Documentos semFYC

Informatización y confidencialidad de la historia clínica

Grupo de trabajo de Bioética de la semFYC

Nº 20

Informatización y confidencialidad de la historia clínica

Grupo de trabajo de Bioética de la semFYC

Grupo sanofi aventis
La Salud es lo esencial

Laboratorio cooperador

Los laboratorios cooperadores participan de forma no condicionada en la formación y desarrollo de la medicina de familia y comunitaria. Los laboratorios cooperadores colaboran en el desarrollo de las actividades científicas de la semFYC y comparten en su integridad los criterios de independencia y calidad científica de la misma.

Portaferrissa, 8, pral.
08002 Barcelona
www.semfyc.es

Coordinación y dirección editorial:

semfyc ediciones
Carrer del Pi, 11, 2a pl., of. 14
08002 Barcelona

Depósito legal:
ISBN: 84-96216-67-5

Índice

Introducción

En las Comunidades Autónomas del Estado español existe actualmente un despliegue de sistemas informáticos aplicados a la documentación clínica que se caracteriza por su diversidad, escasa compatibilidad y unas condiciones de seguridad que están generando algunas dudas sobre las garantías de confidencialidad de los datos personales almacenados. En el seno de la semFYC se ha considerado necesario promover la reflexión sobre esta relevante cuestión que tiene implicaciones importantes tanto desde la perspectiva de la ética profesional como para la sociedad en su conjunto. Con este fin, se hace público el presente documento dirigido no sólo a los médicos de familia, sino también a los agentes sociales y, en especial, a los responsables de la Administración sanitaria.

Utilidad, medidas de seguridad y transparencia

La informatización en medicina se ha convertido en un elemento más de la buena práctica médica, al constituir un instrumento de gran utilidad tanto para la asistencia como para la gestión. Frente a estas ventajas surgen los conocidos inconvenientes, relacionados principalmente con la seguridad de los datos y la salvaguarda de la confidencialidad, no ya de un paciente concreto, sino de toda una comunidad, tanto más cuanto mayor sea el grado de centralización de los datos informatizados. Por otra parte, los grandes beneficios potenciales de la informática y las tecnologías de la comunicación no deben hacernos perder de vista que la práctica de la medicina, más si cabe de la medicina de familia, se basa en la relación clínica y que estas tecnologías deben estar siempre al servicio de la misma y no al contrario.

Las necesarias medidas de seguridad en los sistemas de información implican un coste de equipamiento, personal, programas y mantenimiento que obligan, habida cuenta que el presupuesto es limitado, a buscar un equilibrio entre inversión y seguridad, teniendo siempre presente que ningún sistema garantiza el riesgo cero (tampoco el tradicional en soporte de papel, como de todos es sabido). Por otra parte, los sistemas tienen que generar confianza y para ello no sólo deben contar con las mejores medidas de seguridad y procedimientos de uso, sino que sus usuarios así han de percibirlo.

Un sistema informático que funciona bien y aplica todas las medidas de protección a su alcance no tiene inconveniente, todo lo contrario, en hacer transparente el uso de la información, permitien-

do que el paciente tenga conocimiento, si lo solicita, de quiénes han tenido acceso a sus datos personales, en qué momento y con qué finalidad.

Consideraciones éticas sobre el secreto y la confidencialidad

El deber de secreto y el derecho a la confidencialidad siempre han sido inherentes a la relación clínica y se fundamentan en sólidos argumentos éticos (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). Se recogen en todos los códigos deontológicos de las profesiones sanitarias, constituyendo su incumplimiento un delito tipificado y duramente castigado por la ley, que reafirma el derecho de las personas a la intimidad y a la confidencialidad.

Sin embargo, no constituyen una obligación absoluta, y puede revelarse información confidencial cuando existan razones fundadas para ello. La ley impone en ocasiones la revelación de información confidencial (conocimiento o sospecha de delitos, testificación en procesos judiciales) y permite compartir datos personales para finalidades distintas de aquellas que llevaron a su recogida, si se cuenta con el adecuado consentimiento de sus propietarios.

Con todo, dicho consentimiento puede únicamente ser presupuesto, como en el caso de los datos sanitarios recogidos para una finalidad asistencial y utilizados también para las funciones de inspección, evaluación, planificación sanitaria, etc., quedando sus depositarios siempre obligados por el deber de secreto.

En la medicina institucionalizada se producen una serie de circunstancias que no favorecen la salvaguarda de la confidencialidad. Una de ellas es el elevado número de personas que por cuestiones operativas, tienen acceso a este tipo de información y que hace imposible, en la práctica, la observancia de una reserva absoluta. Conviene recordar, sin embargo, que lo único que justifica el acceso a información confidencial es la función de *confidente necesario*, y que todo aquel que llegue a conocer datos confidenciales se encuentra obligado por un deber de secreto derivado o compartido que afecta a la institución sanitaria en su conjunto. Esto, hoy por hoy, implica un cambio cultural y de actitud que es necesario realizar.

Las consideraciones éticas sobre la confidencialidad son las mismas para los datos sanitarios recogidos y conservados en soporte papel o mediante las nuevas tecnologías (historias clínicas computerizadas y sistemas de transferencia e intercambio de información). Pero, aunque los sistemas de informatización pueden asegurar, en principio, un mayor control del acceso a los datos clínicos registrados sobre un paciente y una mayor transparencia, también pueden generar un mayor riesgo de acceso y divulgación no autorizada de los datos para fines distintos de los que llevaron a su recogida y conservación.

Además del peligro que podría suponer un "ataque" informático en la red sanitaria (posibilidad para la que siempre se debe estar prevenido, preparado y actualizado), hay que tener en cuenta a las personas que trabajan en el propio sistema sanitario. Ningún conjunto de medidas físicas de seguridad, ni sistema de claves, encriptamientos, verificaciones, restricciones, niveles de acceso, etc., aún siendo

imprescindible y necesario, puede proteger los datos computerizados de una persona que, teniendo acceso a ellos, permita usarlos o los utilice -por desconocimiento, descuido o intencionadamente- para una finalidad distinta de la formalmente establecida.

Principios deontológicos específicos

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, exclusiva-

mente 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).

Una llamada a la responsabilidad en la formación

Debe reiterarse la necesidad de promover y conseguir un cambio cultural (que pasa por la necesaria información y formación, tanto ética como técnica) para que la seguridad y confidencialidad de la

información clínica sean asumidas de forma práctica tanto por el personal sanitario como no sanitario, sin olvidar a los directivos de las instituciones sanitarias. La Dirección debería enfocar la cuestión de la seguridad evaluando qué beneficio justificaría la posible fuga de información de un número elevado de historias clínicas o de determinados pacientes, y con qué coste admisible, económico y moral, se podría evitar. Si la instauración de un sistema de información informatizado no ofrece garantías, puede verse afectada la esencia de la relación clínica - que es la confianza- y eso sería maleficencia.

Recomendaciones y conclusiones

En el ámbito de la Atención Primaria, conviene hacer algunas reflexiones dirigidas a potenciar la relación clínica entre usuarios y profesionales y la necesaria confianza social en la reserva de la profesión médica. En este contexto pueden resultar de utilidad algunos consejos de índole práctica:

a) El objetivo de cualquier sistema de salud debe ser prestar la mejor asistencia posible a los ciudadanos. Para ello es necesario un buen sistema de información que garantice prioritariamente la atención personal donde ésta tenga lugar, y a la vez, facilite las imprescindibles necesidades de gestión y planificación, así como la investigación. Ahora bien, el sistema de información es sólo el instrumento para alcanzar la meta: atender las necesidades de salud de las personas, moduladas por la opinión no sólo de la Administración y los profesionales, sino también de la población. Es en la meta donde debe centrarse el necesa-

rio debate. En medicina de familia la prioridad es que el sistema sirva a la relación clínica con el paciente -una relación de confianza-, y no al revés, resultando útil un instrumento en la medida en que colabore con este fin.

b) El diseño de los sistemas y de los soportes informáticos dirigidos al registro y utilización de la información clínica por parte del médico de familia deben, no sólo permitir, sino favorecer la mejor práctica clínica, integral, integrada, centrada en la persona y en su contexto sociofamiliar. Por ello deben estar preparados para contener, utilizar y custodiar, además de la patobiografía de los pacientes, elementos contextuales que incluyen información de terceros que pertenecen al ámbito sociofamiliar, datos sobre la estructura y estado de salud de la unidad familiar y sus características funcionales y relacionales.

c) No es correcto participar en la creación ni el mantenimiento de sistemas de elaboración, archivo o informatización de datos clínicos que no garanticen la máxima seguridad de los mismos. Los esfuerzos en medidas de seguridad deben fomentarse y no escatimarse, tanto más cuanto mayor sea el daño, siempre irreparable, que podría causar un acceso no autorizado.

d) La centralización de datos informáticos pasa por la necesaria transparencia y pertinencia, asegurándose en todo caso las máximas medidas de seguridad necesarias para el nivel de centralización que, con la máxima prudencia, se

decida. Se debe tener en cuenta que a mayor nivel de centralización, más personas se verán afectadas por una vulneración de los sistemas de protección.

e) 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.

f) El respeto a la autonomía y dignidad del paciente implica contar con él para el tratamiento de los datos de salud que le conciernen. El paciente debe tener un derecho efectivo a conocer quién accede a sus datos y en qué condiciones, así como a decidir qué información es accesible para otros profesionales y cuál no, siempre que esto no afecte a su atención sanitaria ni suponga un riesgo para la colectividad. Del mismo modo, podrá solicitar la cancelación o modificación de aquellos contenidos que sean inexactos o que no mantengan su vigencia. El problema es cómo llevar a la práctica estos derechos, asegurando el deber de guarda y custodia de la institución.

g) En las historias clínicas informatizadas deberían existir **3 niveles de almacenamiento** de datos. En el *primer nivel* se hallarían los 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. En un *segundo nivel*, aquellos datos privados, a los que sólo se tiene acceso con el permiso expreso del paciente (una opción sería una clave de acceso mixta: clave de nivel 3 del profesional más clave de autorización aportada por el paciente). En un *tercer nivel* se pueden situar ciertos 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. Quedaría por resolver en la práctica qué se considera información subjetiva del profesional, así como el modo de realizar su auditoría.

h) Las instituciones y centros sanitarios deben garantizar que los sistemas de registro adoptados y los circuitos de funcionamiento, mantenimiento y resolución de problemas son seguros. Además de cumplir los requisitos que establece la ley, se debe alcanzar un grado razonable de aceptación por los profesionales y los ciudadanos. La solución no es sólo de formación, sino de responsabilidad y de organización, tema que atañe directamente a las gerencias y exige destinar recursos económicos y humanos específicos a esta tarea.

i) Es muy conveniente que en Atención Primaria se desarrollen unidades funcionales de documentación clínica donde se supervisen las medidas de seguridad en los centros de salud, así como la formación de los profesionales en esta materia.

j) Tratándose de datos especialmente sensibles, las instituciones deben dar a conocer los usos posibles de esta información, su finalidad, las personas que tienen acceso, las situaciones que precisan consentimiento expreso y las medidas de seguridad aplicadas.

k) Una garantía adicional de transparencia y seguridad sería que todo el sistema fuera evaluado por un comité independiente en el que estuvieran representados los usuarios además de los profesionales sanitarios y los gestores.