LA FIRMA DIGITAL Y LA HISTORIA CLINICA WEB ENABLED

Dr. Humberto Fernán Mandirola Brieux, Lic. Jorge Guerra, Lic. Sebastián Guillen , Lic. Pablo Laguzzi

GIBBA & BIOCOM The Biocomputer Reasearch Group of Argentina

Resumen

La firma digital FD es un elemento indiscutiblemente necesario para la HCC en Internet, por varias razones que tienen que ver con el aspecto legal y la accesibilidad controlada de los datos clínicos.

La misma herramienta tecnológica que se utiliza para Firmar Digitalmente, permite mediante la encriptación de los datos proteger la información medica asegurándose la privacidad de los datos de los pacientes y que los mismos solo sean leídos por las personas autorizadas.

Tal como se estructura la información de la HCC en las bases relacionales no es posible firmarla, por lo cual hay que pasar por un paso intermedio de depuración de toda la información que debe firmase. También es importa guardar la información de quienes están autorizados a ver la información y garantizar la accesibilidad y transportabilidad de los datos del verdadero dueño de la información que es el paciente.

La Tecnología de los mecanismos de encriptación y la Ley de Firma Digital, son los elementos técnicos y jurídicos que hacen posible que la historia clínica computarizada no sea cuestionable desde el punto de vista legal. No es necesario esperar una Ley que regule las historias Clínicas computarizadas para que estas tengan valor legal.

Summary

The digital sign (FD) is an unquestionably necessary element for the Medical records(HCC) in Internet, for several reasons that they have to do with the legal aspect and the accessibility controlled of the clinical information

The same technological tool that is in use To sign Digitalmente, it allows by means of the encriptación of the information to protect the information medicates insuring itself the privacy of the information of the patients and that the same ones only should be read by the authorized persons.

As the information is constructed of it HCC in the relational bases is not possible to sign it, thus is necessary to happen through an intermediate step of shaving of all the information that must signed.
Also is matters to keep the information from those who are authorized to see the information and to guarantee the accessibility of the data of the true owner of the information that is the patient.

The Technology of the encystations mechanisms and the Law Digital Company, they are the technical and legal elements that make possible that computerized clinical history is not questionable from the legal point of view. It is not necessary to wait for a Law that regulates computerized Clinical histories so that these have legal value.

Palabras Clave

Protección de datos, Firma Digital Historia Clínica Computarizada, Firma Electrónica, Expediente Clínico informatizado, Registros Médicos informatizados, Evolución Clínica, Modelo de Datos

Introducción.

Indagando en el tema, encontramos pocas pero claras referencias legislativas en la Argentina conexas al tema de la información médica, muy difundidas, aunque no muy bien conocidas y un tanto mitificadas. Básicamente tienen que ver con el secreto médico y la prescripción de medicamentos.

No existe una legislación que indique la forma en que el médico deba registrar la información de sus pacientes hasta fines del siglo XX.

Aunque este hecho cambia a partir del 2000, como veremos más adelante, todos los que alguna vez historiamos sobre el tema nos encontramos con la sensación de un vacío legal. Consultando gente del Derecho, nos enteramos sorpresivamente que este hecho, lejos de ser un problema, es una ventaja porque cuando sobre un tema hay mucho legislado la cuestión muchas veces es insalvable o, por lo menos, muy difícil hasta para los juristas más avezados.

Como contrapartida podemos citar no pocos casos jurisprudenciales en donde la justicia falla en contra de los facultativos en los casos en donde hay ausencia de registración de la información; en esos casos, se considera que "si no está escrito es porque no se hizo", sin embargo, actualmente contamos con medios informáticos con fuerza legal para poder garantizar la legitimidad de la información.

¿Porque es necesario firmar digitalmente la HCC?

Básicamente por dos aspectos:

1. Para poder reconocer quien generó la información y cuando.
2. Para proteger los datos personales y cumplir con:
    a. La **"ley de habeas data"** (Ley Nro. 25.326 y su decreto reglamentario 1558/2001), garantiza un nivel adecuado de protección de acuerdo a la directiva comunitaria en la materia.
    b. Como con la Constitución Nacional (Art. Nº 43): Protección de datos de las personas y acceso a la información.

Es indiscutible que la HCC tiene que ser firmada digitalmente, tanto por los aspectos legales que tienen que ver con el valor probatorio de la información, como con el Habeas data. El tema es como hacerlo.

La historia clínica esta conformada por información provista por distintos actores, cada uno de los cuales tiene que ser responsable de la información que genera, las decisiones que toma él medico están realizada sobre la base de lo que él medico per se recoge del examen físico de sus pacientes y de la información que proveen otros profesionales como los bioquímicos, radiólogos, otros colegas que realizan practicas y estudios, enfermeros y farmacéuticos entre otras fuentes de información para realizar el acto medico de la consulta. En nuestra opinión todos los actores que generen información en la historia clínica computarizada deben firmar digitalmente.

Si bien el medico es el responsable final, también es importante que se consigne adecuadamente la información en la cual se basa su actividad. El modelo que presentamos en este estudio, arma la información de manera tal que incluya:

- la que el medico tuvo en cuenta,
- sus propias observaciones y acciones

El registro resultante es el que se debe firmar digitalmente.

Características que debe cumplir la HCC:

- **Inviolabilidad**: que la información no pueda ser adulterada.
- **Autoría:** que toda evolución pueda ser atribuible al autor (No Repudio). Esto se logra con la Firma Digital.
- **Confidencialidad:** que no se pueda difundir libremente (Habeas Data). Esto se logra con políticas de accesibilidad controlada (la Firma Digital, también se puede utilizar para controlar como control de acceso) y con la utilización de criptografía.
- **Secuencialidad:** Asegurarse que los datos sean ingresados en forma cronológica.
- **Disponibilidad:** que la información este disponible para cuando se la necesite y pueda ser accedida desde cualquier lugar fuera del ámbito institucional (consultorio particular del médico).
- **Integridad:** que se pueda alertar si el registro fue adulterado a posteriori de su firma. La herramienta de Firma Digital mediante la utilización de la Clave Pública del firmante, permite corroborar esta situación.
- **Temporalidad**: que todo registro en la HCC, lleve adosado el día y la hora en que se realizó.
- **Durabilidad:** que la información se pueda mantener en el tiempo.

¿Quién es el verdadero dueño de la historia clínica?

Muchos médicos piensan que los pacientes no tienen que acceder a los datos de la Historia Clínica "para protección de los propios pacientes", esto no tiene mucho sustento, tanto desde el punto de vista moral como legal. Actualmente la ley de la mayoría de los países del mundo considera que el verdadero dueño de la información es el paciente y este tiene que tener garantizado el acceso a los datos por los motivos que fuera, quedan solo la institución prestadora de servicios con la guarda de los mismos y a cargo de la seguridad de la información.

Existe una gran diferencia en firmar digitalmente un mail o un documento de Word a datos de una evolución clínica.

La información médica en la historia clínica computarizada (HCC) suele estar atomizada en registros de varias tablas, en estructura de datos relacionales. A su ves esos datos pueden ser alterados por distintos procesos, por lo tanto se impone utilizar 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 hay que contemplar un campo en donde guardar el hash del registro firmado

Elementos del Trabajo y metodología.

Nuestro Objetivo es presentar un modelo de datos que permita firmar digitalmente lo que el medico observó, pensó y actuó en un momento dato, para proteger y hacer que los Registros Médicos Informatizados (RMI), tengan valor legal. Se incluyen dentro de los RMI a todos los archivos informáticos que tengan alguna información relativa al paciente, sus estudios complementarios y su tratamiento:

Historia Clínica Computarizada (HCC)
Registros de admisión y egresos
Archivos de laboratorio de análisis clínicos
Bases de estudios complementarios (Rayos, Tomografías, Ecografías y otros)
Archivos de reserva de turnos
Archivos de facturación y otros

Tabla:1

La HCC, documento principal que registra el acto médico en sí, es el que más debe estar protegido. Sin embargo, todos deben tener restricciones y reservas, dado que contienen información que puede perjudicar a los pacientes en caso de difundirse.

Características que deben preservarse:

Además de las indiscutibles y fundamentales características, como idoneidad, veracidad y legilibilidad,(*27) que dependen del usuario que genera la información exclusivamente e igual que su homóloga en papel, se deben tener en cuenta los conceptos del Código de Etica de la AMA (Asociación Médica Argentina) con respecto a la Historia Clínica.
La HCC es un documento privado que, además de servir técnicamente al acto médico, tiene fines administrativos, estadísticos y legales (derechos y obligaciones de los pacientes, profesionales e instituciones involucradas en el acto médico) que deben poder garantizar por sí mismos los principios de:

Inviolabilidad:	Que la información no pueda ser adulterada
Autoría:	Identificación del responsable que la generó .
Reserva: “Confidencialidad”:	No puede difundirse libremente, tiene que tener control de quienes tienen acceso.
Secuencialidad	Debe seguir el orden en que fue escrita.
Disponibilidad:	Debe garantizar la posibilidad de consulta cuando el paciente y los profesionales lo necesiten en tiempo y forma.
Integridad: “Total y Completa”:	Los que están justificadamente habilitados deben poder acceder a toda la información que se requiera para el acto médico, así como para la auditoria, estadísticas, epidemiología, planes de prevención y peritajes legales.
Temporalidad precisa:	Fecha y hora en que se generó.
Durabilidad	Debe permanecer inalterable en el tiempo para que su información pueda ser consultada.

Tabla:2

Mecanismos de Seguridad Informáticos (MSI).

Siempre hay que considerar que el ingenio existe en todos los sentidos, tanto para el bien como para el mal, y que así como mucha gente piensa inteligentemente cómo se pueden proteger las cosas, otros, con mucho ingenio, se dedican a ver como violarlas.
Fundamentalmente para los Médicos que no están acostumbrados a pensar en ambos sentidos, es importante recalcar que siempre que hablamos de Conflictos, Seguridad, Legalidad, es necesario cumplir también el papel de abogado del diablo para probar realmente la confianza de lo que estamos postulando.

Los dividimos en:

CLASICOS	Nombre de Usuario y Clave
	Tarjetas magneticas combinadas con clave
	Técnicas de back-up
BIOMÉTRICOS	fingerprint
	hand key
	Reconocimiento del iris
	Reconocimiento Facial
CRIPTOGRAFRICOS	Firma Digital
	Mecanismos de encriptación
	Time-stamping

Tabla:3

MSI CLÁSICOS.

Estos comprenden:

- los nombres de usuarios con clave de acceso,
- las tarjetas magnéticas combinadas con claves,
- las técnicas de back-up y depósito del histórico de la información (depósito de la información en escribanias).

Desde los comienzos de la informática la implementación de nombres de usuarios y claves de acceso constituyen elementos corrientes. Sin embargo la efectividad de los mismos es relativa dependiendo de pautas culturales de los lugares en donde se implemente más que del mecanismo informático en sÍ.
Existen no pocas instituciones en donde las claves son las mismas para todos los usuarios o donde las claves son obvias. Siempre hay formas de optimizar este mecanismo de protección clásico de la información que, no por viejo, deja de tener un grado aceptable de seguridad de acceso a la información si es bien utilizado.
Además de servir como elemento de control de las actividades de un usuario dentro del sistema, los MSI CLÁSICOS presentan las siguientes ventajas:

- Fácil implementación y bajo costo.
- Son relativamente seguros si son bien implementados y utilizados.

Con respecto a las desventajas:

- Pautas culturales negligentes de usuarios para uso de claves de acceso.

- Los ¨Super Usuarios¨ (administradores de sistema): Siempre tienen el control sobre la administración y la información generada por estos usuarios de más bajo nivel.
- No garantizan la identidad (sobre todo si se utilizan mal) del que genera la información, ya que las claves de acceso se pueden pasar de un usuario a otro y no son 100 % vinculantes con el Usuario.

Optimización de los mecanismos de seguridad clásicos

- Obligar a los usuarios a cambiar la clave en forma periódica
- Tercerizar la administración de la seguridad informática
- Usar técnicas criptográficas para el almacenamiento de claves y nombres de usuarios.
- Registrar en una bitácora la actividad de los usuarios.
- Registrar los usuarios de alta de datos con fecha y hora y los usuarios que modifican datos con fecha y hora.

MSI BIOMÉTRICOS.

Estos mecanismos básicamente reconocen estructuras corporales que son propias de cada individuo, como las huellas dactilares (fingerprint), la estructura de la mano (hand key), la del iris o la de la cara (*38). Es decir, que recogen información biométrica propia de cada ser, elementos que en cierta manera garantizan la identidad de la persona. A diferencia de una tarjeta magnética o clave pueden ser utilizadas por cualquiera que la conozca. 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. Los productos existentes en el mercado son variados, su grado de confiabilidad también es muy diverso así como su costo que va desde los 50 a los 50.000 dólares por dispositivo. El Ing. Juan Franchino (*41) dio varios ejemplos de cómo se pueden hackear estos elementos de manera ingeniosa y pavorosamente sencilla, por ejemplo, empañando con el aliento un lector de huellas dactilares luego de que éste ha sido usado por un usuario permitido; es factible confundir a algunos censores ingresando luego al sistema. En honor a la verdad hay que decir que hay distintos dispositivos lectores de huellas dactilares, los mas sencillos funcionan reconociendo la imagen en forma bidireccional tal cual como funciona un scanner, pero los hay tridimensionales capaces de detectar diferencias en la profundidad de los surcos dactilares, los cuales no podrían ser engañados tan fácilmente. El hecho es que no se puede confiar ciegamente en nada y menos en un dispositivo. Es necesario elegir los mismos de acuerdo a su sensibilidad y especificidad para cada tipo de acceso. Sin embargo creemos que son elementos útiles pero que están lejos de ser infalibles, por lo cual hay que considerarlos con ciertas reservas.
Al igual que los MSI CLÁSICOS, los BIOMÉTRICOS dependen también del control de los Super Usuarios, por lo cual es necesario asociarlos a técnicas criptográficas para aumentar su grado de confiabilidad.

MSI CRIPTOGRAFRICOS.

Hay antecedentes del uso de la criptografía aún antes de la era cristiana, así que referirse a los mismos no es haber inventado la pólvora. Durantes las guerras, los mensajes cifrados por clave eran y son aún algo común desde hace siglos.
En los MSI CRIPTOGRAFICOS está la solución a nuestro problema 'EL VALOR LEGAL DE LA HCC'. Mas aún, en la Argentina existe la ley 25.506 sancionada el 14

de diciembre del 2001 (*28) que reconoce el empleo de la firma electrónica y de la FD y su eficacia jurídica; el artículo 3 de la misma dice que ¨
Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una FD. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias por su ausencia ¨.

La FD es mucho más que la firma convencional desde el punto de vista de garantía de la identidad e inviolabilidad del documento que se firma electrónicamente. El problema de la Autoría y la inviolabilidad están resueltos desde el punto de vista legal si los RMI utilizan estos mecanismos. Pero no resuelve por sí sola todo el problema relativo a la protección y legalidad de los documentos médicos, ya que si bien tiene la presunción de autoría no garantiza la secuencialidad y la temporalidad que deben tener las evoluciones clínicas.

SINERGISMO DE LA COMBINACIÓN DE MSI.

Así como la racional combinación de antibióticos mejora la eficacia del tratamiento de infecciones complejas, la unión de distintos MSI, mejora el grado de seguridad y disminuye sustancialmente el riesgo de hackeo. Debe evaluarse siempre el costo beneficio de la implementación de varios MSI en relación al volumen de datos y calidad de la información que se debe proteger.

Los Servicios de TS (Time-stamping o sellado digital de fechas) y utilidades de base de datos de campos auto numéricos combinados con técnicas de MSI, resuelven el problema de la secuencialidad de las evoluciones y la temporalidad de las mismas. Debe considerarse la Imposibilidad de acceder a la base de datos en forma directa y el Control de actividades de los Usuarios en el sistema.
Las técnicas de replicación o duplicación de la información, combinadas con esquemas seguros de backup y seguridad física de la información, deben considerarse en la implementación de sistemas médicos.

Combinación de la FD con el TS.

Utilizamos estos elementos combinados con dos objetivos:

1. Probar la autoría de quién generó la información evitando que ésta sea adulterada.
2. Determinar cuando se generó esa información

El primer objetivo esta cubierto por la FD. Para el segundo objetivo es necesario el TS.

La tecnología de FD nos permite asegurar la autoría de un documento. Pero para poder dar valor legal a las transacciones hace falta probar otro elemento indispensable que es el tiempo en que se generó. Incluso, el uso de la FD, sin un servicio confiable de TS, se presta a fraude: Si alguien firma un documento y luego revoca su certificado, podría luego negar la autoría de la firma diciendo que el hecho se produjo con posterioridad a su revocación. Por otra parte, una de las causas de la caducidad de los certificados es la posibilidad de que el avance tecnológico haga posible la rotura de la clave. Por tanto, se podrían en el futuro generar transacciones a nombre de ese certificado vencido afirmando que se produjeron con anterioridad.

Si se analizan los tiempos de duración de los certificados que se emiten actualmente se puede ver que los mismos no suelen superar los dos o tres años. ¿Pero qué hacer para

dar validez a los documentos, como la HCC, que se desea sean válidos por cinco, diez o aún más años con certificados que solo valen dos o tres? Algunos ingenuamente hablan de que se podría re-firmar cada tanto los documentos. La solución de todos esos casos es un TS que asegure en qué momento se efectuó cada transacción.

Problemas a resolver:

1. Atomización de la información
2. Recopilar la información en un sólo registro firmable.
3. Guardar el hash. generado por la clave privada.
4. Control de acceso a la lectura de los datos firmados.
5. Disponibilidad de la información tanto para los facultativos que la necesitan para la atención como para el paciente el cual según la ley es el verdadero dueño de la información.

1. Atomización de la información:
   Como dijimos anteriormente la información sobre la cual toma el medico la decisión esta atomizada en distintos registros (información del laboratorio de análisis clínicos, informes de los estudios complementarios, informes de enfermería, consultas de otros colegas), otro tanto con la que registra, por lo tanto hay que correr un procedimiento para unificar toda esta en un registro.
2. Recopilar la información en un solo registro firmable:
   es imposible firmar información atomizada de un mismo paciente atomizada en distintas tablas, bases de datos y registros, por lo tanto hay que correr un procedimiento para centralizar en un único registro toda la información que se desea firmar.
3. Guardar el hash. Generado por la clave privada.
   Es necesario crear una tabla en donde se almacenen la información que se firma, quien la genera, quienes están autorizados a leerla de quien es esa información en que momento se genero.

Resultados.

La **Ley Firma Digital**, es el elementos técnicos y jurídicos que hace posible que la historia clínica computarizada no sea cuestionable desde el punto de vista legal. No es necesario esperar una Ley que regule las historias Clínicas computarizadas para que estas tengan valor legal.

Deben considerar los MSI, particularmente la FD, en sus desarrollos de los sistemas informáticos de historias clínicas computarizadas para que estos tengan valor legal.

Discusión.

Este modelo de datos pretende aportar una solución a la atomización de datos que existe en la HCC (en las tablas relacionales), encontrándose los datos que el medico tiene que evaluar, los que tiene que consigar en distintos registros de distintas tablas...
Por lo tanto antes de firmar se impone un procedimiento previo para poder juntar y hacer la integración de datos en un registro Firmable.
Para lograr esto se crea una tabla Clínica hash, en la cual se encuentran los datos necesarios para garantizar la firma del documento, su recuperación y lectura.

La evolución del conocimiento es constante, por lo cual también la revisión y actualización continua de las cosas que están vigentes hoy en día es una necesidad. No

hay tema que se agote en la actualidad y un aporte significativo de este grupo de instituciones sería auspiciar y realizar actividades académicas en congresos facultades y sociedades sobre grupos de trabajo y cursos sobre RMI y MSI, tal como actualmente lo hacen sobre importantísimos temas como Mensajería HL7, codificación de enfermedades o leguaje médico unificado.

No es necesario esperar una Ley de HCC, ya que con la Ley de FD más el TS y lo que actualmente existe en MSI es suficiente desde el punto de vista legal para que los RMI tengan valor probatorio de la información que contienen tal que sus homólogos en papel. Igualmente una Ley Nacional que regule los RMI sería de gran importancia, sin embargo consideramos que hay elementos prioritarios que recomendamos tener en cuenta a continuación.

Agradecimientos
Esta Trabajo está dedicado a la memoria de quienes en innumerables oportunidades han hecho importantes aportes a la informática médica y se han referido a este tema: los Dres Daniel Jares (*1), (*30) , (*36) y Domingo Antonio Lago (*2), (*37).
Queremos agradecer a todos los profesionales "raras avis" Argentinos y Extranjeros, mujeres y hombres, provenientes de distintas áreas, cuya lista, gracias a Dios, cada vez es más extensa. Se los puede encontrar en forma independiente o convocados por grupos con caprichosas siglas como SIS, SIB, FIM, OPS, RAN, Lista SALUD, HL7, SADIO, GIBBA, IMIA, AMIA, AAIM, ADIERA, USAL, UBA y otros..... Ellos hicieron y hacen importantes aportes, la mayoría de las veces "Ad-Honorem", que suelen encontrarse en ámbitos académicos, en listas de discusión de Internet y en la web.

Nomenclatura utilizada.
MSI: MECANISMOS DE SEGURIDAD DE INFORMATICOS
RMI: REGISTROS MEDICOS INFORMATIZADOS
HCC: HISTORIA CLINICA COMPUTARIZADA
FD: FIRMA DIGITAL
TS: TIME STAMPING (SELLADO DIGITAL DE FECHAS)

Referencias.
[1] http://www.healthig.com/informatica/informatica6.html
[2] http://www.informaticamedica.org.ar/numero4/in_memoria.htm
[3] MEDICINA LEGAL EMILIO FEDERICO PABLO BONNET LOPEZ LIBREROS EDITORES CUARTA EDICION
[4] CODIGO DE ETICA MEDICA
[5] REVISTA DE LA CONFEDERACION MEDICA DE LA REPUBLICA ARG 965 N 72 PAG 14-30
[6] DERECHO PENAL ARGENTINO SEBASTIAN SOLER 1973 TOMO IV PAG 535
[7] INSURANCE IDENTIFICATION CARD--PRIVILEGE OF LEGAL HEALTH INSURANCE? SCHAEFER OP VERSICHERUNGSMEDIZIN (GERMANY) AUG 1 1992 44 (4) P105
[8] AUTOMATED PATIENT CARE SYSTEMS: THE ETHICAL IMPACT.
FAAOSO N NURS MANAGE (UNITED STATES) JUL 1992 23 (7) P46-8
[9] MANAGEMENT OF PERSONAL HEALTH EXAMINATION DATA FOR A POPULATION BY USE OF A PORTABLE COMPUTER
[10] KAWADA T; AOKI S; SUZUKI S DEPARTMENT OF PUBLIC HEALTH, GUNMA UNIVERSITY SCHOOL OF MEDICINE.
NIPPON KOSHU EISEI ZASSHI (JAPAN) FEB 1992 39 (2) P105
[11] VALOR LEGAL DE LOS REGISTROS INFORMATIZADOS DR. SERGIO STEIMBERG LATINMED VOL01 Nº5 ABRIL DE 1994 15-19
[12] DATA SECURITY IN MEDICAL INFORMATION SYSTEMS: TECHNICAL ASPECTS OF A PROPOSED LEGISLATION.
GRITZALIS D; KATSIKAS S; KEKLIKOGLOU J; TOMARAS A
[13] TECHNOLOGICAL EDUCATIONAL INSTITUTE OF ATHENS, DEPARTMENT OF INFORMATICS, EGALEO, GREECE. MED INF (LOND) (ENGLAND) OCT-DEC 1991 16 (4) P371-83
[14] ACCESS TO HEALTH RECORDS [LETTER] MCLAREN P BR J PSYCHIATRY (ENGLAND) OCT 1991 159 P590-1

[15] LEGAL ASPECTS OF THE USE OF THE COMPUTER IN A HOSPITAL DEPARTMENT EINIGE JURISTISCHE ASPEKTE DER NUTZUNG DES COMPUTERS IN EINER KRANKENHAUSABTEILUNG.
POLAK L; STENCL J; POLAKOVA M
ACTA MED LEG SOC (LIEGE) (BELGIUM) 1986 36 (2) P83-5
[16] VALIDEZ JURIDICA DE LAS HISTORIAS CLINICAS EN MEDIO DIGITAL Ing. Mariano Poli, Master en Ingeniería Biomédica - Dr. Claudio Zurlo, Master en Ingeniería Biomédica
[17] Recomendación n. R (97) 5, del 13.02.97, del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre Protección de Datos Médicos
[18] VETERINARY MEDICAL RECORDS--SOME LEGAL CONSIDERATIONS. HANNAH HW AGRICULTURAL AND VETERINARY MEDICAL LAW, UNIVERSITY OF ILLINOIS, URBANA. J AM VET MED ASSOC JAN 1 1991 198 (1) P67-9
[19] HOMES DOUBT THEY CAN COMPUTERIZE PER HCFA'S REQUEST. EUBANKS P HOSPITALS DEC 5 1990 64 (23) P56
[20] CODIGO PENAL DE LA NACION ARGENTINA
[21] CODIGO CIVIL DE LA NACION ARGENTINA
[22] LEY numero 153 del Gobierno de la Ciudad de Bs As
[23] Criado del Río Mª T; Seoane Prado J. Aspectos médicolegales de la historia clínica, Madrid, 1999.
[24] Aulló Chaves M; Pelayo Pardos S. Responsabilidad legal profesional: la historia clínica. Madrid, 1997.
[25] Ley General de Sanidad LOPD / RD 994/1999 de 11 de junio
[26] Codi de Deontologia: Normes d'ètica mèdica. Consell de Col.legi de Metges de Catalunya, 1997.
[27] DECRETO N° 208/2001"Reglamentación de la Ley Básica de Salud (Ley N° 154/99, DE LA C.B.A.)
[28] Ley 25.506 Sancionada: Noviembre 14 de 2001. Promulgada de Hecho: Diciembre 11 de 2001 por El Senado y Cámara de Diputados de la Nación Argentina http://www.certificadodigital.com.ar
[29] http://www.pki.gov.ar/PKIdocs/ley25506.pdf
[30] Revista INFORMATICA MEDICA º 5 http://www.informaticamedica.org.ar/numero5/art3.htm
[31] http://www.signelec.com/content/se/argentine_resolution_45_97_html
[32] http://www.mediotec.com.ar
[33] http://www.biocom.com
[34] http://www.salvador.edu.ar/ui2-35-franchino.pps
[35] http://www.austral.edu.ar/web/biomedica
[36] http://www.medcenter.com.ar/vol_5/hccompu.asp Historias Clínicas Computadas Su utilización y validez legal Dr. Daniel Jares. Esc. Daniel Paulucci.
[37] http://www.informaticamedica.org.ar/numero9/instituciones2.htm
[38] http://www.tekhnosur.com/pdf/Hand.pdf Tekhnosur S.A.Contacto: Lic. Claudio A. Rivero
[39] http://www.tekhnosur.com/es/nosotros/nosotros.htm
[40] http://www.delitosinformaticos.com
[41] http://www.mediotec.com.ar/formdl.php/of_sin_papeles.ppt
[42] http://csrc.nist.gov/CryptoToolkit/tkhash.html
[43] http://www.acis.org.co
[44] http://sistemas.ing.ula.ve/ed/tablasHash.html
[45] http://delitosinformaticos.com/legislacion/argentina.shtml ANTEPROYECTO DE LEY DE DELITOS INFORMATICOS SOMETIDO A CONSULTA PUBLICA POR LA SECRETARIA DE COMUNICACIONES POR RESOLUCIÓN No. 476/2001 DEL 21.11.2001

Datos de Contacto:

Humberto Fernán Mandirola Brieux BIOCOM Amenabar 1645 Buenos Aires Argentina CP C1426 AKE
Email hmandirola@biocom.com

Jorge Armando Guerra Management en Salud Buenos Aires Argentina, www.jorgeguerra.com.ar

Grupo de Informática Biomedica de Buenos Aires (GIBBA): www.gibba.org.ar