3]

Por otra parte el gobierno de Estados Unidos al ver el constante desarrollo de las redes informáticas crea la ley Privacy Act of 1974 en la cual en el Titulo 5, numeral 552a. se instaura el concepto de dato personal como “Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or

the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." [4]

No obstante en Colombia la definición del concepto de dato personal se instituye solo hasta el año 2008 con la expedición de la Ley 1266 del mismo año, en la cual en el artículo 3 se establece:"Dato personal es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados." [5]

2.2 Datos Médicos

Bajo el concepto anterior y entendiendo que existen diferentes tipos de datos personales se crea una definición especial para los datos que tienen que ver con la salud, los cuales según la normatividad del país son llamados datos médicos, sanitarios o datos de información médica.
En la Comunidad Europea Según la Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa los datos médicos son "*Todos los datos personales relativos a la salud de un individuo. Se refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos.*" No obstante teniendo en cuenta que en España la Ley LOPD no establece un concepto de dato médico, se dicta el Real Decreto 1720 de 2007 con el cual se regula la ley LOPD y en el cual se estable el concepto de dato medico en el Articulo 3 numeral g) como "*Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.*"[6]

Sin embargo en otros países como Estados Unidos, viendo la importancia de regular y proteger especialmente este tipo de datos nace la Ley de Portabilidad y Responsabilidad del Seguro Médico *(Health Insurance Portability and Accountability Act (HIPAA) of 1996)* en la cual aparece el concepto de Información de Salud (Health Information) como "*Any information, whether oral or recorded in any form or medium, that:*
a) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and b) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual." [7]

Por otra parte en países como Colombia aunque tenemos el concepto de Dato personal en nuestras leyes, y estamos entrando en una nueva etapa del derecho colombiano en la cual se ve la relevancia de regular el desarrollo tecnológico y junto con este la información que se maneja a través de el mismo, aun no se ha visto la importancia de la protección de la información que radica en los datos médicos, ni de salvaguardar la intimidad de los pacientes; la ley que hace referencia en cuanto a la protección de datos se trata, es la ley 1266, sin embargo la misma no hace menciones con respecto a datos relativos a la salud, por el contrario es una ley de aplicación sectorial es decir la ley 1266 de 2008 es una regulación parcial y solo resulta aplicable a los datos e información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, según el concepto 2009029082 – 002 del 2 de junio del 2009

de la Superintendencia Financiera de Colombia. Por ello para la Ley colombiana existe el concepto de dato personal y su protección pero no existe el concepto de dato médico, ni su regulación.

3. La Historia Clínica

Uno de los documentos más complejos y de mayor importancia en la salud de un paciente es la historia clínica, pues contiene un registro cronológico y detallado de todos los aspectos de su salud y de su familia, así como también todos los procedimientos médicos efectuados a lo largo de su vida. Sin embargo pese a su connotación este puede ser un documento de carácter público en cuanto el mismo es utilizado para fines de investigación médica, privado ya que maneja datos íntimos del paciente que requieren su previa autorización, o semipúblico pues los derechos de su acceso son limitados y dados solo en ciertas ocasiones especiales.

Con base en el concepto anterior, la mayoría de los países han creado una legislación especial para la Historia Clínica (HC), pues maneja datos fundamentales de los cuales puede llegar a depender la vida del paciente en cualquier momento.

La legislación Española definió el concepto de HC a través de la Ley 41 de 2002 en los Artículos 3 y 14 (Ley Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica) en la cual la HC es "*El conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.*"[8]

Por otra parte en la Ley Privacy Act of 1974 en el 552(a)4 de Estados Unidos se establece el concepto de Registro como "*The term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."* [4] En el cual se incorpora las historias clínicas de los pacientes como registros que contienen información que permiten identificar a un individuo.

En Colombia de igual manera, con el fin de tener un concepto claro acerca de la HC el cual pueda ser regulado, se expide la Ley 23 de 1981 en la cual en el artículo 34 se define el concepto de HC como "*El registro obligatorio de las condiciones de salud del paciente. Es un documento privado, sometido a reserva, que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley."[*9] Debido a su importancia para la prestación de los servicios de salud, para el desarrollo científico e igualmente el desarrollo cultural y al ver la necesidad de proteger la confidencialidad del paciente, se expide en Colombia la Resolución 1995 de 1999, en la cual en el Articulo 1 también se hace referencia al concepto de HC como "*Un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.*"[10] De igual manera se establecen normas para el manejo de la HC y se aclaran otros conceptos como el de Estado de Salud, Equipo de Salud e HC para

efectos archivísticos.

4. La Historia Clínica Electrónica

Teniendo un concepto claro de lo que es un dato personal, un dato médico o información de salud y lo que es la HC para cada país, con la revolución de las telecomunicaciones y el desarrollo de la tecnología, esta logra penetrar en el área de la salud, con el único fin de facilitar el manejo de la información de los pacientes, como también de brindarle diferentes servicios y facilidades tanto a la empresas prestadoras de servicios de salud como al personal médico a cargo.

No obstante ya que la HC es utilizada como un acta que guarda todo lo relacionado con la salud, la misma está amparada por normas de privacidad y confidencialidad, por ser de igual forma un elemento jurídico y de carácter pericial probatorio, está sujeto a todos los requerimientos de la ley; por ser un elemento de evaluación de calidad sanitaria, a través de esta es posible realizar un análisis técnico, como también ser objeto de estudio y finalmente por ser una de las mayores fuentes de información para la construcción de bases de datos epidemiológicas y poblacionales, su naturaleza legal depende completamente de su modo de empleo. [11]

De acuerdo a las características descritas y teniendo como base el actual desarrollo aparece el concepto de Historia Clínica Electrónica (HCE) o Historia Clínica Informatizada (HCI), el cual a nivel general podríamos definirlo como "*El conjunto global y estructurado de información, relacionado con los procesos de la asistencia médico-sanitaria de los pacientes, soportado en una plataforma informática para cumplir con las expectativas de todos los usuarios*."[11] Uno de los primeros países en implementar las tecnologías de la información y arriesgarse a la sustitución de la HC tradicional por la HCE fue Estados Unidos, el cual a través de la Ley de de Tecnología de la Información de Salud (*Health Information Technology for Economic and Clinical Health Act (HITECH)*) establece el concepto de Historia Clínica Electrónica como "*Electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.*"[12]

De igual forma países como España al ver este nuevo auge de las telecomunicaciones en los diferentes sectores, expidieron nuevas leyes en las cuales se pudiera regular el tratamiento, la recolección y el almacenamiento de datos médicos a través de los sistemas de información(SI), y aunque no existe una definición normativa de la HCE, la misma es considerada como "*el conjunto de documentos, tanto escritos como gráficos, que hacen referencia a los episodios de salud y enfermedad de una persona, y a la actividad sanitaria que se genera con motivo de esos episodios*". [13]
De la misma manera en Colombia al ver la necesidad de implementar sistemas informáticos para mejorar la calidad, eficiencia, efectividad y disponibilidad de los datos de la HC, e igualmente el ver los resultados de la implementación de la HCE en otros países, se impulso al estado a legislar de una manera muy precaria la iniciativa de instaurar la HCE en Colombia, razón por la cual aunque no se tiene un concepto normativo legal de la HCE, si se hace mención y se establece que la misma debe ser implementada antes del 31 de Diciembre de 2013 según la Ley 1438 del 19 de Enero de 2011.

5. La Privacidad y La Seguridad de la HCE en Estados Unidos y España.

La privacidad y la seguridad de los datos médicos son unos de los pilares más importantes para el tratamiento de la información, razón por la cual resulta de vital importancia que los mismos estén regulados por unas medidas básicas de seguridad de acuerdo a la legislación de cada país. A continuación se describen las medidas de seguridad instauradas en la normativa legal de España y Estados Unidos.

5.1 España

En la creación tanto de la HC tradicional como de la HCE es necesario resaltar la importancia de la relación Médico-Paciente, pues en ella se ve reflejada la confidencialidad por parte del paciente hacia el personal médico, el secreto profesional por parte del médico hacia sus pacientes y la privacidad por parte del personal médico e instituciones, como un derecho de los pacientes a mantener ciertos datos reservados. Así mismo reconociendo que el sistema sanitario español trata datos que se consideran especialmente protegidos y de los cuales al mismo tiempo se demandan características como la confidencialidad (Acceda solo quien está autorizado), Disponibilidad (Se pueda acceder en cualquier momento) e Integridad (que no hayan sido modificados); se hace indispensable instituir mecanismos de seguridad y protección que garanticen el respeto y cumplimiento de los derechos de los pacientes así como el cumplimiento de las leyes y normas éticas.

En vista de lo anterior en España se crea la normativa de protección de datos de carácter personal la LOPD, y se establece el conjunto mínimo de medidas de seguridad aplicables a los datos de carácter personal, en el Real Decreto (RD) 1720 de 2007:

- Documento de Seguridad:

Es un documento que debe elaborar el encargado de los ficheros y contiene las medidas técnicas y organizativas de obligatorio cumplimiento para el personal con acceso al sistema de información.

Contenido mínimo del documento:

- Ámbito de aplicación
- Medidas, Normas y Procedimientos de Actuación para garantizar la seguridad de los datos.
- Funciones y Obligaciones del personal con acceso a datos personales.
- Estructura de los ficheros
- Procedimiento de Notificación y Gestión de Incidencias
- Gestión de Soportes y Documentos.
- Identificación del responsable de Seguridad

- Niveles de Seguridad:

Las medidas de seguridad de los ficheros informatizados y no informatizados se clasifican en tres niveles Básico, Medio y Alto. De acuerdo al tipo de ficheros o tratamientos de datos de carácter personal se le aplican los niveles de seguridad, en este caso los ficheros y datos relativos a la salud se le aplican las medidas de seguridad de alto nivel.

- Medidas de Seguridad de Nivel Básico

- Definición de Funciones y Obligaciones del personal
- Registro de Incidencias
- Controles de Acceso
- Gestión de Soportes y Documentos
- Identificación y Autenticación
- Copias de Respaldo y Recuperación

- Medidas de Seguridad de Nivel Medio

Además de las medidas de seguridad Básicas a los ficheros o datos que se consideren de nivel medio se les deben aplicar las siguientes medidas:

- Responsable de Seguridad
- Auditoría
- Gestión de Soportes y Documentos.
- Identificación y Autenticación
- Controles de Acceso Físico
- Registro de Incidencias

- Medidas de Seguridad de Nivel Alto

Para todos los ficheros y datos de alto nivel deberán adoptarse además de las medidas del contenido mínimo del Documento se Seguridad, las establecidas para nivel medio, bajo y las siguientes:

- Gestión y Distribución de soportes.
- Copias de Respaldo y Recuperación.
- Registro de Accesos.
- Telecomunicaciones: cifrado de los datos que se transmitan por las mismas. [14], [15]

A pesar de las medidas de seguridad descritas previamente, a los datos contenidos en la HCE se les debe brindar una privacidad máxima, e igualmente deben ser compartidos entre las diferentes instituciones prestadoras de salud, por ello es necesaria la adopción de estándares para garantizar la interoperabilidad entre los diferentes sistemas de información (SI) que contienen la HCE. En España los estándares utilizados por las entidades sanitarias, así como también medidas de seguridad adicionales a la HCE son regulados y establecidos conforme al criterio de cada Comunidad Autónoma, no obstante los más utilizados en su mayoría son el HL7 y el CEN 251. [16] [17]

5.2 Estados Unidos

En el afán por hacer cumplir los derechos de todos los ciudadanos estadounidenses, por proteger la privacidad y confidencialidad de sus datos médicos, como también asegurar invaluables beneficios en cuanto a velocidad, flexibilidad y disponibilidad de su información médica; el Departamento de Salud y Servicios Humanos de Estados Unidos aprobó la Regla de Seguridad (*Security Rule (SR)*) bajo la Ley HIPAA, en la cual aparece una nueva definición de Información de Salud Protegida (*Protected Health Information (PHI)*) la cual es definida como

"*Información Medica personal identificable (individually identifiable health information) que:*

(i) Es transmitida por medios Electrónicos.
(ii) Es Mantenida en medios electrónicos.
(iii) *Es Transmitida o Mantenida en cualquier otra forma o medio.* [18]

La nueva Regla de seguridad establece los requisitos generales de seguridad para todas las entidades cubiertas (covered entities) o entidades de salud que manejan datos PHI, como también brinda un amplio margen de discrecionalidad para la selección de la tecnología a aplicar, esto con el fin de garantizar uno de los principios rectores de la Regla, la neutralidad tecnológica, ya que según esta los reguladores no deben imponer el uso de determinadas tecnologías pues las mismas pueden ser inadecuadas en ciertas circunstancias. [19]

Conviene indicar que SR establece cuatro requisitos generales para todas las entidades cubiertas:
"*1) Asegurar la confidencialidad, integridad y disponibilidad de los datos PHI que producen, obtienen, mantienen o transmiten.*
2) Proteger los datos PHI contra amenazas anticipadas que afecten su seguridad o integridad.
3) Proteger los datos PHI contra su divulgación o uso no permitido.
4) Asegurar que sus empleados cumplan con la norma." [20]

La SR de HIPAA proporciona las normas y las especificaciones de implementación de las mismas. Hay dos tipos de especificaciones de implementación: Las Requeridas u Obligatorias y las Deseables, sin embargo para las deseables, las entidades cubiertas pueden escoger la implementación de las mismas, una medida alternativa o no hacerlo y documentar la justificación.
De igual manera la SR establece tres clases de medidas de seguridad: Las Medidas Administrativas, Técnicas y Físicas; cada una de las cuales tiene sus normas con sus respectivas especificaciones de implementación.

5.2.1 Medidas Administrativas

- Gestión de procesos de Seguridad
- Asignación del Responsable de Seguridad.
- Empleados de Seguridad
- Gestión del Acceso a la Información.
- Concientización y Formación en Seguridad
- Procedimientos de Incidentes de Seguridad
- Plan de Contingencia
- Evaluación
- Contratos de Negocios Asociados y otros Arreglos. [21]

5.2.2 Medidas Físicas

- Controles de Acceso
- Uso de la Estación de Trabajo
- Seguridad de la Estación de Trabajo
- Dispositivos y Controles de los Medios de Comunicación. [22]

5.2.3 Medidas Técnicas

- Controles de Acceso
- Controles de Auditoria
- Integridad
- Persona o Entidad de Autenticación.
- Seguridad en la Transmisión. [23]

Adicional a la Regla de Seguridad el Departamento de Salud y Servicios Humanos de Estados Unidos aprobó la Regla de Privacidad, en la cual se establece que los datos PHI no pueden ser revelados sino por orden judicial o autorización expresa del paciente y más adelante en el 2009 se aprobó la Ley HITECH, en la cual las obligaciones de las reglas anteriores se extendían a todas las entidades que manejaran datos PHI y se establece el informe al Departamento de Salud y Servicios Humanos, cuando los datos PHI del paciente se vean comprometidos por violaciones o brechas de seguridad.

6. Medidas De Protección De La Historia Clínica Electrónica Para El Caso Colombiano

6.1 Garantizar la Confidencialidad, Integridad, Disponibilidad y No repudio de los datos de la HCE

Los factores más importantes en los sistemas de información es garantizar la confidencialidad, disponibilidad e integridad de los datos, estos mismos factores se deben aplicar al tratamiento de los datos médicos o información clínica. A continuación se presentan algunas medidas de seguridad que se deberían tomar para implementar de forma segura la HCE en Colombia:

@ La confidencialidad: Es garantizar que solo acceda a la información quien está autorizado, para logar esto se recomienda utilizar controles de acceso lógicos y otros mecanismos de seguridad:
  - Inicialmente una Definición de Roles y Asignación de Permisos; a través de este control se busca que solo acceda quien está autorizado, a la información permitida y el tiempo establecido.

- Autenticación de Usuarios, este control se debe implementar con el fin de identificar quien accede al sistema para evitar suplantaciones.
- Monitorización, registro y Auditoria, con el fin que todas las actividades tanto de acceso como del tratamiento de los datos queden registradas.
- Cifrado de Datos para impedir que los datos sean interpretados por personal no autorizado.

@ La Disponibilidad: Es garantizar que la información siempre este accesible en cualquier momento y desde cualquier parte, para lograrlo se recomienda definir niveles de servicio de los sistemas de información, suministrar los recursos necesarios para la operación de los mismos y si es el caso adaptar los sistemas de información existentes a los acuerdos de niveles de servicios definidos previamente.

@ La Integridad: Es garantizar que la información recopilada y almacenada no ha sido modificada, para lograr la integridad de la información se recomienda la implementación de mecanismos de prevención y detección de ataques, el uso de copias de seguridad y el empleo de la Firma Digital.

@ El No Repudio: Es garantizar que ninguna de las partes identificadas, pueda negar la participación en una determinada transacción. Para asegurar el No Repudio se recomienda el uso de las Firmas Digitales y la revisión periódica de Auditorias.[15] [24]

6.2. Definición de un Marco Legal y Regulatorio.

La única forma de lograr obtener los controles necesarios que nos brinden la disponibilidad, confidencialidad e integridad de la información es a través de una legislación del tratamiento de los datos médicos o información médica y de un marco regulatorio que brinde los mecanismos y las especificaciones técnicas para garantizar la seguridad y la privacidad de la información de salud.

Para poder implementar adecuadamente el sistema de HCE en Colombia se hace necesario la aprobación de una ley como mencionábamos anteriormente y de unos decretos reglamentarios que regulen esa ley ya que como se mencionaba en párrafos anteriores, el estado colombiano en un intento por impulsar el desarrollo con las tecnologías de la información y alcanzar el avance tecnológico de otros países, legislo de forma muy precaria la instauración de la HCE, manejando aspectos como la confidencialidad, integridad y disponibilidad de la HCE a consideración de cada institución, sin instaurar las recomendaciones u exigencias básicas necesarias de obligatorio cumplimiento para las instituciones prestadoras de servicios de salud, los requerimientos técnicos mínimos y los requisitos mínimos de seguridad para garantizar los aspectos mencionados tales como la confidencialidad, integridad y disponibilidad a los pacientes, así como también asegurar el cumplimiento de sus derechos fundamentales.

Por lo tanto, teniendo en cuenta que el derecho Colombiano tiene su base en el Derecho Español y tomando como base las dos legislaciones que se han enunciado a lo largo de este artículo y que ambas nos llevan una gran ventaja en la implementación de la HCE se sugiere:

- Inicialmente definir dentro de un Marco legal el concepto de Dato médico o información de salud.

- Instaurar una Ley de protección de los datos relativos a la salud.
- Establecer los Decretos Reglamentarios donde se definan los requisitos mínimos de seguridad que deben tener las entidades que manejen datos relativos a la salud.

Con respecto a este último ítem, teniendo en cuenta y basándonos en la legislación Española en especial en el Real Decreto 1720 y La Ley Hipaa de Estados Unidos en especial la Security Rule, en cuanto a los requisitos mínimos de seguridad se sugiere:

- Crear unas medidas de seguridad en las cuales se traten temas como los procesos de gestión de la seguridad, análisis de riesgos, gestión de riesgos, sanciones, el responsable de seguridad, entre otras. Estas medidas corresponden a las que se describen en el Real Decreto 1720 como el Documento de Seguridad, y en la Hipaa SR como Medidas Administrativas.

- Crear o establecer unos niveles de seguridad de acuerdo al tipo de datos que se trate.

- De acuerdo al nivel en que se encuentren los datos establecer unos mecanismos Físicos de seguridad tales como: Controles de acceso Físicos, registro de incidentes, Uso y seguridad de las estaciones de trabajo, Controles de los medios o equipos de comunicación, entre otras. Estas medidas corresponden a las que se describen en el Real Decreto 1720 para cada uno de los niveles de seguridad y en la Hipaa SR como Medidas Físicas.

- De igual forma de acuerdo al nivel en que se encuentren los datos establecer unos mecanismos Lógicos de seguridad tales como: Controles de Acceso Lógicos, copias de respaldo y recuperación, auditorias, seguridad en la transmisión, entre otras. Estas medidas corresponden a las que se describen en el Real Decreto 1720 para cada uno de los niveles de seguridad y en la Hipaa SR como Medidas Técnicas.

6.3 Establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI)

Para poder implementar adecuadamente la HCE es recomendable que cada institución prestadora de servicios de salud, establezca un SGSI el cual este alineado con sus objetivos, le permita cumplir más fácilmente los requisitos mínimos de seguridad establecidos en un marco legal en caso que este exista, cubrir las necesidades de todos los pacientes, así como también garantizar el cumplimiento de sus derechos.

La implementación de un SGSI en las instituciones de salud les permite abordar todos elementos que tienen que ver con la seguridad de la información desde una perspectiva global, permitiendo diseñar y seguir un esquema de acción basado en el conocimiento de los riesgos así como también a la mejora continua del mismo facilitando la adopción de nuevos objetivos y aplicando nuevas medidas.

6.4 Elección de un Estándar Internacional

Uno de los elementos más importantes para implementar la HCE es la interoperabilidad entre los diferentes SI, pues constituye el elemento fundamental para garantizar la confidencialidad,

integridad y disponibilidad de los datos entre todas las estructuras prestadoras de servicios de salud.
Para lograr la interoperabilidad es necesario planificar los SI de todas las entidades prestadoras de salud en forma integral; alineando el diseño de los SI con los objetivos del sistema de salud así como también con las necesidades de los usuarios, pensando en sistemas flexibles, modulares y escalables. [25]
Para alcanzar la correcta aplicación de un estándar y logar la interoperabilidad SI, se deben crear 3 niveles:

- *"Nivel de Sistemas: los sistemas individuales deben cumplir con un nivel básico de estandarización sobre sus datos, códigos, estructuras, relaciones y restricciones.*
- *Nivel de redes: en este nivel se aplican estándares como protocolos de comunicación, interfaces, definición de procesos, mensajes seguridad, entre otros.*
- *Nivel de infraestructura de información y servicios: este nivel implica la interconexión de diversas redes que intercambian información libremente según perfiles, convenios, reglamentos y criterios de seguridad bien determinados."* [25]

Finalmente existe una gran variedad de estándares entre los cuales Colombia debe seleccionar uno para alcanzar la interoperabilidad de los SI y lograr implementar adecuadamente la HCE, a continuación se nombran los más importantes:

- HL7 v2 y v3
- DICOM
- CEN/ISO 13606
- CDA (Otro Estándar HL7)
- OpenEHR
- IHE

7. Conclusiones

En Colombia se estableció el uso de la Historia Clínica Electrónica y aunque esto representa un gran avance en cuanto a la implementación de las tecnologías de la información en todas las áreas, el estado colombiano no tuvo en cuenta la importancia ni la privacidad de los datos que se manejan en la HCE, por el contrario como se menciona en el artículo su legislación fue de una forma muy precaria, sin garantizar el cumplimiento de los derechos de todos los pacientes; razón por la cual es necesario establecer unas medidas mínimas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la HCE, un marco legal que obligue a las instituciones prestadoras de salud a alinear sus sistemas de información para garantizar la seguridad adecuada a los datos que manejan, así como también una estandarización de todos los sistemas de información con el único fin de promover el desarrollo tecnológico, la interoperabilidad de los sistemas y el intercambio de información con otros países.

8. Agradecimientos

Doy gracias a Dios porque el da la sabiduría y de su boca viene el conocimiento y la inteligencia y a mis padres por el apoyo moral e intelectual brindado en todos los aspectos.

9. Biografía

Nicole Julieth Alfonso Nieto, Bucaramanga, Candidata a Especialista en Seguridad Informática, Especialista en Gestión y Regulación de las Telecomunicaciones, Ingeniera de Telecomunicaciones.

10. Referencias

[1]Directiva 95/46/CE, De 24 de Octubre, de 1995, del Parlamento Europeo y del Consejo de la Unión Europea, 1995.

[2] Recomendación Nº R (97) 5, De 13 de Febrero de 1997, del Comité de Ministros del Consejo de Europa, 1997.

[3] Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) 15/1999, España, 1999.

[4] Privacy Act of 1974, Estados Unidos, 1974.

[5] Ley Estatutaria 1266, Colombia, 2008.

[6] Real Decreto 1720/2007, De 21 de Diciembre, España, 2007.

[7] Health Insurance Portability and Accountability Act of 1996, Estados Unidos, 1996.

[8] Ley 41/2002 Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica, De 14 de Noviembre, España, 2002.

[9] Ley 23 de 1981 Por lo Cual se Dictan Normas de Ética Medica, De 18 de Febrero, Colombia, 1981.

[10] Resolución Numero 1995 de 1999, De 8 de Julio, Colombia, 1999.

[11] Christian Eduardo Rueda-Clausen Pinzón, “La Historia Clínica Informatizada. Evaluación de los Casos Colombiano y Español,” MedUnab, Vol. 9 Numero 1, pp. 63 – 71, Abril 2006.

[12] The Health Information Technology for Economic and Clinical Health Act, De 17 de Febrero, Estados Unidos, 2009.

[13] Javier Carnicero Giménez de Azcarate, "De La Historia Clínica a la Historia de Salud Electrónica," Informe Seis (Sociedad Española de Informática y Salud), Vol. 5, pp. 21 – 66, 18 de Diciembre de 2003.

[14] Instituto Nacional de Tecnologías de la Comunicación (INTECO), Agencia de Protección de Datos de la Comunidad de Madrid., Estudio sobre la Privacidad y la Seguridad de los Datos Personales en el Sector Sanitario Español, Instituto Nacional de Tecnologías de la Comunicación (INTECO), Octubre de 2010.

[15] R. de la E. David, S. C. Ricardo, A. D. Natxo, B. R. Oscar, G. C. Manuel, L. S. Pilar, O. G. Rafael, Seguridad de la Información en Entornos Sanitarios, Primera Edición, Ed. España: Sociedad Española de Informática de la Salud (SEIS), 2008.

[16] Javier Carnicero Giménez de Azcarate, Andrés Fernández., "Manual de Salud Electrónica para Directivos de Servicios y Sistemas de Salud," IX Informe Seis (Sociedad Española de Informática y Salud), Enero de 2012.

[17] Jorge Núñez García, Isabel de la Torre, "Medidas de Seguridad en la Implantación Historial Clínico Electrónico (HCE)," RevistaeSalud.com, Vol. 7 Numero 27, 2011.

[18] Health Insurance Portability and Accountability Act of 1996 Security Rule, 45 CFR Part 160.103, Estados Unidos, 2005.

[19] Sharona Hoffman, Andy Podgurski, "In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information", Bepress Legal Series, 2006.

[20] Health Insurance Portability and Accountability Act of 1996 Security Rule, 45 CFR Part 164.306 (a) 2005, Estados Unidos, 2005.

[21] Health Insurance Portability and Accountability Act of 1996 Security Rule, 45 CFR Part 164.308 2005, Estados Unidos, 2005.

[22] Health Insurance Portability and Accountability Act of 1996 Security Rule, 45 CFR Part 164.310 2005, Estados Unidos, 2005.

[23] Health Insurance Portability and Accountability Act of 1996 Security Rule, 45 CFR Part 164.312 2005, Estados Unidos, 2005.

[24] José Antonio Garbayo Sánchez, Jokin Sanz Ureta, "La Seguridad, Confidencialidad y la Disponibilidad de la Información Clínica," Informe Seis (Sociedad Española de Informática y Salud), Vol. 5, pp. 255 – 286, 18 de Diciembre de 2003.

[25] Selene Indarte, "Manual de Salud Electrónica para Directivos de Servicios y Sistemas de Salud," IX Informe Seis (Sociedad Española de Informática y Salud), pp. 317 – 329, Enero de 2012.