C O N C L U S I O N E S *

* Las conclusiones del informe fueron acordadas en el curso de la reunión por todos los asistentes a la jornada.

INTRODUCCIÓN

En la jornada llevada a cabo el 12 de diciembre del 2000 en Pamplona, para elaborar el Informe SEIS sobre "La Seguridad y la Confidencialidad de la Información Clínica", se expusieron y debatieron las 8 ponencias incluidas en este documento, y se desarrolló una sesión de trabajo para obtener las conclusiones globales.

Aquí se recogen las conclusiones acordadas por los participantes en la jornada de trabajo, que se apoyan en sus aspectos de detalle en las 8 ponencias, a las que se hace referencia más concreta cuando ello es necesario.

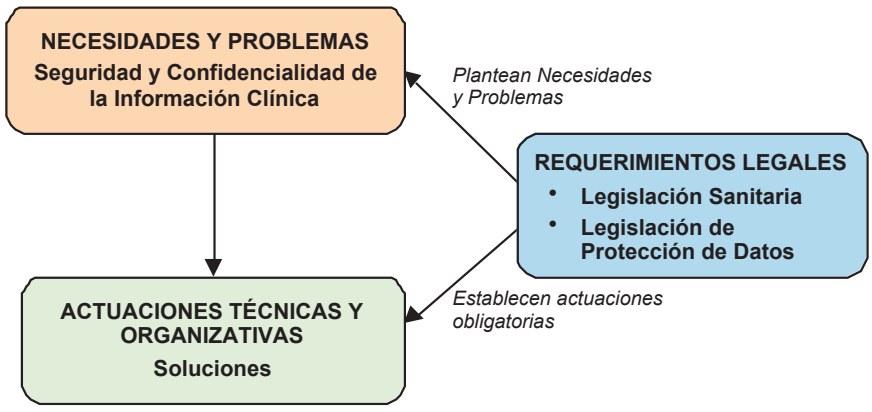
El primer aspecto a considerar es la propia estructura argumental de las conclusiones, para lo cual, teniendo en cuenta que las propias ponencias se agrupan en 3 bloques de forma natural:

–La visión de los usuarios (médicos, gestores e investigadores): ponencias 1, 2 y 3,

–La visión de los técnicos en SS.II.: ponencias 4, 5 y 6,

–La visión legal: ponencias 7 y 8,

se decidió seguir el siguiente esquema:



En cada apartado se discutieron los siguientes aspectos principales:

–Necesidades y problemas

- Aspectos previos: Necesidad de información sanitaria (recogida, tratamiento, difusión); el problema de la estandarización; qué información se ha de proteger.

- Quién ha de acceder a la información, para qué, con qué seguridad. Problemas para garantizar la seguridad y confidencialidad.

–Requerimientos legales: los requerimientos legales, producto de la propia legislación sanitaria y de la legislación en materia de protección de datos de carácter personal, afectan tanto a las necesidades y problemas, como a las actuaciones técnicas y organizativas. Por ello, en las conclusiones no se ha desarrollado como un apartado independiente, sino que se ha integrado en los otros dos. Por otra parte, un tratamiento detallado del marco legal se puede encontrar en la ponencia "Aspectos legales de la seguridad y confidencialidad en la información clínica".

–La titularidad de los derechos de la información clínica fue ampliamente discutida. Esta cuestión está tratada además de en la ponencia sobre aspectos legales, en otros trabajos del mismo autor* a los que pueden recurrir las personas interesadas en estos aspectos

–Actuaciones técnicas y organizativas: una vez identificadas las necesidades y problemas fundamentales, se identificaron las principales actuaciones a realizar, tanto técnicas como organizativas, para atender las necesidades en materia de seguridad y confidencialidad de la información clínica, que deben enmarcarse en un plan global de seguridad.

NECESIDADES Y PROBLEMAS

Aspectos previos

Tratamiento y disponibilidad de la información

El objetivo de cualquier sistema de salud ha de ser prestar la mejor asistencia posible a los ciudadanos. Un elemento necesario para proporcionar una mejor asistencia es el tratamiento y disponibilidad de la información, tanto para la propia asistencia, como para los aspectos de gestión e investigación asociados.

* Andérez A, Historia Clínica e informática: aspectos legales.
I. Informática y salud 1999, n.º 18 (896-899). II. Informática y salud 1999, n.º 19 (968-969). III. Informática y salud 1999, n.º 20 (1022-1026).

Estandarización de la información

Un aspecto que se trató en la jornada de trabajo, y que se reseña también en alguna ponencia, es el problema que supone la falta de estandarización de la información clínica. Aunque éste no era el objeto del informe, resulta interesante incluir una breve síntesis de las reflexiones efectuadas:

–Los diferentes servicios de salud requieren en muchos casos compartir información clínica. Este proceso actualmente no está automatizado, ya que cada servicio de salud estructura la información recogida en la historia clínica de manera diferente. El intercambio de información se ha de hacer de modo manual, lo cual es lento y costoso, amén de susceptible de errores de transcripción. A la escasa estandarización de las historias clínicas, se une la inexistencia de un número de identificación único por paciente de ámbito estatal, porque los códigos de identificación de la Tarjeta Individual Sanitaria (TIS) son diferentes en los distintos servicios de salud.

Teniendo en cuenta estos problemas, parece lógico que se establezca una estructura estándar mínima de historia clínica informatizada, en el ámbito nacional e incluso en el ámbito europeo, que vaya más allá del Conjunto Mínimo Básico de Datos (CMBD).

–Además de los intercambios de información entre servicios de salud, para estandarizar la historia clínica, se deberán tener cuenta los niveles de atención sanitaria, atención primaria y especializada, porque la necesidad de información clínica de ambos niveles es diferente.

En definitiva, existe consenso a la hora de considerar como necesario para un mejor aprovechamiento de la información, la estandarización de los aspectos fundamentales de la historia clínica, así como la existencia de un identificador único para la TIS.

Seguridad y la confidencialidad de la información

El tratamiento de la información clínica siempre ha tenido asociada la necesidad de seguridad y confidencialidad, debido al carácter especialmente sensible de los datos de salud.

Esta necesidad, los problemas que plantea satisfacerla, y las formas de abordarlos son el objetivo del presente informe.

Qué información se ha de proteger

Se considera que información clínica es la relativa a la salud de una persona identificada o identificable.

Necesidades y problemas en materia de seguridad y confidencialidad

La seguridad y confidencialidad de la información clínica es un mandato claro para todas las personas que intervienen en el proceso asistencial, y en sus aspectos derivados como la gestión e investigación. Esta obligación está establecida desde diferentes fuentes:

–Legislación en materia sanitaria.

–Legislación en materia de protección de datos de carácter personal.

–La propia ética profesional.

Además de ser una obligación ética y legal, la seguridad y confidencialidad de la información clínica es una condición para que los profesionales sanitarios acepten usar las Tecnologías de la Información y las Comunicaciones (TIC), y las aprovechen para prestar un mejor servicio a los pacientes.

Aunque la necesidad del secreto y la confidencialidad es anterior al desarrollo de las tecnologías de la información; su desarrollo y difusión, a la vez que permite un mejor manejo de la información, plantea necesidades y problemas adicionales.

Los problemas básicos de la seguridad de la información clínica, al igual que la de cualquier tipo de información, son cuatro:

–Autentificación.

–Integridad.

–Confidencialidad.

–No Repudio.

Entre las necesidades y problemas identificados en las ponencias incluidas en este informe, en la sesión dedicada a conclusiones se identificaron algunos por su carácter destacado.

A continuación, se detallan las necesidades y requerimientos del sistema sanitario relacionados con la seguridad y confidencialidad que se identificaron como fundamentales:

Regulación de la seguridad y confidencialidad de la información clínica

La seguridad y confidencialidad de la información clínica están reguladas por diferentes leyes y normas, que en la actualidad no siempre son congruentes. Esta falta de coherencia puede provocar una confusión que lleve a desaprovechar algunas de las posibilidades de las TIC bien por temor a infringir alguna norma, bien por excederse en su cumplimiento.

Se hace necesario unificar criterios en lo que respecta a la confidencialidad de la información clínica, lo que en una primera instancia podría resolverse con códigos tipo como permite la Ley Orgánica de Protección de Datos, y con el tiempo en una regulación legal más clara.

Esos criterios claros en el tratamiento de la información se han de establecer en las distintas funciones del proceso sanitario: asistencia, docencia, investigación, evaluación y gestión.

Acceso a la información

Dentro de la seguridad y confidencialidad de la información un aspecto clave es el control de acceso a la información, es decir, quién y a qué puede acceder.

Entre los problemas en el acceso a la información, se pueden destacar algunos:

–Como los datos clínicos son información especialmente sensible, es necesario establecer perfiles de usuarios, delimitando el acceso a la información dependiendo de las funciones a desarrollar en cada puesto de trabajo. Del mismo modo habrá que definir por cada perfil establecido el tipo de operaciones que puede realizar (escritura, solo lectura…). También se deberán ocultar los datos de carácter personal en aquellas tareas en las que no sea necesario la identificación del paciente, como por ejemplo en la realización de estadísticas.

Acceso con autorización, sólo a la información necesaria y para operaciones necesarias.

–Del mismo modo que es necesario establecer los niveles de acceso a la información, será necesario que se garantice la autenticidad de los accesos a los sistemas de información, es decir que tanto las personas, como los recursos (conexiones externas, servidores en red...) que acceden a los sistemas de información estén correctamente identificados y se asegure su autenticidad.

Verificar quién accede y comprobar que está autorizado a ello.

–Debido a la alta rotación del personal de enfermería en los servicios de salud, la gestión de los usuarios de los sistemas de información se hace muy complicada, lo que hace que se generen usuarios genéricos, y por tanto se pierde el control de la información tanto consultada, como introducida.

Gestión ágil de altas y bajas de autorizaciones.

–El proceso de automatización de la historia clínica permite en muchos casos delegar tareas en personal administrativo, que debe ser autorizado para acceder a

información sensible, pero se requiere que esté formado en la importancia de la confidencialidad, en los procedimientos de seguridad y en la responsabilidad en que incurre. Por otra parte, el contenido de la información clínica sigue siendo responsabilidad del personal sanitario que debe asegurarse de su validez y fiabilidad.

La desburocratización y la delegación de tareas exigen hacer explícitos los procedimientos y normas de seguridad, y la responsabilidad de todos los implicados en el proceso asistencial.

Intercambio de información

El intercambio de información clínica con terceros plantea dos tipos particulares de problemas:

–Técnicos: El uso de las redes públicas de comunicaciones plantea problemas a la hora de garantizar que la información circulante por dichas redes esté lo suficientemente protegida. Por ello, para salvaguardar la confidencialidad, dicha información se deberá transmitir cifrada. Además, este requerimiento lo establece el Reglamento de Medidas de Seguridad de la LOPD para los datos relativos a la salud.

Red segura.

–Legales: La cesión de información a terceros está regulada legalmente. Por lo que, cuando se realice, deberán cumplirse las normas establecidas, y seguir los procedimientos adecuados. Se deberá delimitar la información que se suministra, de manera que se cedan únicamente los datos estrictamente necesarios. Excepto en los casos previstos legalmente, para realizar la cesión será necesario el consentimiento expreso del afectado.

Cesión de información en los casos estrictamente necesarios, y de acuerdo con las normas y procedimientos legales establecidos.

Coste de la seguridad

Alcanzar los niveles de seguridad necesarios en el tratamiento de la información clínica, requiere de una dotación de recursos específica:

–Estructura. La función de seguridad en la organización debe contar con una estructura que garantice la disponibilidad de personal con sólidos conocimientos en materia de seguridad de sistemas de información.

–Recursos Económicos: La implantación de medidas de seguridad en los sistemas de información implica un coste de equipamiento, personal y programas. Esta situación debe tenerse en cuenta y valorar el coste de oportunidad que suponen las medidas de seguridad, frente a proyectos nuevos en sistemas de información, continuamente demandados en el sistema sanitario. Por ello debe buscarse un equilibrio entre inversión y seguridad, valorando que ningún sistema de seguridad garantiza el riesgo cero.

Necesidad de un cambio cultural

La necesidad de la seguridad y confidencialidad en la información clínica no está comúnmente asumida de forma práctica por el personal. Si no se consigue un cambio cultural en materia de seguridad, todas las medidas de índole técnico que se acometan estarán condenadas al fracaso.

Los síntomas de esa necesidad de cambio cultural son múltiples, pero pueden destacarse algunos:

–En la mayoría de los centros existen multitud de aplicaciones departamentales y bases de datos particulares que no se encuentran vigiladas o tuteladas por el personal técnico. Este tipo de aplicaciones no cumplen las normas legales vigentes en materia de protección de datos, y por lo tanto se deberían adecuar a dichas normativas o promover normas que se puedan cumplir y aseguren este tipo de ficheros de usuario.

–Existe una actitud reacia de los usuarios a utilizar los sistemas de información corporativos, y además es habitual en estos la cesión de contraseñas entre usuarios.

–La seguridad se concibe como un asunto secundario, ya que como norma general existe confianza en que no va a pasar nada. En muchos casos no se percibe la necesidad de la seguridad hasta que ocurre algo.

–Frecuentemente, se presta mas atención en disponer de la tecnología más avanzada, como por ejemplo la firma digital, que a solucionar los problemas básicos de seguridad, como las copias de seguridad o la cesión de contraseñas. Generalmente, estos problemas básicos son más organizativos que tecnológicos.

–En algunos casos el personal hace un uso indebido de los recursos y de la información clínica, por ejemplo comunicando información a pesar de su carácter confidencial.

–El personal directivo no tiene como una prioridad la seguridad y confidencialidad de la información clínica a la hora de asignar recursos.

Para conseguir el cambio cultural deseado en materia de seguridad se han de tener en cuenta varios aspectos:

–Parece más eficaz enfocar el problema de la seguridad como un problema de coste y riesgo, es decir, evaluar el coste que tendría la pérdida de un número elevado de historias clínicas, o la fuga de la información clínica de determinados pacientes. Para solventar estos problemas es necesario impulsar el cambio de cultura.

–Para impulsar el cambio se requiere una política de seguridad que marque las estrategias, fije las responsabilidades y delimite lo que se puede y no se puede hacer en lo que a seguridad de la información se refiere.

–Tanto para tener éxito en la implantación de las medidas de seguridad, como para conseguir mentalizar y concienciar al personal de los servicios de salud en la confidencialidad de la información y el correcto uso de los Sistemas de Información, será estrictamente necesario que los puestos directivos estén comprometidos con la implantación de las medidas de seguridad, así como en la concienciación del resto del personal.

ACTUACIONES TÉCNICAS Y ORGANIZATIVAS

Se han de acometer actuaciones técnicas y organizativas para satisfacer los requerimientos sanitarios, y además cumplir los requerimientos legales en lo que a protección de datos se refiere. De hecho, en el RD 994/1994 que aprueba el "Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal", se establecen una serie de actuaciones técnicas y organizativas concretas con carácter obligatorio.

Solución global de seguridad

La implantación de medidas de seguridad, para que proporcionen el nivel de seguridad requerido, se debe hacer de una manera organizada y coherente, planificando las actividades y proyectos que se deben llevar a cabo. El resultado ha de ser un Plan Integral de Seguridad en el ámbito de la información, que forme parte del Plan global de la empresa o entidad. La seguridad es uno de los componentes del Plan de Sistemas de Información.

Para llevar a buen termino el Plan Integral de Seguridad es imprescindible la implicación de los puestos directivos, de forma que el resto del personal acate las políticas y normas establecidas en materia de seguridad de la información.

El Plan Integral de Seguridad de la Información se deberá abordar mediante las siguientes actividades:

–Como punto de partida se realizará un Diagnóstico de Seguridad de la información y un Análisis de Impacto y de Riesgo.

–Definir y desarrollar la estrategia y políticas de seguridad, articulando y difundiendo las normativas de seguridad al resto de la organización.

–Definición de la estructura organizativa de seguridad y elaborar el manual de funciones y responsabilidades para cada puesto de la estructura definida. El propio Reglamento de medidas de seguridad de la LOPD obliga a tener un Documento de Seguridad que recoja estos aspectos.

–Seguridad Preventiva: Elaborar el Plan de Seguridad Preventiva Física, Lógica y de Comunicaciones, en el cual se incluirán las medidas necesarias a implantar para salvaguardar los elementos críticos de los sistemas de información de posibles ataques o vulnerabilidades.

> *La solución técnica a los problemas de autentificación, confidencialidad, integridad y no repudio estará basada en técnicas criptográficas.*

–Seguridad Correctiva: Elaboración del Plan de Contingencias y Recuperación de Desastres, de forma que se minimice el impacto ante un desastre sea del tipo que sea, recuperando un nivel de servicio aceptable en el menor tiempo posible.

–Por último, se deberá establecer un Plan de Auditorías mediante el cual se controle y verifique que se están cumpliendo las normativas y procedimientos establecidos.

Cambio Cultural

La técnica no puede solucionar los problemas de seguridad, salvo que vaya acompañada por un uso correcto por parte de las personas.

En el sector sanitario, es necesario un cambio cultural de las personas que lo componen, de forma que:

–Los profesionales sanitarios hagan uso de las posibilidades de los sistemas de información, para lo que se precisa, entre otras cuestiones, que confíen en su seguridad y confidencialidad.

–Las personas sean conscientes de la importancia de la seguridad y confidencialidad (no revelar datos, no compartir contraseñas, hacer copias de seguridad, etc.)

–Se recabe y use la información personal estrictamente necesaria.

–Se asuman los derechos del paciente, y de las personas en general, sobre sus datos.

Para conseguir este cambio cultural las actuaciones básicas son:

–Implicar a la Dirección.

–Clarificar, ordenar y hacer inteligible la normativa aplicable para que los profesionales sepan a qué atenerse.

> *En primera instancia recopilar la normativa aplicable y ejemplos prácticos de su aplicación en diferentes entornos sanitarios. A más largo plazo una forma de clarificar la situación sería la promulgación de un "Código Tipo" para el sector.*

–Implantar mecanismos técnicos de seguridad que sean lo más "amigables" posible para los usuarios. La seguridad no ha de suponer una falta de disponibilidad de la información para los profesionales sanitarios.

> *Si los profesionales han de recordar un gran número de contraseñas, se está abocado a que las escriban o sean muy fáciles.*

–Formación ética y técnica en materia de protección de datos personales.

PREVISIONES DE FUTURO

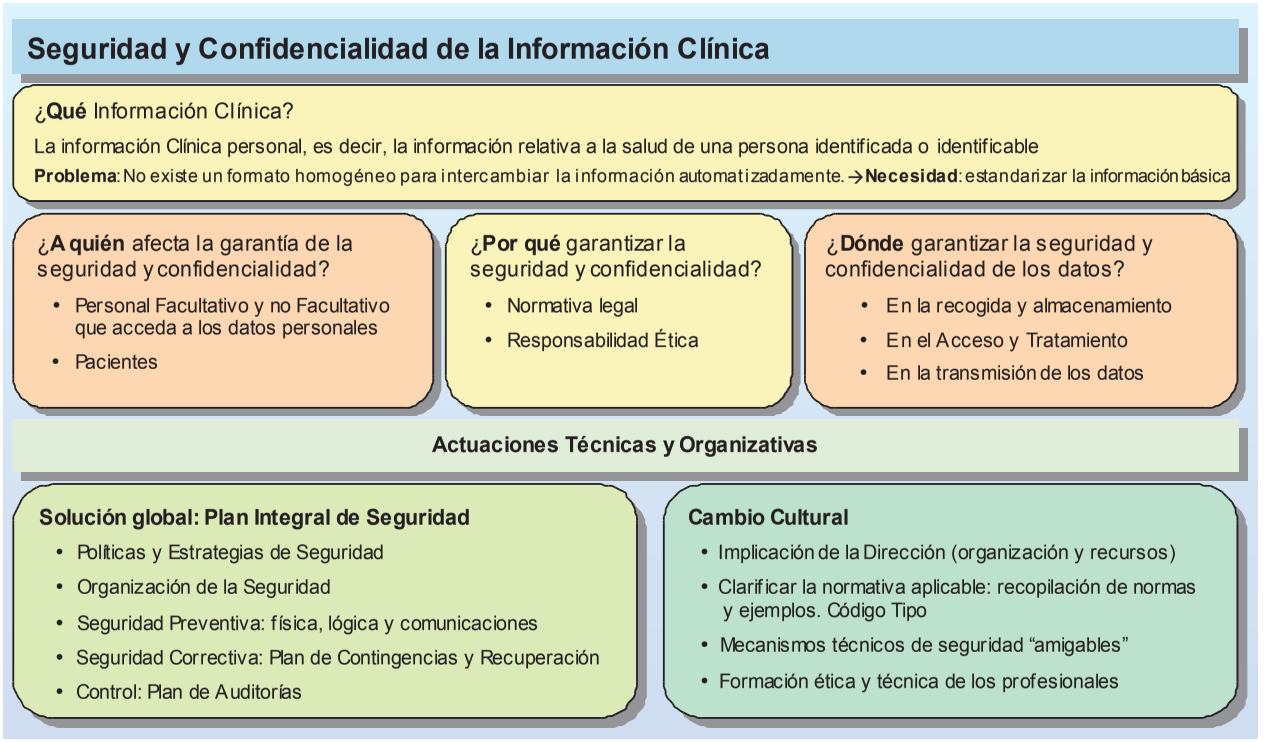
En los próximos tres años, los aspectos más importantes que se pueden prever son:

Se completará y clarificará la normativa, así como se desarrollarán los reglamentos necesarios tanto a nivel de los estados como de las diferentes regiones europeas.

Se estabilizará el mercado de las autoridades de certificación. Se verá si han quedado pocas autoridades que han fidelizado a muchas organizaciones, o bien han surgido muchas autoridades de ámbito menor y con valor añadido, que están relacionadas entre sí a través de entidades supranacionales.

Las políticas de seguridad se habrán establecido en la mayor parte de las organizaciones, estando además implantada la función de seguridad en las mismas, no como algo impuesto sino como necesario e incorporado a la cultura de las personas.

Los clientes y empleados de las organizaciones dispondrán de tarjetas inteligentes como medio de acceso en los terminales (PC, móviles, Web TV, etc.) con los que se comunican con las mismas.


Seguridad y Confidencialidad de la Información Clínica
¿Qué Información Clínica?
La información Clínica personal, es decir, la información relativa a la salud de una persona identificada o identificable
Problema: No existe un formato homogéneo para intercambiar la información automatizadamente. → Necesidad: estandarizar la información básica
¿A quién afecta la garantía de la seguridad y confidencialidad?
• Personal Facultativo y no Facultativo que acceda a los datos personales
• Pacientes
¿Por qué garantizar la seguridad y confidencialidad?
• Normativa legal
• Responsabilidad Ética
¿Dónde garantizar la seguridad y confidencialidad de los datos?
• En la recogida y almacenamiento
• En el Acceso y Tratamiento
• En la transmisión de los datos
Actuaciones Técnicas y Organizativas
Solución global: Plan Integral de Seguridad
• Políticas y Estrategias de Seguridad
• Organización de la Seguridad
• Seguridad Preventiva: física, lógica y comunicaciones
• Seguridad Correctiva: Plan de Contingencias y Recuperación
• Control: Plan de Auditorías
Cambio Cultural
• Implicación de la Dirección (organización y recursos)
• Clarificar la normativa aplicable: recopilación de normas y ejemplos. Código Tipo
• Mecanismos técnicos de seguridad “amigables”
• Formación ética y técnica de los profesionales