

## **CONFIDENCIALIDAD DE PROCEDIMIENTOS Y DATOS, UNA REALIDAD ENTRE LA ÉTICA Y LO JURIDICO**

**Ponente: Isabel Tomé Tamame**  
XXIX Congreso Nacional de Enfermería  
Especialistas en Análisis Clínicos  
Junio 2010

Uno de los elementos que han distinguido históricamente las profesiones de los meros oficios es que sus responsabilidades se han definido más en términos morales que jurídicos. Tanto es así que la elaboración de un Código Deontológico de comportamiento, era uno de los requisitos que marcaban tradicionalmente la conversión de un oficio en una profesión. De esta manera la responsabilidad moral, por encima de la responsabilidad jurídica, constituía, junto con la elevada cualificación en un determinado campo del saber, el santo y seña de la identidad de un profesional.

Los Códigos Deontológico, los Comités Deontológico profesionales, las Reuniones y Declaraciones sobre ética han formado parte de la vida profesional del derecho, de la Medicina y la Enfermería más que de ninguna otra profesión.

La palabra ética viene termino griego ethos. En su sentido etimológico comprende una pluralidad de conceptos: costumbre, hábito, carácter, manera de ser adquirida....

La ética remite al compromiso que toda persona tiene, de formarse un buen carácter, que le permita vivir bien, llevar una “buena vida”.

Es importante reconocer que la libertad es la condición imprescindible para que sea posible la ética; sin libertad no hay ética.

Como decía Aristóteles en su Ética a Nicómaco: “No podemos escoger si somos de mármol o de arcilla, pero sí la forma que damos a este mármol o a esta arcilla”

Los valores éticos enfermeros se centran, en la persona como agente moral autónomo, la salud como equilibrio y adaptación y el cuidado como apoyo y ayuda a las personas con necesidades reales o potenciales de salud.

Entendemos que el acto de cuidar es un acto de vida, un acto que todos nos damos a nosotros mismos y que permite la continuidad de nuestra existencia.

Se cuida con el gesto, con la palabra, con la mirada, con el contacto y la presencia.

En las últimas décadas hemos asistido a un cambio radical en la manera de entender la relación con el paciente, evolucionando desde el concepto del paciente como mero receptor del acto médico, (paternalismo, maternalismo) hasta el modelo actual que le reconoce al paciente el derecho a gestionar su cuerpo, su vida y también su intimidad.

En nuestro país este cambio quedó plasmado en la ley General de Sanidad de 1986. A partir de ese momento la persona enferma recuperó derechos tradicionalmente relegados a un segundo plano ante la prioridad de restablecer su bienestar físico. De este modo pudo incluir sus valores, sus prioridades, su manera de entender la vida en las decisiones que le afectaban.

La intimidad se reconoce como un derecho fundamental del individuo, ligado al honor y a la libertad, en el artículo 12 de la Declaración Universal de

los Derechos Humanos y en el artículo 18.1 de la Constitución española de 1978, y como tal está contemplado en nuestro ordenamiento jurídico que contempla incluso penas de cárcel para quien lo vulnere (Código Penal, arts. 197-201).

De un lado, limita el acceso a la esfera íntima de las personas y además, reconoce el derecho a la confidencialidad de los datos personales, de este modo que quienes hayan entrado en conocimiento íntimos de otra persona no pueden revelarlos ni utilizarlos sin la autorización expresa del interesado o de una ley.

Intimidad y confidencialidad se complementan con el derecho a la protección de datos de carácter personal que otorga a su titular un poder de control sobre ellos. Este derecho impone a terceros la realización u omisión de determinados comportamientos relacionados con los datos personales en:

- Su recogida, obtención y acceso.
- Su posterior almacenamiento y tratamiento.
- Su uso por terceros
- El conocimiento sobre quién dispone de ellos y a qué uso los está sometiendo.

En la actualidad, los medios tecnológicos, en concreto, los informáticos, han obligado a que se regulen los accesos a los datos de carácter personal y sanitarios, garantizando así la protección del derecho fundamental a la intimidad personal y familiar, recogido en el artículo 18.1 de la Constitución Española, de manera general y en su apartado 4 en lo relativo al uso de la informática.

Los datos de laboratorio, como parte de la historia clínica y como datos referentes a la salud, están por tanto especialmente protegidos, por lo que se deben adecuar las bases de datos a la Ley Orgánica de Protección de datos 15/1999 y a la Ley Básica sobre la Autonomía del Paciente 41/2002 de 14 de Noviembre.

Los laboratorios, están gestionados en general por un sistema único, con captura automatizada de solicitudes mediante impresos grafitados, emisión de informes en papel y acceso a resultados a través de la Intranet del Hospital.

Tanto los datos capturados del Host, los circuitos de informes, la accesibilidad de los resultados, la conservación de muestras y serotecas, los consentimientos informados, la eliminación de impresos e informes y la concienciación del personal, deben ser abordados con objeto de poder garantizar los derechos de los pacientes.

### **Impresos de Solicitud**

Los impresos de solicitud deben ser protegidos, como documentos de los que se pueden extraer datos referente a la salud y datos personales, contenidos en las etiquetas de identificación, obtenidas a su vez, de un archivo que sí está protegido, por lo que debemos extremar las precauciones para garantizar la preservación de los derechos constitucionales, a través de cuatro mecanismos: Recepción cuidadosa, utilización restrictiva, custodia adecuada y eliminación por destrucción.

### **Captura de datos**

La Ley Orgánica 15/1999 establece que los datos capturados deben ser de "calidad", es decir, deben ser adecuados, pertinentes y no excesivos en un

ámbito y finalidad determinadas, explícitas y legítimas para los que se hubieran obtenido.

Hay registros donde figuran datos personales, como teléfono, dirección..., que no son necesarios. Lo idóneo sería limitar la captura a los datos estrictamente necesarios para realizar con calidad nuestro trabajo.

### **Informes y consulta de datos**

Los datos de laboratorio, como parte integrante de la Historia Clínica, están sujetos al secreto profesional, lo que obliga a su acceso controlado. El sistema debe garantizar la seguridad de la información, es decir su integridad, disponibilidad y confidencialidad. Esto significa que los datos no se pierdan, que nadie pueda robarlos o manipularlos, que estén accesibles y que sólo sean consultados por las personas involucradas, de uno u otro modo, en la tarea asistencial.

Todo esto aconseja promover la correcta utilización de dicha herramienta y, en general, una mayor concienciación de los profesionales sobre el adecuado tratamiento de la información que los pacientes ponen en sus manos al abrigo de una confianza que no se pueden traicionar.

Por otra parte, los pacientes tienen derecho a acceder a sus datos analíticos, como datos objetivos, salvo los supuestos establecidos por la Ley 41/2002 de 14 de noviembre Art. 4.1 toda persona tiene derecho a que se respete su voluntad de no ser informada y Art. 5.4 limitarse la información a los pacientes por un estado de necesidad terapéutica llegado este caso el médico debe comunicar su decisión a las personas vinculadas al paciente y dejarlo reflejado en la H<sup>a</sup> Clínica.

Es muy importante considerar que los informes que se emiten a través de la intranet y en papel debe hacerse con suficiente control de acceso.

Se debería eliminar los informes que se realizan en soporte papel y extender el acceso electrónico, con las características adecuadas de seguridad.

### **Consentimiento informado**

Como desarrollo normativo de los derechos constitucionales, la Ley básica sobre la autonomía del paciente (41/2002) define, en su artículo 3 y desarrolla en sus artículos 8, 9 y 10 el consentimiento informado (CI), como el derecho incluido en el respeto a la autonomía del paciente. La ley permite un CI verbal por regla general, salvo en procedimientos diagnósticos invasores o de riesgo.

La extracción de sangre mediante venopunción, al no ser de riesgo, no necesita CI específico, pues por el hecho de acudir al laboratorio, se está consintiendo. Sin embargo, se debe facilitar información oral cuando la extracción no va a ser realizada de la forma habitual (P.E. yugular), y siempre

que el paciente la solicita. La punción medular y la lumbar si requieren consentimiento escrito.

Seria necesario solicitar el CI escrito cuando se pretenda usar los datos de un paciente para un fin diferente para el que fueron obtenidos, salvo su anonimización.

Por todo lo anteriormente expuesto surge la necesidad de que los centros se doten de Sistemas Seguros, entendiéndose por éstos aquellos que garanticen tres conceptos básicos:

- La confidencialidad.
- La integridad.
- La disponibilidad.

Este plan de seguridad deberá abarcar tres aspectos:

- Normas administrativo-organizativas.
- Normas lógicas.
- Normas físicas.

### ANÁLISIS

El derecho a la intimidad se muestra como uno de los derechos más frecuentemente vulnerados en la sociedad. La incursión en la vida de los demás es un hecho cotidiano en nuestra sociedad. Existe un interés desmedido por noticias que conlleven cierto morbo, circunstancia siempre presente en un proceso de enfermedad. Es frecuente asistir a todo tipo de comentarios en la calle, en las casas, incluso en los medios de comunicación.. Estamos acostumbrados a que los programas televisivos, la radio, y los rotativos, sensacionalistas o no, nos mantengan puntualmente informados del estado de salud de los personajes públicos.

La “cultura” de comentar lo que sólo a otros pertenece no se detiene en la puerta del hospital a pesar de que guardar secretos forma parte de la esencia de los códigos deontológicos de todas las profesiones sanitarias, ha dejado de ser un deber auto-impuesto por la ética profesional para convertirse en un mandato legal que emana del reconocimiento de la soberanía del paciente sobre su vida y su intimidad.

Así la “ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica” en su capítulo III, art. 7.1 dice **“Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la ley”**.

En el punto 7.2, la ley 41/2002 dice: **“Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refieren el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos que garanticen el acceso legal a los datos de los pacientes”**.

Intimidad deriva del superlativo “Intimus”, es decir, lo más interior del interior de cada persona.

Un hecho que recuerda la relevancia de la intimidad de las personas es que, así como la mayoría de los derechos se extinguen con la vida del individuo,

éste va más allá de la muerte. El difunto sigue teniendo derecho al honor y no por haber fallecido pueden hacerse públicas realidades personales que pudieran lesionarlo.

El desarrollo de un marco jurídico-normativo sobre la protección a la intimidad ha sido extraordinariamente intenso en los últimos años a nivel internacional, comunitario, estatal y autonómico. En diversas sentencias del tribunal Constitucional se recoge que: "El derecho a la intimidad personal es necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de vida humana". Ha habido también en nuestro país sentencias duras en este terreno: el Tribunal supremo condenó en el año 2002 a un médico residente por compartir con su madre datos de un paciente y

Una sentencia de la Audiencia Nacional anuló la Orden Ministerial de 18 de diciembre de 2000 que regulaba el funcionamiento del sistema de información sobre nuevas infecciones por VIH por considerar que no garantizaba de manera adecuada la intimidad de los interesados.

### **CONCLUSIONES**

Podemos concluir diciendo que la situación de la seguridad en los laboratorios sigue siendo una de las asignaturas pendientes de los mismos, en algunas ocasiones por falta de recursos económicos, que no permite implantar el software necesario para el nivel de seguridad alto, en sus sistemas de información; en otras ocasiones, la falta de medidas de seguridad viene atribuida al factor humano.

Las medidas de seguridad que tienen que implantarse comienzan por la definición del documento de seguridad del laboratorio, que contendrá las medidas de nivel básico, medio, y alto de aplicación a los ficheros; además ha de ser siempre un documento completo y adaptado a la situación real.

Todas las personas que integran el laboratorio tienen que conocer con exactitud sus funciones y obligaciones, las normas de seguridad que les afectan y las consecuencias que vayan a derivarse de su cumplimiento.

Frecuentemente aparecen casos en que los historiales de los pacientes se descubren entre la basura de un hospital, con los datos perfectamente identificados. De este modo, al desechar la información en soporte papel deberá procederse a su destrucción, impidiendo que pueda ser recuperada.

En relación con las copias de seguridad, se aconseja que se realicen en distintos soportes, de forma que se utilicen alternativamente, pudiendo asegurar de este modo la recuperación de los datos cuando se detecte una pérdida. Además esta copia en ningún momento podrá situarse dentro del laboratorio.

Se debería designar un responsable de seguridad, ya que normalmente nadie quiere asumir dicho cargo, debido a la creencia de que están asumiendo una mayor responsabilidad dentro del centro; sin embargo, su designación no supone una delegación de la responsabilidad del laboratorio, sino que

únicamente el que sea nombrado para tal cargo se dedicará a controlar las medidas de seguridad que se hayan definido.

Las personas que trabajan en el laboratorio han de disponer además de mecanismos que les permitan estar perfectamente identificadas en los sistemas, de modo que la dirección del laboratorio pueda conocer en que momento y a qué tipo de información ha tenido acceso un usuario, así como el tratamiento que ha realizado de esa información, recomendando además que su deber de secreto se encuentre regulado mediante la firma de un compromiso de confidencialidad.

Los riesgos más comunes en los laboratorios son la entrega de resultados o su envío a través de redes de telecomunicaciones como el fax, internet, etc. En el caso del correo electrónico, existen herramientas que permiten la encriptación, pero ello obliga a que el destinatario disponga del mismo programa y conozca la clave de desencriptación; o en su caso, también podría optarse porque ambos, emisor y receptor, dispongan de firma electrónica.

Las medidas de seguridad que he descrito no son todas las que deberían aplicarse, pero sí que constituyen una aproximación a la obligación legal de la seguridad para todos los responsables de ficheros con datos de carácter personal.