

**PROYECTO DE LEY**  
**LA LEGISLATURA DE LA PROVINCIA DE ENTRE RÍOS, SANCIONA CON FUERZA**  
**DE LEY**

**OBJETO Y ÁMBITO DE APLICACIÓN**

**ARTICULO 1º.-** Establécese el sistema de HISTORIAS CLINICAS DIGITALES (HCD) para todo paciente de cualquier Efector de Salud de la Provincia de Entre Rios.

**ARTICULO 2º.-** La presente Ley tiene por objeto:

- a) Regular el establecimiento del sistema de HCD en toda la provincia y facultar a la AUTORIDAD DE APLICACIÓN para llevar adelante esta iniciativa;
- b) Establecer los estándares mínimos de confección de las HCD para cada paciente;
- c) Garantizar el acceso de los pacientes a la información contenida en las HCD por medio de consultas electrónicas o presenciales por los pacientes o facultativos debidamente autorizados por los mismos;
- d) Efectivizar el derecho a la salud de la población mediante la provisión oportuna, en todo lugar y en tiempo real de sus datos y archivos médicos;
- e) Mejorar la eficiencia del sistema de salud en su conjunto;
- f) Proveer a la confidencialidad y suficiente protección de los datos personales y clínicos de cada paciente.

**ARTICULO 3º.-**La presente Ley será de aplicación a todo tipo de asistencia sanitaria que se preste en el territorio provincial. Se entenderá como asistencia sanitaria a toda consulta o acto médico brindado en cualquiera de los siguientes efectores:

- a) Hospitales y establecimientos sanitarios públicos en general. Se encuentran comprendidas en esta clasificación las siguientes jurisdicciones:
  - i) provincial,
  - ii) municipal.
  - iii) Unidades sanitarias

**ARTÍCULO 4º.-** DEFINICIONES. Los términos listados a continuación se entenderán definidos como sigue:

- a) HISTORIA CLINICA DIGITAL (HCD) es el conjunto de datos clínicos, catastrales y socio económicos referidos a la salud de una persona, inclusivos de sus

antecedentes familiares de enfermedades, composición del grupo familiar y hábitos del mismo, entre otros, procesados y sistematizados usando medios informáticos e incorporados por los Efectores a bases de datos relacionales y disponibles para su consulta mediante redes electrónicas de información de uso público existentes o nuevas y autorizadas o licenciadas por la Secretaría de Comunicaciones.

- b)EFECTOR DE SALUD(o Efeotor): se entiende por tal a los hospitales generales de agudos, hospitales generales de niños, hospitales especializados, centros de salud polivalentes y monovalentes, médicos de cabecera, y toda otra sede de los subsectores público o privado en la que se realizan acciones de salud.
- c)PACIENTE: Persona que padece física y corporalmente, y especialmente quien se halla bajo atención médica. Se entenderá por tal, asimismo, a aquella persona que es o va a ser reconocida médicamente.;

### TÍTULO III

#### DE LAS HISTORIAS CLINICAS DIGITALES – PRINCIPIOS APLICABLES

**ARTÍCULO 5º.-** Toda HCD constituye documentación auténtica y como tal, será válida y admisible como medio probatorio, haciendo plena fe a todos los efectos, siempre que se encuentre autenticada.

**ARTÍCULO 6º.-**Se considerará debidamente autenticada toda HCD cuyo contenido haya sido validado por una o más firmas digitales aplicadas mediante claves u otras técnicas de seguras de encriptación, conforme los procedimientos previstos en la Ley de Firma Digital N° 25.506

**ARTÍCULO 7º.-**El sistema de HCD establecido en el artículo 6º a) deberá ajustarse en todo momento a los siguientes principios generales de actuación y funcionamiento:

- a) Finalidad;
- b) veracidad;
- c) confidencialidad;
- d) accesibilidad y;
- e) titularidad particular.

Los datos que contenga la misma:

- a) Serán considerados personales, confidenciales y sensibles.
- b) No podrán ser usados en forma nominada para otros fines que no sean los asistenciales.
- c) No podrán ser objeto de tratamiento nominado alguno por medios informáticos, a menos que medie para ello expreso consentimiento informado del paciente.
- d) Sólo podrán ser considerados en términos estadísticos, conforme a las pautas que dicte la reglamentación.

**ARTÍCULO 8º.-PRINCIPIO DE VERACIDAD.** Este principio impone incluir en la HCD todos los procedimientos, sean diagnósticos o terapéuticos, que se indiquen al paciente, incluyendo la semiología realizada, la evolución del caso y todo otro dato referencial o gráfico que permita conocer la situación real del mismo.

**ARTÍCULO 9º.-**La información contenida en la historia clínica electrónica deberá exponerse en forma inteligible por el paciente y no podrá ser alterada sin que quede registrada la modificación de que se trate, aún en el caso de que ella tuviera por objeto subsanar un error. Una vez validado, ningún dato de la historia clínica electrónica podrá ser eliminado y en caso de ser necesario su corrección, se agregará el nuevo dato con la fecha, hora y contraseña (LOGIN) del que hizo la corrección, sin suprimir lo corregido.

**ARTÍCULO 10º.-PRINCIPIO DE CONFIDENCIALIDAD.** Este principio obliga a los facultativos, Efectores, el AIRIHCD y la Autoridad de Aplicación, a tratar los datos relativos a la salud de la persona con la más absoluta reserva. A tal efecto, la HCD deberá respetar los lineamientos establecidos en el artículo 6º a).

**ARTÍCULO 11º.-PRINCIPIO DE ACCESIBILIDAD.** Mediante la aplicación de este principio, el paciente tendrá en todo momento derecho a conocer los datos consignados en la HCD, a que le sean explicados ya a que se rectifiquen si fueran probadamente erróneos. No obstante, en casos excepcionales, a juicio del médico tratante y bajo su responsabilidad como parte del proceso de atención, podrán establecerse restricciones parciales o temporales a su acceso. Los métodos de acceso del Paciente a su HCD podrán ser: (a) presencial; y/o (b) electrónico a través de redes públicas o privadas de comunicaciones, conforme lo establecido en el artículo 6º d) iii).

## **TÍTULO IV**

### **DE LA AUTORIDAD DE APLICACION**

**ARTÍCULO 12º.-** La Autoridad de Aplicación de la presente Ley será determinada por el Poder Ejecutivo, en la respectiva reglamentación.

**ARTÍCULO 13º.-** La Autoridad de Aplicación adoptará las medidas adecuadas tendientes a la informatización progresiva de las historias clínicas de hasta diez (10) años de antigüedad, garantizando la integración de la información relativa a cada paciente con independencia del soporte en que se encuentre.

**ARTÍCULO 14º.-** De Forma.

## FUNDAMENTOS

Desde tiempos de Hipócrates, hasta no hace muchos años, la relación médico-paciente ha estado impregnada por el denominado "paternalismo médico", fundado entre otras cosas en la autoridad que emana del vocabulario e imagen social que representa el galeno, así como en la asimetría de información sobre una determinada patología o dolencia del que disponen las partes.

Sin menoscabo de tales consideraciones, fue abriéndose paso, impuesto por el progresivo desarrollo humano, la conciencia que tienen los pacientes de sus derechos elementales y básicos en el plano de las relaciones genéricamente denominadas "médico asistenciales", no habiendo sido ajeno a ello la labor desarrollada por los Organismos Internacionales con competencia en la materia, en especial la Organización Mundial de la Salud, que se ha preocupado específicamente sobre los derechos de los pacientes. La propia Unión Europea ha suscripto en 1997 el Convenio sobre los Derechos del Hombre y la Bio-medicina, que fue el primer instrumento internacional que da tratamiento explícito sobre los derechos de los pacientes, entre los que resalta el derecho a la información, el consentimiento informado y la intimidad de la información de la salud de las personas.

Es así que universalmente se consideran derechos inherentes a la condición de pacientes, entre otros, los siguientes:

- a) El de recibir atención médica adecuada;
- b) El de recibir un trato respetuoso y digno por parte de los profesionales de la salud;
- c) El de recibir información veraz, suficiente, clara y oportuna sobre el diagnóstico, pronóstico y tratamiento médico y a ser tratado con confidencialidad;
- d) Contar con historia o expediente clínico completo y acceso directo y personal a tal expediente;

En función del principio básico de respeto a la dignidad humana, advertimos que un conjunto de disciplinas relacionadas con la bioética, poniendo el acento en la autonomía, del cual se nutren el derecho a la información, el consentimiento

informado y el debido resguardo a la intimidad. La armonización de ambas concepciones nos facilitará reconocer tanto el respeto a la autoridad de la palabra médica, como el respeto a la voluntad del sujeto-paciente.

Entendemos que la historia clínica (independientemente del carácter público o privado que se le asigne) es un documento médico sui generis, que no participa enteramente de las características de los instrumentos públicos o privados, pero que siempre servirá como principio de prueba por escrito de los actos médicos que se incorporen a su contenido.

La historia clínica es un instrumento de forma libre, o del cual la ley no exige una forma determinada.

Como podemos observar, la obligatoriedad de firmar la historia clínica no procede explícitamente de la ley 17.132, sino que tal deber lo impone el principio general que parte del artículo 1012 del Cód. Civil, o la costumbre de la buena práctica profesional, o del cumplimiento de disposiciones reglamentarias con las que se regula la vida administrativa de los centros sanitarios en donde los médicos cumplen funciones<sup>[17]</sup>.

Con la entrada en vigencia de la ley de firma digital se equiparó al requerimiento legal de una firma manuscrita, satisfaciendo a esa exigencia, una firma digital. Este principio se aplica a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia (art. 3º, ley 25.506).

El artículo 2º de la ley 25.506 expresa que: Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Para que esta firma digital sea válida (art. 9º) debe cumplir además con los siguientes requisitos: a) haber sido creada durante el período de vigencia del certificado digital válido del firmante; b) ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; y c) Que dicho certificado haya sido emitido o reconocido, por un certificador licenciado (art. 16).

El artículo 5º de la ley 25.506 expresa que: Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de

ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

A diferencia de la firma digital, la firma electrónica no garantiza la inalterabilidad, integridad, autenticidad, autoría, verificación por terceros y confidencialidad (o bien son plasmadas fuera del período de vigencia de los certificados, o bien el certificado no ha sido emitido o reconocido por un certificador licenciado).

En el caso de utilizar firmas electrónicas corresponde acreditarla a quien la invoca ya que no goza de la presunción de autoría de la firma digital (art. 7º). Los documentos firmados electrónicamente deben ser considerados principio de prueba por escrito (art. 1192, Cód. Civil).

El artículo 13 de la ley 25.506 expresa que: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

Para que estos certificados digitales sean válidos (arts. 14 y 15) deben: a) ser emitidos por un certificador licenciado por el ente licenciante; b) responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan: 1) identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única; 2) ser susceptible de verificación respecto de su estado de revocación; 3) diferenciar claramente la información verificada de la no verificada incluidas en el certificado; 4) contemplar la información necesaria para la verificación de la firma; y 5) identificar la política de certificación bajo la cual fue emitido; y c) ser emitidos únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado. La fecha de vencimiento del certificado digital referido en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió. No obstante, la autoridad de aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

En cuanto al certificador licenciado (art. 17) es entendido como toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante[.].

La ley entiende por documento digital o electrónico a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento

o archivo. Y agrega que un documento digital también satisface el requerimiento de escritura (art. 6º, ley 25.506 y anexo I, decr. 2628/02).

Éste artículo define a los documentos digitales repitiendo en la definición el concepto del término “digital” sin explicarlo. En nuestra legislación se utilizaron indistintamente los términos “electrónico” y “digital” al momento de determinar el verdadero contenido y alcance del concepto jurídico de “documento digital” [se utilizan como sinónimos los vocablos “documento digital” (art. 6º), “documentos electrónicos” (art. 11) y “datos electrónicos” (art. 5º)] [\[20\]](#).

Los documentos digitales han sido precisados como una secuencia informática de bits, representados mediante un código binario (sistema por el cual, mediante la combinación de los dígitos binarios 0 y 1, se construyen los datos que interpretan los sistemas informáticos), que pueden interpretar cualquier tipo de información y que requieren de medios técnicos para su inteligibilidad [\[21\]](#).

Por sus características, suelen ser necesarios cuatro elementos para la existencia de estos documentos digitales, ellos son: 1) El contenido, Al igual que en los documentos manuscritos, constituido por la información o datos que en éste se incluyen. 2) El hardware, que es el soporte que contiene la información o datos (en los documentos manuscritos suele ser papel, en los digitales puede ser un disquete, CD-Rom, DVD o disco rígido entre otros). 3) El software, que es la programación informática que permite codificar la información o datos en sistema binario para que sean contenidos en el hardware. Y 4) La reproducción, que implica la utilización de hardware y software para copiar, recuperar y editar la información o datos decodificándolos p.ej. en un monitor o en una impresión gráfica.

Hay muchas ventajas que impulsan a realizar las historias clínicas informáticas.

Éstas tienen un costo más económico a mediano y largo plazo, permiten tener la información siempre disponible ocupando un mínimo lugar de almacenamiento. De esto surge invariablemente una mejora en la calidad del servicio de salud.

Una historia clínica puede estar disponible en varios consultorios al mismo tiempo, puede ser trasladada a otros hospitales (en Argentina o en el mundo) en cuestión de segundos.

Por supuesto esta nueva tecnología genera riesgos que deben ser superados. Para los hackers entrar a un ordenador suele ser una tarea relativamente sencilla... habría que garantizar que esto no ocurra con las historias clínicas ya que contienen datos sensibles que deben ser guardados con el mayor celo posible.



Asimismo se debe garantizar que los datos guardados no se extravíen y que podrán ser accedidos con el hardware correspondiente[27].

Para desarrollar didácticamente este punto creemos conveniente realizar la comparación en un cuadro sinóptico:

| Punto a comparar          | Historia clínica informática  | Historia clínica manuscrita   |
|---------------------------|---|---|
| Disponibilidad            | Siempre disponible en todo momento y varios lugares simultáneamente.                    | Disponible en un solo lugar físico y a veces extraviada.                  |
| Contenido                 | Siempre completa.   | A veces fragmentada para atender las necesidades de varios usuarios.      |
| Tipografía                | Siempre legible.  | Algunas veces ilegible.   |
| Firma                     | Siempre firmada.  | A veces sin firma.  |
| Datación                  | Siempre con fecha y hora.   | A veces sin fecha y hora.   |
| Continuidad               | Los hechos y actos son expuestos cronológicamente.                                      | Es posible modificar la continuación temporal de los sucesos.             |
| Calidad de la información | Potenciales tratamientos redundantes reducidos.   | Incompleta y a la vez plagada de información duplicada e innecesaria.     |
| Ingreso de datos          | Es estandarizado.   | Varía según la necesidad de cada servicio.                                |
| Almacenamiento            | Es más económico el soporte físico y su reproducción. Además ocupa un espacio reducido. | Es más costoso y ocupa un mayor espacio físico.                           |
| Errores                   | Por los motivos antes expuestos, suelen ser menor la cantidad de errores.               | Por los motivos antes expuestos, suelen ser mayor la cantidad de errores. |

Como se puede apreciar, las ventajas surgen de esta simple comparación y nos hace pensar que la tendencia será hacia la digitalización de la historia clínica; solo resta discutir como debe ser realizada.

Con el transcurso del tiempo se han ido fijando criterios para elaborar y conceder autenticidad a la historia clínica manuscrita. Creemos conveniente que la historia clínica

informática garantice ciertos aspectos[29]:

1) Inviolabilidad e inalterabilidad de los datos que contiene

Esto incluye tomar las medidas de seguridad pertinentes para impedir el ingreso de virus o hackers en el sistema, impidiendo la consulta, el borrado o modificación de datos ya incorporados por personas sin autorización. Para esto es conveniente que esté equipada con un sistema de alarmas o alertas.

2) Recuperación de los archivos

El sistema debe contemplar la posibilidad de que los datos sean recopilados en una o más copias de seguridad (back up), que faciliten su transporte e incluso generar fácil y económicamente copias para el propio paciente.

3) Perdurabilidad de la información

También deben asegurar la conservación del hardware que contiene al software, es decir que debe estar almacenado en un medio adecuado en el que no lo afecte la humedad, la temperatura, etcétera.

Este software debe ser siempre contenido en un hardware útil del cuál sea fácil la extracción de la información con dispositivos actuales en materia de informática (por ejemplo si los datos están almacenados en disquetes de 5 ¼ y teniendo en cuenta que ya no se fabrican ese tipo de disqueteras, debería almacenarse en otro tipo de hardware como por ejemplo disquetes de 3 ½, CDs o DVDs).

4) Continuidad temporal

El programa informático no debe permitir que se altere la secuencia de llenado de la historia clínica, es decir que no sea posible modificar la continuación temporal de los hechos y actos.

5) Garantía sobre la posibilidad de inspección por el ente correspondiente (justicia, organismos estatales de control, etcétera)

Así como se requiere la historia clínica manuscrita, es imprescindible que el sistema informático admita el acceso de las autoridades que ejercen controles por parte de la Administración pública, así como también por parte de la justicia.

6) Aseguramiento de la remisión de la historia clínica al tribunal que la solicite

y recaudos para su posible secuestro judicial

La historia clínica suele ser indispensable como prueba en juicio, es por esto que también se debe contemplar la posibilidad de ser remitida al tribunal que la requiera.

A diferencia de la realizada en soporte papel, la digitalizada evita las medidas anticipativas, como el secuestro judicial ya que se torna innecesario debido a que cada copia que se realiza tiene el mismo valor que la original[30].

#### f) La historia clínica informatizada como base de datos personales

Los datos que deben recopilarse en la historia clínica son aquellos relevantes para el paciente específico al que se está tratando. En líneas generales la información a recoger incluye: 1) características del paciente como edad, sexo, peso, altura; 2) sucesos de la enfermedad actual, historia médica anterior, historia social; 3) alergias, hábitos (alcohol, tabaco, ejercicio), dieta, datos sobre el cumplimiento de los tratamientos prescritos; 4) pruebas de laboratorio, constantes vitales; y 5) farmacoterapia que está recibiendo o que ha recibido[.].

Como estos datos se recogen en un soporte informático, se facilita considerablemente la explotación posterior de los mismos[32], por lo que dicho uso está condicionado por nuestra Constitución nacional y ley 25.326 de hábeas data.

Tengamos en cuenta que esta legislación se aplica tanto a la historia clínica tradicional como a la digital, aunque en el particular caso de ésta última se deben hacer mayores esfuerzos para mantener la privacidad y confidencialidad de los datos almacenados y de los que serán transferidos.

#### g) Privacidad y confidencialidad

La privacidad y confidencialidad de los datos es quizá uno de los desafíos más importantes en esta materia. Estimamos conveniente que las historias clínicas se guarden en una red cerrada en la que solamente se pueda acceder desde dentro de la institución médica y que únicamente se coloquen para ser accedidas por Internet las que deben ser transferidas a otra institución (solamente por el tiempo que dure la transferencia de datos y luego debe ser eliminada de ese lugar).

Trabajando en una red cerrada (intranet) estaríamos restringiendo la posibilidad de que los hackers tengan acceso a los datos de las historias clínicas desde fuera de la institución. Aunque esto no garantiza de que se acceda desde alguna terminal de la red interna (de darse este supuesto es muy probable que se trate de un sabotaje, pero tengamos en cuenta que los sabotajes también pueden llevarse a cabo con las historias

clínicas tradicionales).

Estamos en condiciones de afirmar que ésta debe ser la forma de trabajo que debe utilizarse para llevar las historias clínicas informáticas para garantizar los niveles más altos de privacidad y confidencialidad de los datos.

La importancia de la historia clínica no es tema de discusión, independientemente del soporte en el que se plasme.

Entendemos que es necesaria una legislación que la regule en forma concreta ya que este documento médico es imprescindible por lo que dice, o por lo que no dice y prueba por lo que explícitamente tiene registrado, o por lo que implícitamente se deduce de sus anotaciones.

En dos años, los 40 millones de argentinos estarían registrados en el Sistema de Identificación Biométrico y podrán ser identificados, con el Sistema Federal de Identificación Biométrica para la Seguridad (Sibios).

Sobre el tema, la presidente Cristina Fernández de Kirchner explicó además que se aplicará en todos los recién nacidos para "combatir el delito" y el tráfico de menores. El sistema Sibios permitirá contar con información que individualice a todos los ciudadanos a través de un software de última generación, mediante un convenio con el Registro Nacional de la Personas.

El Registro Nacional tiene a su cargo la inscripción e identificación de las personas físicas domiciliadas en territorio argentino o en jurisdicciones argentinas y el otorgamiento de Documento Nacional de Identidad y de Pasaportes Nacionales. El Ministerio de Seguridad será la autoridad de aplicación del sistema que será utilizado por la Policía Federal, Gendarmería Nacional, Prefectura Naval, Policía de Seguridad Aeroportuaria, Registro Nacional de las Personas y la Dirección Nacional de Migraciones.

Además, el dispositivo instituido por la presidenta de la Nación está diseñado para incorporar al sistema a las provincias. El decreto presidencial invita a las Provincias y a la Ciudad Autónoma de Buenos Aires a adherirse al SIBIOS con miras a que también puedan formular consultas biométricas en tiempo real.

El año pasado una falla de seguridad permitió la descarga de fotos de todos los argentinos del padrón electoral, por lo que hoy la base de datos ya estaría en manos privadas o en manos de un servicio de inteligencia extranjero. El Registro Nacional de las Personas reconoció la falla pero le echó la culpa al Poder Judicial. Esta es la antesala de

lo que vendrá: los organismos se echarán la culpa entre sí mientras que el daño ya estará hecho.

Que el Estado garantice la identidad de cada ciudadano es un derecho humano fundamental, y a eso deben limitarse los documentos; todo lo demás son aditivos que, además de su dudosa constitucionalidad, son prescindibles y traerán más riesgos que beneficios. Porque a diferencia de una llave o clave virtual, no podremos reemplazar nuestras huellas o rostro ante alguna suplantación de identidad o error técnico.

Las ventajas en cuanto a la informatización de éste documento son abrumadoras. Entendemos que no debe haber una prohibición que impida realizarlas en soporte magnético, pero si que deben estar debidamente controladas garantizando los más altos niveles de confidencialidad de los datos que contienen.

En cuanto a las exclusiones de la ley de firma digital (actos personalísimos y de última voluntad) estimamos conveniente que para un óptimo provecho de la nueva tecnología, no deberían ser aplicadas estas restricciones.

Por todo lo expuesto solicito a los señores legisladores acompañar con su voto afirmativo el presente proyecto.