OMC
ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA

CONSEJO GENERAL DE COLEGIOS MÉDICOS

VILLANUEVA, 11 - TEL.: 91 431 77 80 - FAX: 91 576 43 88 (PRESIDENCIA) 91 431 96 20 (SECRETARIA) - 28001 MADRID

La Asamblea General del Consejo General de Colegios Oficiales de Médicos, en sesión celebrada el día 3 de diciembre de 2005, adoptó el acuerdo de aprobar, la siguiente declaración elaborada por la Comisión Central de Deontología:

CENTRALIZACIÓN INFORMÁTICA DE DATOS E HISTORIAS CLÍNICAS. PRINCIPIOS ÉTICOS DE PROTECCIÓN DE LA INTIMIDAD DEL PACIENTE

I. Introducción

1. En los últimos años, a causa del cambio en el modo de ejercer la Medicina, han surgido problemas al tener que compaginar la custodia de los datos médicos personales y el acceso adecuado a ellos para facilitar la atención de los pacientes. La mayor parte de los actores del sector salud están de acuerdo en la necesidad de informatizar la medicina; entre otros, los argumentos esgrimidos son la reducción de los errores sanitarios y la mayor accesibilidad a la información.

2. Es deber del médico guardar el secreto correspondiente a la salud de sus pacientes. Es derecho del paciente que la institución para la que trabaja el médico ponga todos los medios para salvaguardar la confidencialidad de sus datos de salud.

3. La concentración de datos los hace codiciables, por lo que deben existir razones muy poderosas para justificar el almacenamiento masivo o centralizado de información. La amenaza a la confidencialidad así creada, exige una total transparencia en este tipo de iniciativas, sancionadas por el consenso de grupos independientes (científicos, profesionales, judiciales, políticos, ciudadanos, económicos y comerciales) en cuanto a la pertinencia y relevancia de los datos precisos.

4. También debe determinarse -en la fase previa a toda implantación de almacenamientos masivos o centralizados- el tiempo de almacenamiento y las garantías y medios de destrucción irreversible de la información y todas sus copias, una vez cumplida su función. Asimismo, debe determinarse que datos se guardarán y custodiarán con fines de investigación, epidemiológicos y otros que se especifiquen.

VILLANUEVA, 11 - TEL.: 91 431 77 80 - FAX: 91 576 43 88 (PRESIDENCIA) 91 431 96 20 (SECRETARIA) - 28001 MADRID

II. Conflictos entre el acceso la custodia de la historia clínica informatizada

5. La gran mayoría de los centros sanitarios españoles comparten las mismas necesidades desde un punto de vista informático. Desde la centralización de los archivos clínicos para su consulta desde cualquier ordenador, pasando por el uso de la red para la transferencia de expedientes médicos, o el programa de gestión de un paciente, todo este tipo de procesos son compartidos por cualquier centro sanitario. La utilización de un conjunto de aplicaciones comunes en el conjunto del sistema sanitario nacional permitiría al conjunto de las administraciones públicas el poder gestionar de una manera mucho más eficiente la infraestructura sanitaria pública y poder aplicar los ahorros producidos de esta estandarización, en la implantación de mejores aplicaciones que permitan una mejor atención al paciente.

6. Los sistemas de informatización aseguran un mayor control del acceso a los datos clínicos registrados y una mayor transparencia, pero también pueden generar un mayor riesgo de acceso y divulgación no autorizada de dichos datos para fines distintos de los que llevaron a su recogida y conservación. En la medicina institucionalizada, el elevado número de personas que por cuestiones operativas tiene acceso a este tipo de información hace imposible, en la práctica, la observancia de una reserva absoluta. Los esfuerzos en medidas de seguridad no deben escatimarse, tanto más cuanto mayor sea el daño -siempre irreparable por mucho que se detecte y persiga- que podría causar un acceso no autorizado,

7. La tarjeta sanitaria informatizada puede guardar la historia clínica completa de un paciente; entonces, tiene la ventaja de que accede a la información sólo el profesional que trata al paciente y los datos no están guardados en una aplicación informática institucional. La tarjeta sanitaria puede ser también, sin que contenga datos clínicos, la llave que permite acceder a la información del paciente guardada en un sistema de información asistencial corporativo. Tiene la desventaja de que se puede perder y de que, tradicionalmente, es el hospital o el centro de salud el que cuida las historia clínica; el paciente debería llevar siempre consigo su tarjeta para que pueda ser útil en caso de accidente, agresión, etc. El sistema de tarjeta sanitaria permite que el ciudadano mantenga el control del acceso.

8. La utilización de un único programa informático en los diversos niveles de atención sanitaria, ya sea de lectura/ escritura de tarjeta sanitaria

como de acceso a los bancos de datos sanitarios facilita la atención del paciente, pero hace más problemático el derecho a la confidencialidad, por lo que deben establecerse controles de acceso muy rigurosos (RD 994/1999, de 11 de junio, capítulo N). La Agencia para la Protección de Datos es la encargada de comprobar que esos controles existen y se cumplen.

9. La proporción de los datos y circunstancias registrados por el médico en un documento clínico que pueda ser provechosa para otros sectores asistenciales o gestores es muy pequeña. Dicho de otro modo, una pequeña parte y solo de la información clínica del paciente está justificado que salga del centro en el que se produjo, y sólo cuando se requiera, nunca sistemáticamente.

III. Principios normativos.

Principios generales

10. En la historia clínica informatizada debe quedar registrada la identidad de los médicos y de los demás profesionales que han intervenido y accedido a ella en cualquier momento (Ley 41/2002, Artículo 14.1 y 3, Artículo 16.7). Es importante que custodien con diligencia sus claves de acceso, sin proceder a su revelación o puesta al alcance de otros, para proteger la información clínica, evitando tanto el acceso como la visualización de la misma por terceros. Igualmente, debe quedar registrada toda salida de información de los datos médicos, ya sea por impresión, en soporte informático, por correo electrónico, etc. Sin embargo, la responsabilidad de todos y cada uno de los profesionales que participan directa o indirectamente en la atención sanitaria de los pacientes no puede ser sustituida por ningún sistema de niveles de acceso, claves, encriptamientos y demás medidas necesarias de protección física y técnica de los sistemas de información, dado que también existen programas informáticos para descubrir claves de acceso.

11. Los profesionales sanitarios y no sanitarios que, por el desempeño de sus funciones, tienen contacto con la documentación clínica informatizada, están obligados a guardar el secreto profesional sobre esa información y sus claves de acceso; esta exigencia se mantendrá aunque se extinga el vínculo profesional. Igualmente, son responsables de la custodia y protección de la confidencialidad de dicha información. Las claves de acceso deben poder ser

cambiadas cada cierto tiempo y para cada persona autorizada con el fin de proteger el acceso a los datos.

12. Es básico un acceso selectivo a los datos separando debidamente los datos relativos a identificación de las personas, datos médicos, datos administrativos, datos sociales y datos genéticos. Nadie, excepto el personal sanitario encargado de la atención asistencial de un paciente, podrá tener acceso a los datos completos de su historia clínica, ya que exclusivamente a ellos ha dado permiso el paciente. Esta es la gran ventaja de la tarjeta sanitaria informatizada.

13. El artículo 61 de la Ley General de Sanidad sólo autoriza el acceso a la historia clínica a "los facultativos que directamente están implicados en el diagnóstico y tratamiento del enfermo, así como a afectos de inspección médica o para fines científicos".Todos los demás (familiares del enfermo sin su consentimiento, médicos o personal sanitario que no estén implicados directamente en el tratamiento o diagnóstico, personal para-sanitario o no sanitario que no realice labores de inspección o científicas, mutuas y compañías de seguros -excepto sus peritos médicos y sólo ellos-) no son "personal autorizado" y, consecuentemente, si acceden a estos datos sin consentimiento de su titular pueden cometer el delito previsto, con penas severas, en el artículo 197 del Código Penal. El delito se comete tanto por acceder como por apoderarse, utilizar o modificar datos de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

14. Una historia clínica informatizada puede organizarse en tres niveles de almacenamiento: 1) datos básicos que el paciente sabe que pueden ser utilizados por cualquier profesional que participe en su asistencia, aunque no sea su médico o enfermero habitual (el médico de cabecera negociará con el paciente cuáles han de ser esos datos), 2) datos privados, a los que sólo se tiene acceso con el permiso expreso del paciente, y 3) datos reservados, a los que el paciente no tiene acceso, pues recogen las observaciones subjetivas que los profesionales consideran necesario reservar por razones asistenciales, o datos referidos a terceras personas.

15. El médico con ejercicio privado es responsable de la información sobre pacientes registrada en las aplicaciones informáticas que utilice. En el ejercicio público, también será responsable de aquellos ficheros informatizados

de pacientes de los que no tenga conocimiento el responsable del centro sanitario.

16. El médico podrá cooperar en estudios de auditoria (epidemiológica, económica, de gestión), con la condición expresa de que la información en ellos utilizada no permita identificar ni directa ni indirectamente, a ningún paciente en particular (CEDM Artículo 17.5).

17. El personal con responsabilidades en los sistemas de información y redes de comunicación debe custodiar con especial cuidado identificadores y contraseñas que den acceso a los sistemas con privilegio de administrador. La transmisión de datos médicos a través de las redes de telecomunicaciones se deberá realizar cifrando dichos datos o utilizando un sistema que garantice que la información no sea inteligible ni manipulada por terceros. Mediante el conocimiento y seguimiento de las vulnerabilidades y fallos detectados en los sistemas, los administradores pueden mejorar la seguridad de los equipos que están a su cargo.

Principios deontológico específicos

18. En la búsqueda del ansiado equilibrio que permita aprovechar las ventajas de la introducción responsable de la informática en medicina, minimizando los riesgos para la seguridad de los datos personales, algunos principios deontológicos recogen los requisitos más convenientes para la protección de datos sanitarios informatizados:

- El principio de sobriedad (pertinencia)

De acuerdo con este principio, los profesionales sanitarios deben limitarse a recabar y registrar lo estrictamente necesario para asegurar una atención médica de calidad. Independientemente de lo difícil que puede resultar eliminar definitivamente datos introducidos en algunos tipos de sistemas informáticos que permiten rescatar archivos aparentemente borrados, es conveniente no registrar, salvo que sea imprescindible, aquellos detalles que, de revelarse, podrían poner en peligro datos muy sensibles de la intimidad de nuestros pacientes.

- El principio de transparencia

Es conveniente actuar correctamente, pero también dejar ver que se

está actuando así, de forma que la aplicación de las nuevas tecnologías no se considere como un instrumento más, exclusivamente dirigido a mejorar la eficiencia, sino que sirve, realmente, para promocionar valores humanos como la confidencialidad. Para ello lo mejor es que el paciente conozca qué tipo de información sobre su persona está recogido, así como quién y bajo qué condiciones puede acceder y/o accede a ella.

- El principio de responsabilidad

Este principio está estrechamente relacionado con la máxima hipocrática Primum non nocere. Por una parte implica que los profesionales deben ser cuidadosos y responsables en el manejo de los datos, habida cuenta de las consecuencias que para los pacientes pueden tener pequeños errores u olvidos. Por otra, recuerda que el trabajo en equipo no debe utilizarse como excusa para difuminar responsabilidades.

- El principio de protección universal

Hace referencia a que las medidas de seguridad para proteger los datos sanitarios deben ser aplicadas siempre, en todos los centros y para todos los usuarios (también los profesionales cuando son pacientes, por ejemplo).

IV. Conclusiones

19. Corresponde a los gobiernos autonómicos y central regular los conflictos entre los programas informáticos locales y los de los servicios de salud autonómicos, teniendo en cuenta que deben poner todos los medios para respetar el derecho a la confidencialidad de los pacientes. (CEDM Artículo 17A y Ley Orgánica 15/1999, de 13 de diciembre). Convendría instaurar unidades funcionales de documentación clínica dedicadas a supervisar las medidas de seguridad. No se puede olvidar que la relación médico-paciente requiere una salvaguardia y unos valores (respeto a la autonomía de los pacientes, existencia de un pacto implícito en la relación clínica, confianza social en la reserva de la profesión médica, lealtad debida al paciente), que deben custodiarse siempre si se quiere que el sistema sanitario funcione.

20. Las asociaciones de consumidores y usuarios y las de enfermos deben ser consultadas por los responsables del campo sanitario en cada

autonomía para incluir en las aplicaciones informáticas los varios niveles de seguridad que dichas asociaciones soliciten. Es ésta una forma de que los pacientes participen en las decisiones y sean informados de los peligros que, para la confidencialidad, suponen las bases de datos centralizadas; tienen derecho a estar informados acerca de qué se hace con sus datos y a decidir quien los maneja.

21. Solo deben tener acceso completo a la historia clínica quienes tratan al paciente o quienes codifican los datos de la misma, ya que los profesionales asistenciales del centro que realizan el diagnóstico, el tratamiento y llevan a cabo el cuidado del paciente tienen acceso a la historia clínica de éste como instrumento imprescindible para su adecuada asistencia. Tanto los profesionales de atención primaria como de especializada deben ser informados de manera transparente por el responsable del centro sanitario sobre cómo funciona el sistema informático que utilizan y quien puede tener acceso a él.

22. Los servicios centrales de un servicio de salud autonómico, por ejemplo, que precisan datos epidemiológicos, administrativos, etc. para tomar decisiones, sólo deben tener acceso selectivo, de forma que los datos clínicos y administrativos estarán disociados (CEDM Artículo 17.2 y Ley 41/2002 Artículo 16), y también están obligados al deber de secreto. Por tanto, deben disponerse perfiles de acceso y una segmentación conveniente, tanto de los usuarios de la aplicación informática como de las necesidades de información.

23. Los bancos de datos sanitarios extraídos de historias clínicas estarán bajo la responsabilidad de un médico y no pueden ser conectados a una red informática no médica (CEDM Artículo 17.3 y 4). Los mecanismos que permiten el registro de los datos estarán bajo su control directo sin que se deba permitir, en ningún caso, la desactivación de los mismos.

24. En la actualidad, debe desaconsejarse la centralización de los datos de las historias clínicas hasta que no mejoren las condiciones y sistemas de seguridad.

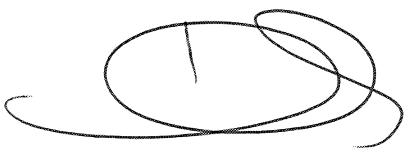
25. Los sistemas debe contar con una auditoria independiente que permita certificar sus características y seguridad así como determinar qué información y datos pertenecen a cada uno de los diferentes niveles, De igual manera y continuadamente un comité independiente y especifico deberá velar por la necesidad, pertinencia, relevancia y tiempo de conservación durante el

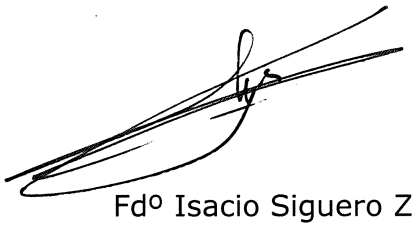
período que razonablemente resulte útil para alcanzar el fin que justificó su captura y tratamiento informático. O en su caso, por interés de la salud pública, de la ciencia médica, o para fines históricos o estadísticos, los datos deben ser anónimos para asegurar la vida privada del paciente.

26. Intereses públicos como, en ocasiones, la atención continuada y compartida de los pacientes, la inspección de servicios sanitarios, la gestión y planificación sanitaria y la investigación científica, aconsejan que una ley de carácter básica, contemple y regule los casos y las circunstancias en los que será posible el acceso a la información clínica. Es necesario establecer una legislación propia para proteger la intimidad de los pacientes, para que nadie pueda ser discriminado por información relativa a la salud y para salvaguardar del secreto médico, en desarrollo de los artículos 14 y 18 de la Constitución.

Madrid, 15 de diciembre de 2005
EL SECRETARIO GENERAL

Vº Bº
EL PRESIDENTE





Fdº Juan J. Rodríguez Sendín

Fdº Isacio Siguero Zurdo