ISSN 1666-5767

Informátic@ Médica

Informatic@Medica Año 3 - N° 10 - Marzo 2002 - FUNDAMEC, Comisión de Informática Médica de AMA y GIBBA

Implicaciones Eticas y Socioeconómicas
de las Historias Clinicas Electrónicas

Encuesta de Opinión por Internet
sobre Medicamentos Genéricos. Análisis de la Metodología Usada

¿Cómo Reducir los Errores en la Práctica
Médica a través de los Sistemas Clínicos de Información?

Historia clínica
Conexión de Bases de Datos y Confidencialidad

Konrad Zuse
El inventor de la primera computadora digital completamente programable

Historia Clínica

Conexión de Bases de Datos y Confidencialidad

Franco Simini. Profesor Agregado de Ingeniería Biomédica, Universidad de la República Investigador del CLAP Centro Latinoamericano de Perinatología (OPS/OMS) Hospital de Clínicas, Casilla de correo 627, 11600 Montevideo, URUGUAY siminifr@clap.ops-oms.org

Introducción

Debido a su naturaleza omnipresente y a su capacidad de memoria y de procesamiento, la aplicación indiscriminada de la Telemática puede llevar a abusos de control sobre la vida y sobre la privacidad de los ciudadanos.

La ausencia de leyes de protección de los datos individuales facilita la aparición de situaciones indeseables. El desafío actual consiste en acordar un conjunto de disposiciones preventivas para que se obtenga el máximo beneficio de la tecnología disponible sin atentar contra los derechos de las personas.

Es preocupante la posible aprobación del Parlamento Británico, en 2001, de la Regulation of Investigatory Powers que obligaría a los proveedores de Internet a mantener un dispositivo "de registro y escucha" a disposición de los servicios de inteligencia.

Esta ley obligaría, incluso, a los que usan criptografía a tener que entregar las contraseñas a las autoridades, con penas por incumplimiento de dos años de prisión. No sería posible aducir el olvido o la pérdida de la clave ante el requerimiento de descifrar un documento encriptado.

Protección de datos individuales

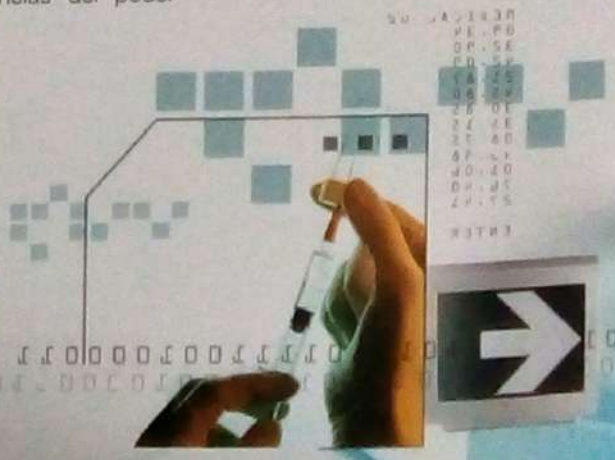
Un principio a establecer es que la relación de todas las bases de datos en forma indiscriminada no debe permitirse, ya que las consecuencias del poder derivado de las relaciones entre aspectos diversos y distantes en el tiempo y espacio de las personas atenta contra derechos establecidos en todas las jurisprudencias, como los derechos al olvido y a la privacidad.

Por otra parte, dentro de una determinada esfera de actividad, es conveniente que los datos dispersos sobre una persona puedan ser vinculados para mejorar el servicio y para dar garantías adicionales a la sociedad.

En la esfera bancaria y del crédito, la puesta en común de informes ha sido utilizada desde mucho antes de la disponibilidad generalizada de medios informáticos. Los organismos policiales de todo el mundo intercambian información sobre individuos requeridos a través de Interpol, que procura cruzar bases de datos de los diferentes países para facilitar la captura de las personas requeridas.

Entre las normas de protección de datos personales, se destacan las disposiciones de la CNIL (Comission Nationale de l'Informatique et des Libertes), organismo francés que regula desde 1978 las bases de datos y la privacidad de la información individual1.

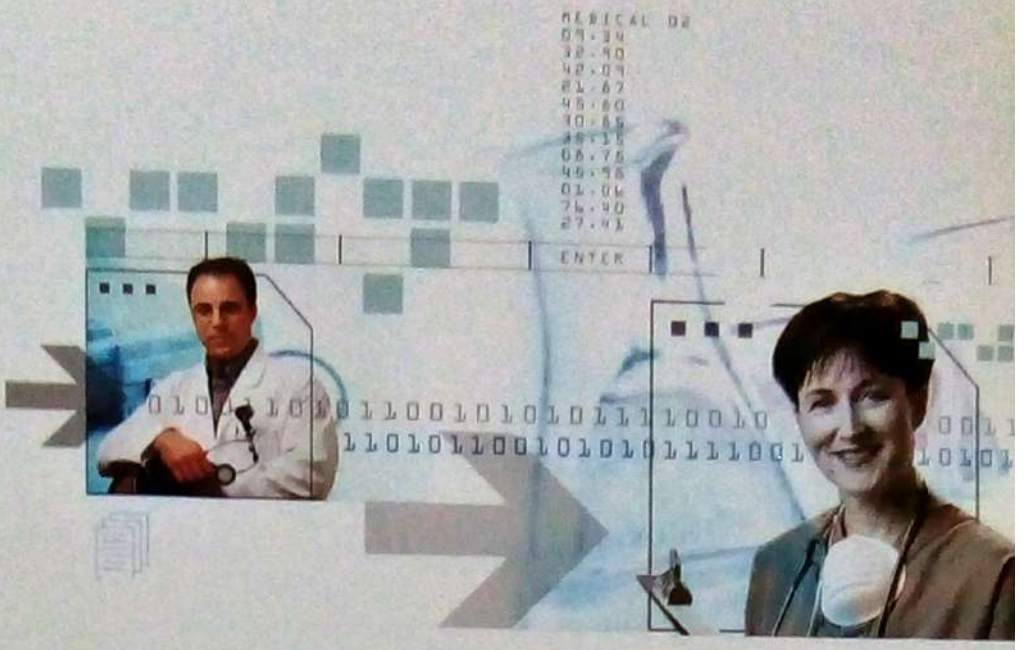
Se prohibe cruzar bases de datos de diferentes orígenes sin el consentimiento expreso de los interesados, quienes pueden solicitar la remoción de sus



datos de toda base de datos. Este enfoque se ha extendido a la mayoría de países europeos mediante la Recomendación del Consejo de Europa R(99) 51.

En Canadá, desde el mes de enero de este año, el Personal Information Protection and Electronic Document Act dispone que las bases de datos personales pueden contener información siempre y cuando el interesado haya dado su consentimiento (2). Esta ley se aplica en este momento sólo a los entes de alcance nacional y se extenderá a todas las empresas en pocos años. Llama la atención que se refiera únicamente a los ciudadanos de Canadá, por lo que queda la duda de si las empresas canadienses pueden capturar libremente datos de personas de otros países.

En el área de la salud, las pocas disposiciones legales son muy recientes. Desde el año 2000 rige en los EE.UU. el Health Insurances Portability and Accountability Act (HIPAA), que limita las informaciones médicas que pueden ser difundidas sin el consentimiento del paciente (2). En este contexto, el HIPAA maneja conceptos tan discutibles y tan poco definidos como la autorización de difundir "únicamente la información relacionada con la salud que sea necesaria para el objetivo propuesto". Esta ley deberá ser aplicada en todas las instituciones de salud antes de 2003.



Investigación clínica y calidad de servicios

Manteniendo la necesidad de preservar la privacidad de cada individuo, es innegable que la posibilidad de vincular datos referentes a la salud y a los servicios prestados en diferentes etapas de la vida, e incluso de una generación a las siguientes, aporta beneficios para la investigación, el control de calidad de la atención médica, y el seguimiento y gerencia de políticas de salud.

Por lo tanto, se debe proponer una modalidad que permita el desarrollo de la vinculación de bases de datos en el ámbito de la salud, preservando al mismo tiempo el derecho a la privacidad de cada individuo y el aislamiento de esta información de otras esferas, como la financiera, laboral, policial, los seguros, etc.

Separar lo privado de lo público

El principio que proponemos aquí es el de separar el ámbito privado del prestador de servicios de salud (médico u hospital) del ámbito semipúblico de los repositorios de datos clínicos.
En el ámbito privado, toda la información médica y personal es imprescindible y se registra localmente. Estos datos deberían estar protegidos legalmente para que se penalice su envío a otros ámbitos acompañados de la identificación personal.

En el ámbito semipúblico, se debe prever la posibilidad de acumular experiencia de salud en repositorios nacionales o regionales con fines de investigación y de control de calidad de los prestadores de salud, preservando el anonimato de cada individuo pero permitiendo su seguimiento a través de instituciones diversas y a lo largo del tiempo.

Es preciso legislar acerca del tipo de datos que no viajarán jamás fuera de la institución (por ejemplo: el nombre, la dirección y el número de documento del paciente) y aquellos que deben hacerlo (por ejemplo: días de internación, diagnósticos, procedimientos realizados y fármacos recibidos).

Para correlacionar datos de diferentes prestadores de salud sobre el mismo paciente y seguir el estado de salud de la población, los datos a enviar al repositorio deberán tener una identificación anónima pero consistente, sin importar de dónde provenga.

El mecanismo que se propone es la "criptografía sin vuelta", o sea, un algoritmo que no permita la "desencriptación", como es el caso de las palabras clave de acceso a programas de computadora.

La información sensible no debe dejar, bajo penas severas, el ámbito del prestador de salud que la recibe en el instituto del secreto médico. Por el contrario, la información clínica, individualizada en forma consistente pero no identificable con ninguna persona, deberá ser remitida para estudios y verificación de calidad de servicios.

El mecanismo de encriptación será de dominio de las instituciones de salud que sabrán cómo fabricar el código encriptado de cada uno de sus pacientes, partiendo de su identificación civil. En caso de tener acceso a una base de datos de salud de carácter nacional, elegido un caso no será posible deducir su identidad (por la característica del encriptado).

De esta forma, se protege al individuo del uso abusivo de su información nominativa en ámbitos alejados de su directo prestador de salud. Sin embargo, a partir de una identidad civil y aplicándole el algoritmo de "encriptado médico", se puede verificar si coincide con la identificación encriptada médica.

Más aún, disponiendo de una base de datos de identificaciones civiles -por ejemplo, con contenido de antecedentes policiales- se le podría aplicar a todos el algoritmo de encriptado médico obteniendo una base de datos policial con numeración encriptada de origen médico y sería posible, entonces, correlacionar las bases, en flagrante violación de la norma de privacidad que se pretende proteger.

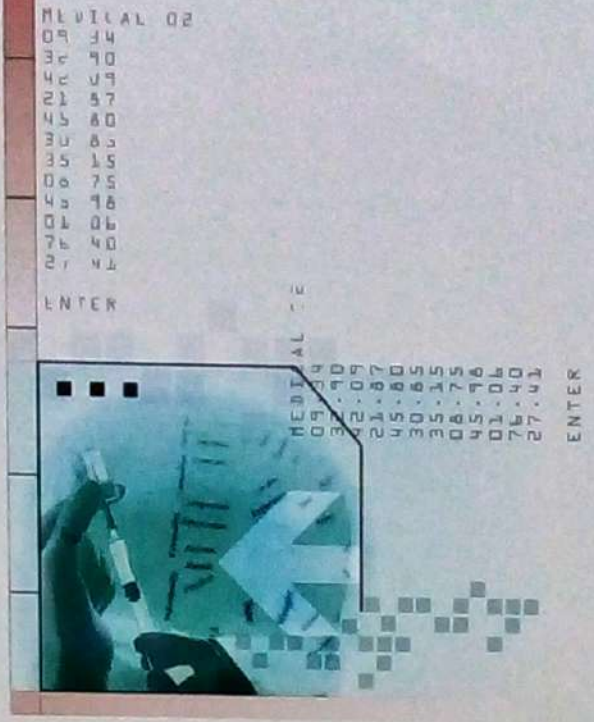
Esta observación lleva a establecer que el conjunto de datos que no debe dejar el ámbito del prestador de salud deba incluir las informaciones que, aun siendo de carácter médico, puedan perjudicar la privacidad en el caso de una asociación fraudulenta de bases de datos clínicos con otras.

La existencia de repositorios de información médica, accesibles en la red global en forma creciente, pone un nuevo desafío a esta propuesta. ¿Deben los datos de identificación nominativa estar incluidos en una historia clínica allí depositada? Actualmente, el conjunto de datos personales es accesible únicamente mediante una clave de acceso y, por lo tanto, se considera protegida su privacidad. Sin embargo, la mera existencia de una base de datos en la que se encuentran simultáneamente datos nominativos y médicos sujetos a reserva es una amenaza a su privacidad.

En efecto, la base puede ser robada en su totalidad o accedida en forma fraudulenta, y su contenido, divulgado o utilizado con otros fines. Una posible solución es, entonces, la de separar la información nominativa para excluirla de los repositorios de historias clínicas cuya identificación encriptada sea asociada con una persona concreta únicamente por la institución de asistencia médica y obtenga la autorización del paciente.

De esta forma, se consagran dos ámbitos separados: el de los datos personales limitados a la esfera local y el de los datos clínicos que se vuelven anónimos en la esfera epidemiológica. Únicamente el paciente o su medico tendrá el derecho y la posibilidad práctica de asociar los dos dominios para el cuidado de la salud y la documentación de los servicios prestados.

Finalmente, se podría asociar a cada dato clínico el carácter de secreto o de disponible a criterio del propio paciente, que es quien debe decidir. La tecnología informática puede adaptarse a este requerimiento, y los prestadores de salud deberán consignar la voluntad del paciente en cada caso y para cada dato.



Es conveniente que los datos dispersos acerca de una persona puedan ser vinculados para mejorar el servicio. Pero no debe permitirse la relación de todas las bases de datos de forma indiscriminada.

La consulta al paciente sería similar a la que se realiza habitualmente para donar órganos y para solicitar el consentimiento informado en caso de participar en protocolos de investigación. En caso de que no se manifieste el paciente, sus datos serán considerados secretos.

El Sistema Informático Perinatal

El Sistema Informático Perinatal (SIP) es el soporte de registro de datos clínicos perinatales de gran parte de las maternidades de América Latina y del Caribe (3), desde 1985. El registro de datos tiene como base el embarazo sin indicación de la identidad de las pacientes.

El nuevo proyecto de SIP 2000 tuvo que enfrentar el desafío esbozado en este artículo. El SIP, en su versión para Windows e Internet, maneja información confidencial de la paciente, tal como la que necesita el prestador de servicios de salud directo.

Al asumir funciones de repositorio de bases de datos, esta información privada es retenida y la identificación es encriptada, lo cual asegura la unicidad de los datos de cada paciente sin divulgar su identidad. Esta protección atañe al número de documento de identidad (que es encriptado) y a las informaciones sensibles (dirección teléfono, nombres, etc.) que se retienen en el ámbito privado y no viajan al repositorio. Los indicadores disponibles en Internet procesan grandes repositorios de datos clínicos (4) donde no figura la identificación de pacientes.

1. Reafirmar el Secreto Médico y establecer penas para su violación.
2. Reafirmar el derecho a la privacidad y al olvido de las personas, en particular sobre sus datos médicos.
3. Prohibir el traslado o accesibilidad de bases de datos (aún de un solo caso) con información personal.
4. Normalizar la constitución de repositorios de datos clínicos con información de interés médico y epidemiológico, con identificación encriptada para permitir estudios en el ámbito de la salud.
5. Difundir ampliamente indicadores de salud, resúmenes epidemiológicos y de control de calidad de las instituciones sobre bases de datos vueltas anónimas.
6. Prohibir la asociación de datos nominativos con datos clínicos en el ámbito de bases de datos en forma explícita, excepto en caso de consentimiento del paciente.

Referencias

1. Comission Nationale de l'Informatique et des Libertes (CNIL) www.cnil.fr.
2. Kowalenko, K. "Protecting your e-health privacy" The Institute IEEE, www.ieee.org
3. Simini, F. Perinatal Information System (SIP): a clinical database in Latin America and the Caribbean.
4. CLAP (OPS/OMS) Sist.Informáticos en www.clap.hc.edu.uy