Seguridad y confidencialidad en Medicina

El tratamiento automático de las historias clínicas presenta problemas de confidencialidad y seguridad diferentes a los que se tienen con modelos clásicos. La presencia física no es necesaria para el acceso y modificación de los datos. Asimismo, las consultas masivas pueden permitir la elaboración de listas de historias clínicas con determinadas características (patologías, hábitos...), cuyo uso puede ser de mucho interés para usuarios ajenos.

El Convenio para la Protección de las Personas con Respecto al Tratamiento Informatizado de Datos de Carácter Personal (ratificado por España el 27-1-1984) recoge esta preocupación. Los datos relativos a la salud sólo pueden ser tratados de forma automática si se dan mecanismos contra su destrucción accidental o no autorizada, la pérdida accidental o el acceso, modificación y difusión no autorizados. El Consejo de Europa ha emitido asimismo tres recomendaciones en las que se pone de manifiesto el interés por la regulación del acceso y el uso de los datos referentes a la salud:

1. Recomendación, R(81) 1, sobre Bancos de Datos Médicos Automatizados, Enero 1981;
2. Propuesta de Recomendación sobre Comunicación de Datos Sanitarios en Hospitales, junio 1992;
3. Recomendación, R(97)5, sobre Protección de datos médicos febrero 1997).

En España, la Ley Orgánica de Regulación del Tratamiento Automático de Datos menciona los apartados de la Ley General de Sanidad bajo los cuales se deberá permitir dicho tratamiento automático. La Agencia de Protección de Datos española se encarga de vigilar la aplicación de dicha Ley Orgánica y tiene la potestad de imponer sanciones en caso de violación de la misma.

Asimismo, la norma UNE-ENV 12924 Informática Médica: "Clasificación de Seguridad y protección para los Sistemas de Información Sanitarios" recoge el trabajo realizado por un grupo europeo de estandarización y da unas normas genéricas que deben regir la seguridad de estos sistemas de información. Finalmente, el Plan de Salud de Canarias recoge explícitamente su preocupación por la confidencialidad de los datos respecto a los portadores del virus VIH.

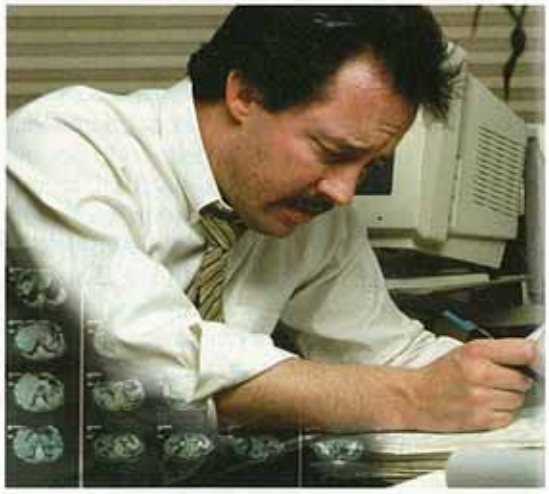
El primer problema que se ha de resolver es la permanencia de los datos frente a destrucción accidental. Existen diferentes soluciones como copias de respaldo, discos en espejo, clustering, etc. La evaluación de las necesidades en cuanto a la tolerancia de pérdida de datos y a su disponibilidad, y el estudio coste/beneficio ha de llevar a alguno de estos esquemas o a una mezcla de ellos.

Frente a los problemas accidentales, cuya resolución está muy ligada a la arquitectura física y de sistema operativo, la seguridad ante acciones no autorizadas supone una complejidad mucho mayor. En esencia, se deben establecer un conjunto de acciones permitidas para cada usuario del sistema y desarrollar dichas restricciones mediante diferentes mecanismos. De esta manera, el médico de atención primaria puede tener una visión de la historia clínica diferente a la del especialista y a la del médico de urgencias. Asimismo, la historia clínica es una fuente de información muy valiosa para estudios epidemiológicos o de gasto en los que la identidad de los usuarios finales del Sistema de Salud no tiene porqué ser conocida, pero sí la parte pertinente de su historia sobre la que se elaboran estadísticas. El pliego de prescripciones técnicas del concurso prevé una integración entre historia clínica y sistemas de gestión de pacientes y de gestión clínica. Para esto se ha de llevar a cabo un estudio que identifique que parte de la historia ha de estar disponible para los usuarios de los dos sistemas mencionados.

Aparte del mencionado requisito de seguridad ante pérdida accidental, cuatro son los principales problemas de seguridad que han de abordarse en todo sistema de información:

a) Autenticación: el usuario de la historia clínica ha de proporcionar su identidad de forma unívoca. Este es el primer paso en los mecanismos de seguridad, pues deberá permitir descartar usuarios del sistema frente a los que no lo son.

b) Integridad: los datos de historia clínica no han sido alterados durante su transmisión y, por tanto, reflejan fielmente la información introducida. Esto

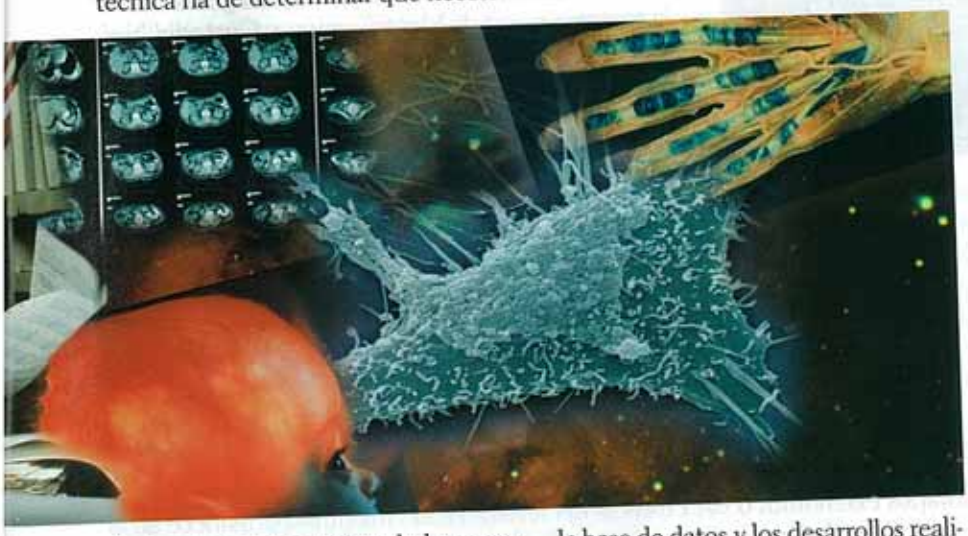


incluye la imposibilidad de modificación o corrupción de datos tanto de forma accidental como intencionada. Este problema se puede presentar por problemas de comunicación con la base de datos de historia clínica o por modificación intencionada de dichos datos durante su transferencia. Se ha de garantizar la integridad en los procesos de comunicación entre el usuario y la base de datos de historia clínica y viceversa. Esta comunicación se establece con frecuencia entre centros mediante redes públicas de comunicaciones.

c) Confidencialidad y acceso: tan sólo las operaciones permitidas al usuario (lectura, borrado, escritura...) sobre los datos accedidos podrán llevarse a cabo. Tal como se indica en el pliego de prescripciones técnicas del concurso, la in-

tegración de historia clínica de atención primaria con especializada va a suponer un reparto entre dos profesionales. La solución adoptada ha de venir precedida por un estudio acerca de los derechos de acceso y modificación por parte de estos. Otros usuarios del sistema (urgencias, gestión de pacientes, gestión clínica...) pueden tener acceso a parte de la historia clínica o a estadísticas o informes acumulados de la misma. Se ha de estudiar la necesidad de cortafuegos (*firewalls*) para limitar los accesos a determinados recursos físicos y lógicos en el caso de redes abiertas y susceptibles de recibir conexiones externas.

d) No recusación: como tal se entiende la incapacidad por parte del usuario que accedió a los datos a negar dicho acceso. De forma menos estricta, la Organización Mundial de la Salud indica como una de las características de la historia clínica la identificación del usuario que anota datos. La asistencia técnica ha de determinar qué necesidades de no recusación de los accesos a la base de datos de historia clínica existen y la forma de garantizarlas. Hay que indicar que este requisito sólo es necesario para los datos y accesos para los que varios usuarios estén autorizados, puesto que en el caso de acceso único (por ejemplo, datos que sólo el médico de atención primaria puede introducir) la no recusación está implícita en los mismos datos.



La forma global de hacer frente a los requisitos de seguridad y confidencialidad está basada típicamente en dos mecanismos:

Usuario/clave y Certificados.

- El primer mecanismo deberá permitir a cada usuario tener una palabra clave de obligada introducción en el sistema de historia clínica. Se da respuesta de esta manera al requisito de autenticación. Sin embargo, la integridad y el acceso han de ser garantizadas por parte de la base de datos de historia clínica. Para asegurar la integridad se recurre a mecanismos como el bloqueo de datos, transacciones atómicas (o se modifica todo o no se modifica nada) y códigos de redundancia que aseguren fiabilidad en las comunicaciones. Asimismo se puede recurrir a mecanismos seguros de comunicación del tipo SSL (*Secure Sockets Layer*). En cuanto a la no recusación, se ha de garantizar que, en el caso de necesitarse, la base de datos almacena la información de quién y cuándo se produjeron los accesos de los que se desee tener traza. Esto supone que la definición de un modelo de datos ha de proporcionar una orientación a la seguridad de los mismos. Como ventajas fundamentales de este mecanismo están su simplicidad y el uso intuitivo que los usuarios no especializados hacen del sistema. Por contra, la base de datos y los desarrollos realizados alrededor de la misma han de garantizar los requisitos de integridad, acceso y no recusación. Este mecanismo puede verse reforzado por la lectura por el sistema de una tarjeta identificativa del personal (médico o de enfermería) que accede al sistema.

- El mecanismo de certificados es más complejo. Involucra a una autoridad de certificación que emite certificados para los usuarios del sistema. Un certificado deberá permitir asegurar la identidad del usuario que envía datos con lo que se resuelve la autenticación, proteger los datos enviados de forma que se cumpla su integridad y tener constancia demostrable de que dicho usuario los envió (no recusación). El procedimiento es complejo, pero en esencia consta de una pareja clave pública/clave privada asignada a cada usuario. Los datos que se desea transmitir se encriptan con la clave pública del receptor, por lo que sólo este puede desencriptarlos con su clave privada. Este mecanismo soluciona el problema de distribución de la clave existente en los algoritmos simétricos donde se usa la misma clave para encriptado y desencriptado. Adicionalmente se hace un resumen corto de los datos mediante un algoritmo no reversible. Si este resumen no coincide con el que el receptor hace por él mismo, se descartan los datos puesto que no se cumpliría la integridad.

El estándar de certificados SET (*Secure Electronic Transactions*) se utiliza para transacciones electrónicas en redes abiertas como Internet. El X.509v3 proporciona certificados asociados a un servicio de directorio del que se recogen las claves públicas de los receptores.

Las principales desventajas de esta solución son su complejidad y la necesidad de una autoridad de certificación. Para el acceso a una base de datos en la que la clave pública del receptor (la base de datos) es única, el usuario tan sólo debe pedir su certificado y guardarlo en su ordenador. Este certificado puede ser usado para otros propósitos como el correo electrónica seguro (con firma y asegurando integridad). La autoridad de certificación puede existir ya (Fabrica Nacional de Moneda y Timbre, ACE...) o ser creada por el Servicio de Salud para uso interno. En este último caso existen productos comerciales de directorio con generación de certificados X.509v3. Una prestación adicional que se ha de plantear es la posibilidad de nombrar usuarios sustitutos de forma automática. Los usuarios sustitutos tendrán los derechos de acceso a las historias clínicas que tengan los titulares durante un periodo de tiempo especificado. Sin embargo, los accesos serán registrados por la base de datos con el nombre del usuario sustituto en el caso de que se prevea el requisito de no recusación.

Como resumen, la asistencia técnica objeto de este concurso ha de estudiar los requerimientos de seguridad y confidencialidad a la luz de la legislación y las prácticas deontológicas médicas para dar respuesta a los aspectos antes mencionados.

Ignacio P. Rodríguez-Santana
Director de Sanidad de Indra