# ASPECTOS MÉDICO-LEGALES DE LA HISTORIA CLÍNICA ELECTRÓNICA.

**Dr. Fabián Vítolo NOBLE S. A. ®**

La progresiva informatización de la documentación médica ha estado acompañada tradicionalmente por dudas de los profesionales y las autoridades de los establecimientos médicos acerca de su validez en procesos judiciales. Esas dudas han dificultado en parte la expansión de un sistema con innumerables ventajas y han conducido a la adopción de medidas parciales (utilización sólo en determinadas áreas) o bien duplicadas (a pesar de contar con la herramienta electrónica, se imprime y firma todo).

En ámbitos médico-legales, hasta principios de este siglo, siempre se hablaba de un cierto vacío legal con respecto a este tema. Las primeras historias clínicas electrónicas solían presentar el inconveniente de que no garantizaban la inalterabilidad de su contenido ni su autoría. Estos inconvenientes las hacían inadmisibles e ineficaces probatoriamente.

Si bien todavía persisten algunas dudas puntuales, la sanción de la Ley 25.506 de Firma Digital en el año 2001 (1) comenzó a llenar gran parte del vacío legal mencionado al brindar un marco normativo a estas nuevas tecnologías, regulando lo concerniente al empleo de la firma digital y la firma electrónica, a las que se les asigna un valor jurídico. La ley modifica sustancialmente el concepto de documento contenido en el Código Civil, asociado a la forma escrita, (art. 978 CC) y realizado en soporte de papel, equiparando a la firma ológrafa con la firma digital y la firma electrónica. Antes de la ley mencionada, cualquier documentación digital no tenía el carácter de documento que ahora sí tiene.(2) Según la legislación se entiende por documento digital a *"la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo, Un documento digital también satisface el requerimiento de escritura (art 6). "* Se equiparan entonces al papel soportes tales como discos rígidos, discos compactos, diskettes, etc. en tanto son medios capaces de contener o almacenar información para su posterior reproducción. La Ley de Firma Digital es el elemento jurídico que hace posible que la historia clínica computarizada no sea cuestionable desde el punto de vista legal.

## Historia Clínica Electrónica (HCE) y Registros Médicos Informatizados (RMI)

Los cambios ocurridos en las últimas décadas en el sistema prestacional requieren el acceso y la integración de la información de los pacientes entre los profesionales, los centros diagnósticos, los hospitales y los pagadores. La historia clínica no sólo cumple fines médicos sino también administrativos, estadísticos y legales.

Si bien la historia clínica es el documento más importante de la atención médica en condiciones de informatización, no es el único registro. Se consideran Registros Médicos Informatizados (RMI) a todos los archivos informáticos que contengan alguna información relativa al paciente, sus estudios complementarios y su tratamiento, entre ellos: (3)

- Historia clínica electrónica (HCE)
- Registros de admisión y egresos
- Archivos de laboratorio de análisis clínicos
- Bases de estudios complementarios (radiología, tomografías, ecografías, otros)
- Archivos de reserva de turnos
- Archivos de facturación y otros.

La HCE es el documento que debe estar más protegido. Sin embargo, todos los otros registros deben tener restricciones y reservas, dado que contienen información que puede perjudicar al paciente en caso de difundirse.

Quienes consideren a la historia clínica electrónica como la simple transcripción a la computadora de lo que se escribiría en un papel con el limitado objetivo de ahorrar su uso, despejar los depósitos y hacer las historias más legibles probablemente desaprovechen las ventajas de un sistema bien diseñado. La mera automatización de la forma, el contenido y los procedimientos de documentación actual en papel perpetuará sus deficiencias y será insuficiente para cumplir con las necesidades crecientes. (4)

La historia clínica está conformada por la información provista por distintos actores (médicos, enfermeras, interconsultores, auxiliares, etc). Cada uno debe hacerse responsable de la información que genera y debiera firmar electrónica o digitalmente. A su vez esta información suele estar atomizada en registros de varias tablas, en estructura de datos relacionales. Estos datos pueden ser alterados por distintos procesos, por lo que se impone una metodología que permita recuperar esos datos de distintas tablas y registros y congelarlos en un campo donde permanezcan inalterables al momento de firmarse. Por otro lado debe contemplarse un campo en donde se almacene quién generó la información, en qué fecha y hora, a quién pertenece y quiénes están autorizados a leerla. (Esto último, en términos técnicos, se denomina guardar el “hash” generado por la clave privada.) (3)

## Ventajas de la Historia Clínica Electrónica

Las ventajas médicas, legales, operativas, económicas y aún ecológicas de la historia clínica electrónica sobre la historia clínica en papel son innumerables. (1) (5) (6) (7)

### Ventajas Médicas

- Mejora el acceso a la información: La recuperación de una pieza específica de la historia es mucho más rápida: una computadora puede entregar un dato en segundos, frente a los minutos u horas que puede requerir localizar, obtener y revisar una historia clínica convencional. Diferentes usuarios autorizados pueden consultar la misma información desde distintos puntos y en forma simultánea. Se facilita de esa forma la comunicación del equipo de salud y se garantiza el acceso en casos de emergencia.

- Facilita la historia clínica única: Se evita la actual fragmentación que existe actualmente en muchas instituciones entre las historias de consultorios externos, de guardia y las de internación. Cada paciente tiene así un solo número de historia y su gestión queda centralizada en un archivo único, garantizando que todos los sucesivos episodios de ese paciente queden conservados juntos. Cada paciente tiene un número de referencia obligatoriamente único, lo cual permite colgar del mismo todos los registros asistenciales que se le presten, pudiendo integrar a su vez dicha información con datos de farmacia, de facturación, etc.

- Permite la incorporación de imágenes digitales. A su vez, las mismas pueden ser revisadas a distancia por médicos expertos en aquellas situaciones en las que se lo requiera.

- Facilita los trabajos estadísticos y científicos: Al estar la historia estructurada en forma de base de datos, es más fácil recuperar la información necesaria que en las historias en papel

- Permite incorporar sistemas de apoyo a la decisión clínica (algoritmos y protocolos de estudio y tratamiento), recordatorios de práctica y conexión con cuerpos de conocimiento médico.

- Permite incorporar un vademecum institucional, con sistemas de alerta en caso de contraindicaciones, interacciones o sobredosis (las dosis incorrectas no son tomadas por los campos).

- El ingreso estandarizado de datos y el uso obligatorio de algunos campos para pasar de pantalla disminuye la posibilidad de olvidos y errores (ej: olvidar chequear alergias)

### Ventajas Legales (1)

- La historia clínica electrónica contribuye a que la documentación médica sea llevada de acuerdo a los requisitos formales establecidos por las distintas normativas y por la jurisprudencia:

  - Siempre legible
  - No permite espacios en blanco ni alteración del orden de los asientos
  - Siempre firmada
  - Siempre con fecha y hora
  - Siempre completa
  - Se evitan las correcciones, raspaduras, agregados, etc.

- Evita las medidas anticipativas, como ser el secuestro judicial, dado que mediante la firma digital se garantiza la identificación de una persona y la autenticidad del documento y la medida resulta entonces innecesaria.

- Por las mismas razones, no resulta necesario solicitar judicialmente el reconocimiento de la firma del profesional que hubiere firmado digitalmente en la historia clínica.

- Como la historia clínica informatizada tiene el valor de un original, cuando el paciente solicita una copia de ella, como es su derecho, (ya sea durante su internación o su egreso), y a posteriori se llegare a producir la pérdida o extravío de la que se encuentra en poder del establecimiento o profesional, habrá hasta el momento en que se produce el extravío, certeza sobre los datos consignados en la historia clínica digital que el paciente tiene en su poder.

**Ventajas operativas, económicas y ecológicas.**

Son bien conocidos los problemas que traen aparejadas a las instituciones y a los profesionales las historias clínicas en papel. El crecimiento continuo del volumen almacenado llega a crear graves problemas de espacio físico, a lo que se suma el inevitable trasiego de documentos originales, con riesgo de pérdida o deterioro.

Son muy ilustrativos algunos ejemplos publicados. Un interesante trabajo de 1998 describe el verdadero caos que representa el manejo de las historias clínicas en un Hospital General de Agudos de la Ciudad de Buenos Aires: (8)

75 m2 de superficie de archivo
504 metros lineales de estantería.
200.000 historias clínicas archivadas por quince años.
100 movimientos de historias de internación
2000 consultas por día
16 empleados administrativos full time.

El total de espacio destinado a archivar aprox. 54.000 historias en el Hospital Municipal de Oncología María Curie es de 152 m2 , empleando 6 personas. Considerando que en un disco rígido de 300 GB, de muy bajo costo (menos de $1000) entran tres contenedores de papel que podrían almacenar aproximadamente 450.000 historias clínicas, es evidente que la informatización es la solución más económica y eficiente. (9)

La informatización evita también evita la redundancia de estudios y de tratamientos. Muchas veces, al no contar con estudios realizados en consultorios, los mismos se repiten en forma innecesaria en la internación y viceversa.

Por último, no puede dejar de mencionarse el importante impacto ecológico que tiene el ahorro de toneladas de papel disminuyendo la contaminación del medio ambiente (papeleras) y la deforestación.

## Características que Deben Preservarse en la Historia Clínica Electrónica

La historia clínica electrónica debe cumplir con una serie de requisitos para que pueda ser reconocida como una herramienta probatoria válida en los tribunales.

La mayoría de las recomendaciones son adaptaciones a nuestro país de normas de los Estados Unidos y de Europa, principalmente las realizadas por el Comité de Ministros del Consejo de Europa a los Estados Miembros sobre la Protección de Datos Médicos.

El Código de Ética de la Asociación Médica Argentina (AMA) (10) da entidad a la informatización de la documentación médica, mediante el art. 185 del Capítulo 11 (referido a la historia clínica):

*“En caso de computarización de la Historia Clínica deberán implementarse sistemas de seguridad suficientes para asegurar la inalterabilidad de los datos y evitar el accionar de violadores de información reservada.”*

Mediante este artículo, la AMA da por tierra con el arraigado y erróneo concepto de que la historia clínica debe ser indefectiblemente manuscrita, si bien deja en claro que deben cumplirse con ciertos requisitos que son considerados en forma unánime por médicos, especialistas en informática y juristas como indispensables. Estos son (3) (11) (12):

**1.Inviolabilidad**

Que la información no pueda ser adulterada. Una vez ingresados los datos no pueden modificarse (algunos sistemas dan una “ventana” de minutos). Cualquier corrección automáticamente se agrega al final del texto preservando la cita original. Se debe impedir el ingreso no autorizado de datos en el sistema de información. Esto incluye las medidas pertinentes para impedir el ingreso de hackers en el sistema.

**2.Autoría**

El sistema deberá otorgar garantías acerca de la identidad de quien ingresa los datos (asegurar que un usuario particular es quien dice ser). Esto se logra con la firma digital.

**3.Confidencialidad**

Se debe impedir que los datos sean leídos, copiados o retirados por personas no autorizadas. Esto puede conseguirse con normas de accesibilidad controlada que permiten al acceso o lo restringen de acuerdo a la función del usuario. Se establece de esa forma un control sobre la utilización de los distintos campos. No todos pueden tener acceso a toda la información (Ej: un empleado administrativo no puede acceder a los antecedentes patológicos de un paciente). Para ello se utilizan técnicas de encriptación que transforman al texto en "jeroglíficos" para quienes no están autorizados a leer dicha información. Cuando un usuario autorizado necesita acceder a la misma, ingresa su clave y esa historia se reprocesa volviendo a un formato legible. En nuestro país, la Ley de Hábeas Data y la Constitución Nacional obligan a garantizar una adecuada protección de los datos de las personas y del acceso a la información.

**4.Secuencialidad**

El sistema debe garantizar que los datos sean ingresados en forma cronológica, siguiendo el orden en que la historia fue escrita e impidiendo que se altere la secuencia de actualización.

**5.Temporalidad**

Todo registro en la historia clínica debe automáticamente llevar adosado el día y la hora en que se realizó. Esto se consigue mediante la aplicación de un mecanismo de seguridad informático: el sellado digital de fechas (time stamping.)

**6.Disponibilidad**

Debe garantizarse que la información se encuentre disponible en todo momento y lugar cuando se la necesite, aún desde fuera del ámbito institucional (ej: consultorio particular del médico). También debe permitir el acceso, cuando corresponda, de los organismos de control de Salud Pública y de la Justicia.

**7.Integridad**

El sistema debe alertar si el registro fue adulterado a posteriori de la firma. La información volcada en la historia clínica sólo debería poder modificarse de acuerdo a un procedimiento claramente especificado de antemano y sólo por personal autorizado. A su vez, deberá quedar en el sistema un registro de la introducción de los datos (quién ingresó, desde dónde, con qué clave, fecha y hora, qué cambió, que agregó, etc.). De forma tal que si las historias son modificadas ya sea en forma legítima como fraudulenta, quedará un registro.
La integridad de la historia clínica electrónica también depende de adecuados softwares de seguridad informática que protejan a la documentación de posibles virus. Los datos deben salvaguardarse mediante back up regulares y copias de seguridad.

**8.Durabilidad**

La información generada debe permanecer inalterable en el tiempo. Las instituciones deberían poder prevenir o eventualmente recuperar cualquier pérdida de datos en la eventualidad de incendios, inundaciones, vandalismo o fallas del sistema. Se deben establecer normas con respecto a la seguridad física de los equipos. También se deberían actualizar los programas obsoletos según pasan los años a fin de que la documentación archivada pueda mantenerse accesible y útil durante el tiempo que marca la ley.

**9.Transportabilidad e Impresión**

El sistema debe permitir que el paciente pueda disponer de una copia de su historia clínica, ya sea en soporte electrónico o en papel. La información transportada vía mail, CD o pen drive debería ser transmitida en clave y con los mismos requisitos descriptos, impidiendo la modificación, la copia y la lectura de personas no autorizadas.

## Mecanismos de Seguridad Informáticos (MSI)

Habiendo analizado qué requisitos de seguridad deben garantizarse en la historia clínica electrónica (HCE), la siguiente pregunta que debe responderse es cómo hacerlo. Cuanta mayor seguridad tenga el sistema, menos reparos podrán realizarse sobre su valor probatorio en un litigio.

Los mecanismos de seguridad informáticos (MSI) se clasifican en: (3)

| | |
|---|---|
| CLÁSICOS | Nombre de usuario y clave<br>Tarjetas magnéticas combinadas con clave.<br>Técnicas de back-up |
| BIOMÉTRICOS | Huellas dactilares (fingerprint)<br>Estructura de la mano (hand key)<br>Reconocimiento del iris<br>Reconocimiento facial |
| CRIPTOGRÁFICOS | Encriptación<br>Firma Digital<br>Sellado digital de fechas (Time Stamping) |

**MSI Clásicos**

La implementación de nombres de usuario y clave de acceso es el mecanismo de seguridad más básico y el más difundido. También es el más inseguro, ya que depende de pautas culturales que son muchas veces difíciles de cambiar. Si este mecanismo se utiliza mal, no se garantiza la identidad del que genera la información, ya que las claves de acceso pueden pasar de un usuario a otro y no son 100% vinculantes con el usuario. En algunos centros todavía se comparten claves o bien las mismas son obvias. Puede agregarse a este sistema una tarjeta magnética que deba ingresarse junto con la clave, aunque si la misma también es compartida continúa presentando el inconveniente anterior. También se encuentran dentro de este grupo las prácticas de muchas instituciones que realizan el back up regular de su información electrónica (CD/Pendrive) y la entregan a un escribano, de forma tal de brindar una mayor garantía acerca de que la documentación no ha sido alterada.

Sin duda los MSI clásicos tienen la ventaja de su fácil implementación y bajo costo. Estos mecanismos pueden ser efectivos si todos los involucrados en el ingreso de datos toman conciencia de la importancia que tiene no compartir su clave y la modifican periódicamente (la mayoría de los sistemas obligan a hacerlo).
Una de las principales falencias de estos MSI radica en que los "Súper Usuarios" (Administradores del Sistema Informático de la Institución Médica) siempre tienen el control sobre la información generada por los médicos y otros profesionales, pudiendo realizarse cambios.
Hoy los mecanismos de seguridad clásicos no alcanzan para brindar certeza de integridad, autoría y confidencialidad, y deben ser complementados con mecanismos de seguridad biométricos y criptográficos.

**MSI Biométricos**

Estos mecanismos reconocen los parámetros biométricos propios de cada individuo: huellas dactilares, la estructura de la mano, del iris o de la cara. Se dan así mayores garantías acerca de la identidad de la persona que ingresa los datos en la historia clínica. Cualquier persona que ingrese con nuestra clave o tarjeta magnética puede acceder tal como nosotros lo hacemos al sistema, pero no lo hará sin nuestro iris o huella dactilar. Estos mecanismos de seguridad son útiles pero están muy lejos de ser infalibles, por lo que deben considerarse con ciertas reservas. No todos son lo suficientemente sensibles y específicos y se han encontrado formas relativamente sencillas de "hackearlos". Los productos existentes en el mercado son muy variables tanto en el precio (que puede ir desde menos de 100 dólares a varias decenas de miles por dispositivo) como en su sensibilidad y especificidad. Se han descripto mecanismos muy ingeniosos para "hackear" estos sistemas, (ej: empañando con el aliento un lector de huellas dactilares luego de que éste ha sido usado por un usuario permitido). Al igual que los mecanismos de seguridad informática clásicos, los mecanismos biométricos también dependen del control de los Súper Usuarios, por lo cual es necesario asociarlos a técnicas criptográficas para aumentar su grado de confiabilidad.

**MSI Criptográficos**

Una de las formas más efectivas para proteger la información consiste en aplicar técnicas de "encriptamiento" a la información contenida en los archivos. Esta técnica, mediante los denominados "algoritmos", transforma el texto en símbolos ilegibles, impidiendo de esta forma su lectura y su adulteración. Sin embargo, dicho texto "encriptado" se puede recuperar cada vez que sea necesario mediante técnicas de desencriptamiento, que entran en juego cuando ingresa al sistema un usuario autorizado.
La criptografía también debe aplicarse para proteger la información que se envía por correo electrónico. Uno de los programas más confiables y difundidos en todo el mundo es el denominado PGP (Pretty Good Privacy) , desarrollada por Phillip Zimmerman en 1991 como freeware (software gratuito). Utilizado correctamente, el PGP puede proporcionar un gran nivel de seguridad. A diferencia de otros protocolos de seguridad que sólo protegen los datos en tránsito, el PGP también puede utilizarse para proteger datos almacenados en discos, copias de seguridad, etc.

En la firma digital y el sellado digital de fechas está la respuesta a la mayoría de los interrogantes planteados acerca de la validez legal de de la historia clínica electrónica. La Ley vigente 25.506 de Firma Digital es el instrumento jurídico que hace posible que las historias computarizadas no sean cuestionables desde el punto de vista legal. Repasemos algunos artículos:

*Art. 1°. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.*

*Art. 3° Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias por su ausencia.*

*Art 6° Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.*

La firma digital permite garantizar la autoría de un documento, pero para poder dar valor legal a las evoluciones e indicaciones médicas hace falta probar otro elemento indispensable: la hora y fecha en la que se realizaron. La presunción de autoría no garantiza la secuencialidad y la temporalidad que deben tener las evoluciones clínicas. El sellado digital de fecha (time stamping) es el mecanismo de seguridad informático que viene a solucionar este problema, ya que garantiza la determinación del momento exacto en que se generó la información.

## Diferencia entre la Firma Electrónica y la Firma Digital

La misma Ley 25.506 claramente establece las diferencias entre ambos tipos de firmas:

**Firma Digital:**

*Art. 2°. 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 esta 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.*

*Art. 7° Presunción de autoría: Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma*

*Art. 8° Presunción de integridad: Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma*

*Art. 9° Validez: Una firma digital es válida si cumple 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 proceso de verificación correspondiente.*
*c)Que dicho certificado haya sido emitido o reconocido, según el art. 16 de la presente, por un certificador licenciado.*

Como vemos, la firma digital es mucho más que ingresar una clave identificatoria. La firma del profesional debe estar certificada por un certificador licenciado. Los certificadores licenciados son por ahora en su mayoría entes públicos (si bien la ley también permite certificar a entes privados) autorizados por la Oficina Nacional de Tecnologías de la Información (ONTI) para emitir certificados digitales. Un certificado digital no es más que un documento electrónico firmado digitalmente por el certificador licenciado donde consta la Clave Pública y los datos del usuario al que hace referencia.

El proceso consiste básicamente en la generación de dos claves, una Pública y otra Privada, ligadas entre sí matemáticamente mediante la aplicación de algoritmos técnicamente confiables. (13)
**La Clave Pública** es de libre distribución y debe estar en disponibilidad de todo aquel que quiera verificar que la firma digital generada con la clave privada se corresponde con dicha clave pública. Se garantiza así que la firma es de quien dice ser y que lo que firmó no ha sido alterado.
**La Clave Privada** es de conocimiento exclusivo del usuario y debe ser resguardada con el máximo nivel de seguridad para evitar su uso por personas no autorizadas.

De esta forma, el autor del documento electrónico procede a codificarlo (encriptarlo), luego lo remite a su destinatario quien no podrá transformar el documento en legible si no posee la clave pública del remitente. Sólo si posee dicha clave pública el destinatario podrá "decodificar" el mensaje y hacerlo nuevamente legible, ya que sólo la clave pública del transmisor es capaz de decodificar el documento cifrado con la clave privada. Dicho en otras palabras, la clave privada funciona como una llave que cierra el documento que sólo puede ser abierto por otra llave, la clave pública.

Al haber control externo de la firma, este sistema permite escapar al control de los "Super Usuarios"- los responsables de sistemas-, de las distintas Instituciones.

Son todavía muy pocos los profesionales de la salud que han certificado su firma de esta forma ya que las entidades que controlan la matrícula (ej: Colegios Médicos) no se han constituido como certificadores licenciados pudiendo hacerlo, según el artículo 18 de la Ley. Hasta el momento ningún certificador privado se ha acreditado para operar como Certificador Licenciado, por lo cual no es posible para un particular obtener un certificado de firma digital. Esto por el momento está privando a la comunidad médica del vehículo más fácil y accesible para validar su firma informática. Lo concreto es que todavía los médicos y profesionales de la salud no tienen a quien recurrir para para obtener un certificado digital y deben contentarse sólo con la firma electrónica, que también es aceptada por la ley pero que no brinda la seguridad de la firma digital.

Los únicos avances en este sentido provienen de la administración pública, siendo los primeros certificadores licenciados la AFIP y el ANSES (Marzo de 2009). Sin embargo, el proceso de obtención del certificado digital – que no sería demasiado complicado- está limitado a funcionarios y agentes de la administración pública. La misma Autoridad Certificante de la Oficina Nacional de Tecnologías de la Información (ONTI) emite certificados de identificación personal en forma gratuita, si bien los mismos también están limitados a empleados estatales y, en el caso del resto de los ciudadanos a la protección de las comunicaciones por correo electrónico, no validando la identidad de la persona sino tan sólo verificando la existencia y disponibilidad de dicha cuenta. Se puede encontrar mucha información al respecto ingresando en la página oficial de la Autoridad Certificante de ONTI: www.ca.pki.gov.ar

En todos los casos, para obtener un certificado digital se deberá comprobar la identidad, bien directamente o por medio de entidades colaboradoras. Recién ahí el certificador licenciado creará con los dispositivos técnicos adecuados el par de claves pública y privada y generará el certificado digital correspondiente a esas claves, entregándole al profesional el certificado, ya sea en un medio magnético o directamente en formato de archivo.

**Firma Electrónica**

Si alguno de los requisitos legales descriptos no se cumple (por ejemplo, no se dispone del certificado digital emitido por un certificador), la ley contempla la figura de la firma electrónica, a la que define en su artículo 5° como "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 algunos 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." Se invierte así la carga de la prueba, siendo el profesional de la salud quien debe demostrar su autenticidad en caso de cuestionamientos (a diferencia de la firma digital).

Como ejemplos de firma electrónica pueden ser considerados los siguientes:

- Una firma hecha con un certificado que no haya sido emitido por una Autoridad Certificante licenciada
- Un password o un número de pin utilizados como autenticación
- La identificación a través de algún procedimiento biométrico
- Un tono o pulso telefónico

Habiendo hecho la distinción entre ambos tipos de firmas, queda claro que la inmensa mayoría de los profesionales de la salud en la actualidad están utilizando la firma electrónica y no la digital. Esto seguirá ocurriendo mientras no haya mayores opciones de certificadores privados que faciliten el trámite a los médicos y otros profesionales de la salud.

## Exclusiones a la Documentación Electrónica: El Consentimiento Informado

El art. 4. de la Ley de Firma Digital establece determinadas exclusiones, entre las cuales se menciona expresamente a los actos personalísimos. Por lo tanto, existen determinados actos que no pueden ser llevados en registros informatizados, tales como la información de riesgos y aceptación del paciente para la realización de estudios y tratamientos (consentimiento informado). Estos actos entran en la esfera de los derechos personalísimos (el derecho a estar informado posibilita el derecho personalísimo a su integridad psicofísica, el derecho de disponer de su propio cuerpo, de decidir su vida, el derecho a una muerte digna, etc.).

De igual forma se legisla en materia de transplantes, que por involucrar actos de tanta trascendencia como son la ablación de un órgano o la realización de un transplante, la Ley 24.193 (De transplante de órganos y tejidos) ha impuesto requisitos muy concretos en cuanto al contenido de la información, quedando por ende también incluidos dentro de la prohibición del art. 4 de la Ley de firma digital.

En todos estos casos (consentimientos informados, directivas anticipadas y transplantes), la declaración de voluntad del paciente debe seguir siendo registrada en la historia clínica u otros registros con las formalidades que imponen las distintas reglamentaciones y la jurisprudencia: firma manuscrita del profesional, aclaración y número de matrícula y fecha. La inobservancia de tales requisitos torna nulo el acto, acarreando las consecuencias jurídicas propias que de ello se derivan (imposibilidad probatoria y responsabilidad objetiva por falta de información). (2)

## Problemas a Resolver

Actualmente la mayoría de la información asistencial en las clínicas, sanatorios y hospitales no se encuentra computarizada. La informatización del sector salud se encuentra retrasada, particularmente entre los prestadores.

Las dudas acerca de la validez legal de documentos informáticos con escasos mecanismos de seguridad y algunas dificultades operativas determinan que en el sector salud, a diferencia de otras industrias donde la nueva tecnología reemplaza a la anterior, la informática conviva con el papel. En la actualidad, los profesionales del equipo de salud escriben más, generan más órdenes de estudios y deben justificar sus pedidos ante los financiadores en papel, reproduciendo en forma geométrica la producción de documentos en este soporte, que a su vez son fotocopiados y faxeados en numerosas oportunidades, con la amenaza a la confidencialidad que esto significa

Se requiere entonces no sólo invertir en equipamiento y desarrollo de software sino también producir un cambio de hábito entre los profesionales que permita pasar de la cultura del papel a la cultura informática. Para ello es necesario involucrar a los médicos y auxiliares en el desarrollo de este proceso.

Uno de los principales problemas a resolver para que el profesional se sienta más cómodo con la utilización de la historia clínica electrónica es la atomización de la información entre los distintos actores que intervienen en la atención de un paciente. En los sistemas electrónicos actuales, la información sobre la cual el médico toma una decisión se encuentra repartida en diferentes registros computarizados (información del laboratorio, informes de estudios complementarios, registros de enfermería, interconsultas, etc). Es imposible firmar información atomizada de un mismo paciente en distintas tablas, bases de datos y registros, por lo que habría que correr un procedimiento para centralizar en un único registro toda la información que se desea firmar. (3)

## Conclusiones

- En toda institución médica la historia clínica es el archivo más importante, conteniendo información vital para la gestión médica, administrativa y legal. Las ventajas comparativas de la informática frente al papel son innumerables desde todo punto de vista (operativo, de seguridad, económico y aún ecológico).

- No existe ningún imperativo legal que priorice la validez de la firma manuscrita por sobre la firma electrónica o digital, salvo cuando se trata de actos personalísimos como el consentimiento informado, las directivas anticipadas o los transplantes.

- Si bien hay quienes abogan por una nueva ley que regule en forma concreta y específica todo lo referente a la historia clínica electrónica, la legislación vigente (Ley de Firma Digital) y el desarrollo actual de los mecanismos de seguridad informáticos descriptos (principalmente la criptografía, el sellado digital de fechas y el control de la modificación de campos) son suficientes desde el punto de vista legal para que los registros médicos informatizados tengan el mismo valor probatorio que sus homólogos en papel.

- Resulta necesario avanzar en el cambio cultural que permita una correcta implementación de la solución. Todo cambio crea dudas e inseguridad ante lo desconocido, por ello es que se debe trabajar en forma conjunta entre profesionales de la salud, en informática y en derecho para brindar todas las garantías necesarias a los usuarios del sistema.

- Por último, se necesitan certificadores licenciados vinculados al sector salud, para difundir y facilitar la certificación de la firma por parte de los profesionales de la salud. Sólo así se podrá pasar de la firma electrónica (modalidad mayormente utilizada en la actualidad) a la firma digital, de forma tal de dar mayor seguridad a la autoría de los documentos.

**Bibliografía:**


1.Ley 25.506 de Firma Digital. Sancionada:14 de Noviembre de 2001. Promulgada de Hecho: 11 de diciembre de 2001. Accedido: www.infoleg.mecon.gov.ar

2.Weingarten, Celia. Informatización y firma digital: Historia Clínica. LA LEY 2005-A.1072

3.Mandirola Brieux HF, Guerra J, Guillén S, Laguzzi P. La firma digital y la historia clínica web enabled. GIBBA & BIOCOM. The Biocomputer Research Group of Argentina- Sociedad Argentina de Informática y Salud. www.sais.gov.ar Accedido 20 de julio 2009.

4.Vítolo F. Historia clínica electrónica. El Monitor. Nov. 1999. St.Paul Argenina Compañía de Seguros

5.Hurvitz M, Lobato C, Pezzella M, Piñero G. Historia Clínica Electrónica. La historia que apenas comienza. Rev. Asoc. Coloproct. Del Sur. Vol 3 N° 4. 2008

6.Parente Aun RA, Mercau JP, Atienza OA. Estudio comparativo entre historia clínica informática e historia clínica en papel. Acta Científica Estudiantil 2006; 4(1): 23-27. Facultad de Ciencias Médicas de la Universidad Nacional de Córdoba.

7.Biocom. Expediente Clínico informatizado. www.biocom.com.ar/sistemas/historias_clinicas/historia_clinica_informatica.html. Accedido el 10 de julio de 2009

8.Mariona F, Chouela E, Rébora R. y col. Derecho Médico: Historia Clínica Manuscrita e Historia Clínica Informatizada. Medios de Prueba Válidos en Sede Judicial. Revista de la Asociación Médica Argentina (AMA). Vol III N°2 1998

9.Baca L, Filgueira E, Hallar L, Landini P, Ratto V, Tealdo M. La historia clínica informatizada. Boletín Científico de la Asociación de Médicos Municipales de la Ciudad de Bs.As. Año 11. N°51-Septiembre 2006

10.Asociación Médica Argentina (AMA). Código de Ética www.ama-med.org.ar/codigoetica.asp

11.Zotto Rodolfo S. Historia Clínica Informática. Revista Persona.

12.Do Pico JC, Do Pico Mai CL, Hutin RA. La historia clínica informatizada. Apreciaciones sobre su viabilidad. Revista de la Asociación Médica Argentina (AMA). 112 (2): 1999

13. Biocom. La firma digital de documentos médicos informatizados. www.biocom.com.ar/informatica_medica/legalrec_firma_digital.html Accedido 10/7/2009