

## La Ley de Protección de Datos. ¿Cómo nos afecta a los médicos?

### LA LEY DE PROTECCIÓN DE DATOS:

#### ¿ COMO NOS AFECTA A LOS MÉDICOS?

*El próximo día 22 de Junio de 2002, finaliza la prórroga prevista en el Real Decreto 994/99 de 11 de Junio, por el que se aprueba el Reglamento de Medidas de Seguridad de ficheros automatizados que contengan Datos de Carácter Personal.*

*De éstos datos, por sus características, están especialmente tratados por la legislación, los datos RELATIVOS A LA SALUD DE LAS PERSONAS, y por ello, con el fin de salvaguardar el derecho constitucional a la intimidad, la confidencialidad de los mismos, está especialmente protegida por la Ley.*

*Con éste objetivo, el mencionado Real Decreto 994/99, establece una serie de medidas de protección, que afectan especialmente a los datos sobre nuestros pacientes, que habitualmente manejamos en nuestra práctica clínica diaria, y por lo tanto nos obliga a implantar una serie de medidas encaminadas a la protección de los mismos, y CUYO INCUMPLIMIENTO PODRÍA ACARREAR MULTAS DE HASTA CIEN MILLONES DE PESETAS*

#### **Origen de éstas medidas.**

Como consecuencia del gran desarrollo de la informática a todos los niveles, y su capacidad de almacenar y transmitir grandes cantidades de información, con los más diversos fines, se vió la necesidad de preservar el derecho a la intimidad de las personas, frente a la amenaza que éstas tecnologías podrían suponer al respecto.

Con el objetivo de preservar el derecho de los ciudadanos a la intimidad personal, recogido en nuestra Constitución, se han ido promulgando diversas leyes y normativas encaminadas a éste fin, de las que conviene destacar la Ley Orgánica 5/92, que limita el uso de la informática en lo referente al tratamiento y difusión de datos de carácter personal, modificada y ampliada por la posterior Ley Orgánica 15/99, que aplica la Directiva 95/46 de la CEE a nuestro derecho interno. Posteriormente, el Real Decreto 994/99, al que ya hemos hecho referencia, desarrolla esta última, y establece una serie de medidas de obligado cumplimiento, encaminadas a la protección de éstos datos.

Se creó en base a ésta legislación, la Agencia de Protección de Datos, como organismo encargado de velar por el estricto cumplimiento de éstas normativas, y como garante del derecho de los ciudadanos, a la protección de los datos referentes a su persona.

El mencionado Real Decreto 994/99, clasifica los diversos datos relativos a las personas, y considera que precisan de una PROTECCIÓN DE NIVEL ALTO, :

*3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, **salud** o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto. (R.D. 994/99, Art.4º. 3).*

### **¿A qué datos nos referimos?**

De acuerdo con lo enunciado en éste artículo, el legislador se refiere claramente, a los ***datos contenidos en la Historia Clínica*** de nuestros pacientes, por lo tanto, ésta normativa afecta de lleno a cualquier consulta privada, clínica, hospital, centro ó empresa, que disponga en sus ordenadores en los que se guarden ficheros con éste tipo de datos, y por tanto nos OBLIGA a disponer de las medidas de protección previstas por la Ley, y que afectan tanto al personal Facultativo, como no facultativo, que por razón de su trabajo deba acceder a éstos datos.

### **Medidas a implantar:**

Es preciso por tanto establecer una serie de mecanismos encaminados a salvaguardar la SEGURIDAD y la CONFIDENCIALIDAD de nuestros ficheros de pacientes, no excesivamente complejos, pero sí suficientes para garantizar esto, estableciendo:

- Un mecanismo de custodia activa y diligente
- Una política de confidencialidad en cuanto a
  - Recogida
  - Almacenamiento
  - Tratamiento
  - Transmisión de los datos
- Limitación de acceso a los datos por terceros
- Garantía del derecho de acceso por el propio paciente
- Responsabilidad de la custodia
- Mantenimiento de la calidad de los datos (actualización)

### **Requisitos de los ficheros de datos sanitarios:**

El especial tratamiento que concede la Ley a éste tipo de datos, nos obligan, a configurarlos y mantenerlos con una serie de requisitos imprescindibles:

- Siempre debemos contar con el consentimiento expreso del afectado (nuestro paciente), y mejor por escrito, ya que no es válido el consentimiento tácito.
- Es preciso informar al afectado (consentimiento informado)
- Siempre hay que respetar el derecho de nuestros pacientes al acceso, rectificación, cancelación y oposición, respecto al almacenamiento de sus datos.
- Es obligatorio inscribir los ficheros en el registro de la Agencia de Protección de datos
- Estamos obligados a mantener una calidad en los datos de nuestros ficheros, y por tanto a actualizarlos.
- Estamos obligados a establecer las medidas precisas de seguridad para el acceso a nuestros ficheros de datos, especialmente las de nivel medio y alto.
- Estamos obligados a mantener la confidencialidad de nuestros datos, mediante las medidas oportunas.

### **El problema de Internet**

Por su propia filosofía, Internet es una red abierta, y por lo tanto, a menos que apliquemos una serie de medidas específicas, INSEGURA. Es decir que los datos de nuestros pacientes que enviemos a través de Internet, a menos que adoptemos una serie de medidas de seguridad, están expuestos a que puedan ser interceptados por terceros, y accedidos, difundidos o publicados, sin nuestro consentimiento ni nuestro conocimiento, pero ello no nos eximiría de nuestra responsabilidad. (Art. 26 R.D.994/99)

Por ello es preciso ser muy cautos en cuanto a la transmisión de datos de pacientes a través de Internet (esa historia que le mandamos a nuestro colega de Barcelona para recabar una segunda opinión), y adoptar mecanismos de encriptación de ficheros y firma digital de los mismos, de manera que los datos solamente puedan ser leídos por el destinatario, e interpretados como provenientes de nuestro propio ordenador.

Existen programas de uso gratuito que permiten ésta facilidad, de uso muy sencillo, y los legisladores están empezando a adoptar una posición activa a éste respecto, es decir que en breve, nos encontraremos con leyes que nos obliguen a adoptar éstas precauciones.

En otro artículo comentaremos más a fondo éste tipo de aplicaciones.

### **¿Cómo consigo la legalidad de mis ficheros de pacientes?**

De acuerdo con lo dispuesto en la legislación antes mencionada, debo cumplir una serie de requisitos, encaminados a:

- Respetar los principios básicos de la Protección de datos
- Respetar las normativas específicas para el Sector Sanitario
- Realizar auditorías periódicas de Protección de Datos, y obligatoriamente cada DOS AÑOS.
- Elaborar un informe de Auditoría y un Documento de Seguridad
- Implantar las medidas de seguridad de NIVEL ALTO, previstas en el R.D. 994/99.
- Informar y formar en éste sentido al personal que por su actividad deba tener acceso a los ficheros de datos.
- Concienciarse de la importancia de la protección de los datos sanitarios.

### **¿Qué debo hacer antes del 22 de Junio?**

De acuerdo con lo establecido en la Disposición Transitoria Única, del R.D. 994/99, antes de la fecha mencionada, debo haber implantado las medidas de protección de datos de nivel alto siguientes.

- Cifrado de los datos, ó utilización de mecanismos que imposibiliten el acceso ó manipulación de la información.
- Mantenimiento de un registro que informe de todas las personas que accedan a los datos.
- Elaboración de un plan mensual de revisiones periódicas de la información de control y problemas detectados.
- Copia de respaldo y copia de los procedimientos de recuperación de datos, custodiada en lugar distinto al lugar de ubicación de los equipos informáticos.
- Una auditoría, interna ó externa, que verifique el cumplimiento del Reglamento de Protección de Datos.
- Elaborar un documento de seguridad, de acuerdo a lo dispuesto en el R.D.

### **¿Quién puede hacerme esto?**

Poner en funcionamiento éstas medidas, en el caso de pequeñas consultas, con un solo ordenador, y una sólo persona que acceda a los datos, puede ser relativamente sencillo, si se es algo hábil en el manejo de la informática, y siguiendo los pasos establecidos en el Rd.

No obstante, en el caso de centros de mayor importancia, con varios ordenadores, y diferentes accesos de distintas personas, habitualmente precisaremos del concurso de alguna empresa especializada, ya que se trata de implantar medidas tanto legales, como técnicas.

Es probable que el Colegio pueda llegar a algún acuerdo con alguna de éstas empresas, en condiciones ventajosas para los Colegiados, y además en el mercado existen multitud de empresas dedicadas a la seguridad informática, a las que recurrir.

### **Conclusión**

Evidentemente, la implantación de estas medidas nos van a suponer un coste, pero hay que verlo como un valor añadido en cuanto a garantías de seguridad y confidencialidad que le vamos a dar a nuestros pacientes, confidencialidad y seguridad a la que de acuerdo con el espíritu de la ley tiene perfecto derecho.

Por otra parte, habría que consultar en cada caso, con nuestra asesoría jurídica, si la puesta en marcha de éstas medidas y el coste que suponga, tienen algún tratamiento fiscal ventajoso para nuestros profesionales.

### **Referencias legislativas y legislación relacionada:**

Ley 14/1986, General de Sanidad

Ley 25/1990, del Medicamento

Ley Orgánica 5/1992 sobre Regulación del tratamiento automatizado de datos.

DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

LEY DE INCORPORACION AL DERECHO ESPAÑOL DE LA DIRECTIVA 96/9/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 11 DE MARZO DE 1996, SOBRE LA PROTECCION JURIDICA DE LAS BASES DE DATOS

INSTRUCCIÓN 1/1998, DE 19 DE ENERO, DE LA AGENCIA DE PROTECCIÓN DE DATOS, RELATIVA AL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN Y CANCELACIÓN.

Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal

Real Decreto 994/99 de 11 de Junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

REAL DECRETO 195/2000, DE 11 DE FEBRERO, POR EL QUE SE ESTABLECE EL PLAZO PARA IMPLEMENTAR LAS MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS PREVISTAS POR EL REGLAMENTO APROBADO POR EL REAL DECRETO 994/1999, DE 11 DE JUNIO

CATALUÑA: Ley 21/2000 de 29 de Diciembre sobre los derechos de información concerniente a la salud y la autonomía del paciente y a la documentación clínica.

GALICIA: Ley 3/2001 de 28 de Mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes