A fondo ...

Protección de Datos de Carácter Personal en el ámbito de la Psicología

La legislación sobre protección de datos de carácter personal tiene como fin salvaguardar el derecho fundamental de los ciudadanos a controlar el uso que se hace de sus datos. En la actual sociedad de la información se hace particularmente importante la protección de este derecho, ya que las nuevas tecnologías, aun teniendo elementos indudablemente positivos para la eficacia administrativa y para el desarrollo económico, y siendo además un instrumento importante para mejorar la calidad asistencial que se ofrece, conllevan también riesgos para la privacidad de las personas. En el caso de la Psicología, al recogerse datos que afectan de lleno a la esfera más personal e íntima del individuo, un mal tratamiento de estos datos puede atentar gravemente contra la intimidad personal de los pacientes.

En las siguientes líneas se tratará de mostrar cómo puede afectar esta normativa al desarrollo de las actividades diarias de los psicólogos.

La Ley de Protección de Datos de Carácter Personal 15/1999 de 13 de diciembre (en adelante LOPD), impone una serie de obligaciones legales para aquellos profesionales que traten con datos de carácter personal.

El RD 994/99 de 11 de junio, desarrolla la mencionada Ley Orgánica y establece una serie de medidas destinadas a garantizar la protección de los datos.

Los psicólogos manejan generalmente datos considerados de carácter personal. Cuando lo hacen por cuenta propia, son responsables de su tratamiento y tienen obligación de adaptarse a la LOPD.

Es de vital importancia adecuarse a la normativa de protección de datos, ya que la LOPD establece una serie de infracciones, calificadas como leves, graves o muy graves, que suponen sanciones que van desde 600 € hasta 600.000 €. Estas sanciones son fáciles de evitar, tomando las siguientes medidas para adaptarse a las exigencias legales.

Principales obligaciones de los profesionales en materia de protección de datos

1. Inscripción de los ficheros de datos personales en el Registro General de la Agencia Española de Protección de Datos (en adelante AGPD).

Se refiere tanto a ficheros integrados en sistemas informáticos, como a ficheros manuales que puedan estar archivados en armarios, cajones o estanterías, siempre que los datos se encuentren estructurados (organizados) por algún criterio que permita acceder con facilidad a los datos de una persona.

Fichero: Conjunto organizado de datos de carácer personal, cualquiera que fuere la forma o modalidad de su creación almacenamiento, organización o acceso.

No se trata de comunicar a la AGPD los datos, sino de informar del tipo de datos que se manejan, por ejemplo "nombre", "dirección postal", "dirección correo electrónico" de los pacientes atendidos en consulta. Por tanto, el primer paso es identificar los ficheros que se manejan para después determinar el nivel de seguridad aplicable. En un centro psicológico, podrían existir ficheros del tipo:

"Historia clínica" con los datos de los pacientes, que al contener datos de salud, tendría un nivel de seguridad alto, y habría que aplicarle las medidas de seguridad correspondientes.

"Personal contratado", que también exigiría un nivel de seguridad alto, si contiene datos relativos a la salud, discapacidad, afiliación sindical de los trabajadores, etc.

"Gestión de citas" sería un fichero de nivel de seguridad básico al contener datos como nombre, dirección, teléfono, para organizar las citas.

Estos son tan sólo algunos ejemplos de posibles ficheros. En cada caso se debe-

rán analizar los datos que se recogen para hacer un inventario de los ficheros utilizados y su nivel de seguridad (ver tabla de niveles de seguridad).

2. Recoger y tratar adecuadamente los datos.

Hay que informar a las personas a las que se les solicitan datos de los siguientes puntos:

a. El nombre del fichero en el que se van a almacenar sus datos.

b. La finalidad de la recogida de datos.

c. El destinatario.

d. El carácter obligatorio o facultativo (opcional) de su respuesta.

e. Las consecuencias de la obtención de los datos o de su negativa a suministrarlos.

Los formularios, o cualquier otro elemento o procedimiento utilizado para la recogida de los datos, debe adecuarse al principio de calidad de los datos, es decir, no se deben contemplar datos excesivos o no necesarios, debe tener una finalidad determinada, explícita y legítima, y ser adecuado, para dicha finalidad.

Si la información se recoge a través de conversación telefónica hay que informar de los puntos anteriores al principio de la conversación.

3. Informar sobre la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación de los datos.

Facilitando a las personas que lo soliciten la posibilidad de ejercerlo así como la dirección dónde hacerlo, de forma totalmente gratuita y en unos plazos determinados. Estos derechos sólo pueden ser ejercidos por el propio interesado.

Derecho de Acceso: el usuario tiene derecho a solicitar información sobre los datos de carácter personal que estén siendo sometidos a tratamiento por el psicólogo, el origen de los datos y si han sido comunicados a terceros.

Derecho de Rectificación: el usuario puede solicitar que se rectifiquen su datos, por ser erróneos o incompletos.

Derecho de Cancelación: cuando el titular de los datos tiene conocimiento de que los datos tratados en un fichero no se ajustan a la LOPD, puede solicitar la cancelación de los mismos.

Derecho de Oposición: en los casos en que no es necesario el consentimiento del interesado para tratar los datos, como por ejemplo en el caso de los datos profesionales de una persona, éste podrá oponerse al tratamiento de los datos cuando existan motivos fundados y legítimos.

4. Redactar un documento de seguridad.

En el que se especifiquen las medidas de seguridad adoptadas por el profesional en función del nivel de seguridad que requiera el tipo de datos recogidos. La LOPD determina tres niveles de medidas de seguridad, BÁSICO, MEDIO y ALTO, los cuales han de ser adoptados en función de los distintos tipos de datos que se manejen. En un documento de seguridad se debe incluir:

- Ámbito de aplicación.
- Medidas, normas, procedimientos encaminados a garantizar los niveles de seguridad.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal, incluyendo una descripción del sistema de información.
- Procedimiento de notificación de incidencias.
- Procedimientos de realización de copias de respaldo.

Hay que adoptar las medidas técnicas y de organización necesarias para garantizar la seguridad de los datos, tanto para los ficheros informáticos como para los manuales. Respecto a los ficheros informatizados, en la tabla de niveles de seguridad aparecen las medidas de seguridad que hay que tomar según el nivel de seguridad del fichero. En cuanto a los ficheros manuales se pueden adoptar medidas de seguridad básicas como las siguientes:

- Romper cualquier papel que contenga datos personales antes de tirarlo a la papelera.
- Establecer procedimientos para desechar papel, garantizando la confidencialidad de los datos.
- No dejar expedientes en una mesa cuando se va a producir una ausencia del puesto de trabajo, guardándolos por ejemplo en un cajón o armario con llave.

Cualquier historia clínica de un paciente contiene datos de un nivel de seguridad alto. La Agencia de Protección de Datos de la Comunidad de Madrid recomienda las siguientes medidas para la custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas:

- Las medidas de seguridad del centro deberán garantizar la confidencialidad de los datos contenidos en el fichero y evitar accesos no autorizados, controlando quién está utilizando la historia desde la salida del fichero hasta su devolución, estableciendo por ejemplo un registro de entrada/salida de historias clínicas. Estas medidas se documentarán por escrito y se darán a conocer al personal.
- El profesional asistencial que realiza el diagnóstico o el tratamiento tiene que tener acceso a la historia clínica completa, como instrumento para su adecuada asistencia, pero el personal de administración y gestión del centro sólo tendrá que acceder a los datos de la historia clínica relacionados con sus propias funciones, como cita previa, funciones contables, control de proveedores, etc. Se recomienda archivar por separado la documentación que forma parte de la historia clínica de toda la documentación administrativa.

- Controlar a las personas ajenas a la empresa, como personal de limpieza o mantenimiento, que deberán acceder en horarios de trabajo del centro.

Estas son sólo algunas de las recomendaciones a tener en cuenta. Para ampliar información sobre historias clínicas o sociales puede consultar la página web de la Agencia de Protección de Datos de la Comunidad de Madrid (www.madrid.org/apdcm).

Niveles de Seguridad

NIVEL BASICO

Es de nivel básico cualquier fichero con datos identificativos, como nombre, apellidos, DNI, etc., características personales, como estado civil, edad, fecha nacimiento, etc., circunstancias sociales, como tipo de vivienda, servicio militar, etc., datos académicos y profesionales, empleo, información comercial (por ejemplo un fichero "proveedores" con nombre, dirección, NIF, datos de información comercial, económicos), etc.

Medidas a aplicar:

- Elaborar un documento de seguridad con las medidas adoptadas.
- Llevar un registro de incidencias (por ejemplo, robo de ordenador con datos personales).
- Identificación y autenticación[2]. Establecer algún método para saber quién accede a los datos (contraseñas, perfiles de usuarios, para saber dónde puede acceder cada miembro del personal).
- Control de acceso lógico[3]. Hay que controlar quién accede y cuándo a los datos en el ordenador.
- Gestión de soportes[4] . Hay que controlar qué disquetes, CDs, etc., con datos salen o entran de las instalaciones.
- Copias de respaldo y recuperación (copias de seguridad).
- Determinar e informar de las funciones y obligaciones del personal.

NIVEL MEDIO

Los datos de nivel básico lo son si permiten establecer un perfil de la persona, de solvencia patrimonial, de hacienda pública, infracciones.

Medidas a aplicar:

Además de las básicas, se añaden:

- Determinar un Responsable de Seguridad que coordinará y controlará las medidas de seguridad.
- Control de acceso físico al espacio de almacenamiento de los datos (por ejemplo guardar bajo llave las historias clínicas), para que sólo pueda acceder el personal autorizado.
- Auditorias bianuales (se recomienda que sean externas).
- No realizar pruebas con datos reales, a no ser que se asegure el nivel de seguridad.

NIVEL ALTO

Se refiere a ficheros con datos especialmente protegidos como ideología, creencias, salud, religión, origen racial, afiliación sindical o vida sexual, como los ficheros con la historia clínica o social, o fichero de personal que puede contener datos de afiliación sindical o salud.

Medidas a aplicar:

A las anteriores, se añade:

- Llevar un registro de acceso lógico, de quién accede y cuándo a los datos. Los sistemas operativos actuales gestionan este tipo de tareas.
- Cifrado[5] de los mensajes de correo electrónico, para impedir su lectura por terceras personas.

5. Garantizar todos los aspectos anteriormente mencionados cuando el tratamiento de los datos sea realizado por un tercero por cuenta nuestra (subcontratación de servicios), redactando y aplicando cláusulas específicas sobre protección de datos en los contratos (por ejemplo, cuando se contrata a una empresa para que realice envíos de correspondencia o tramite las nóminas de los trabajadores).

Plazos para adaptarse a la LOPD

Todos los ficheros de datos de carácter personal, automatizados o no, creados después de la entrada en vigor de la Ley, deben adecuarse a la normativa a partir del 14/01/00. Para los datos que existían antes de la entrada en vigor de la ley, el plazo para adecuarse se amplió hasta el 14/01/03 en el caso de los ficheros automatizados, y hasta el 24/10/07 en el caso de los ficheros manuales.

Siempre se deberá facilitar el derecho de acceso, rectificación y cancelación por parte de las personas cuyos datos están incluidos en los ficheros manuales, incluso aunque éstos no estén registrados en la AGPD.

La información aquí recogida no pretende ser exhaustiva, es un bosquejo de cómo puede afectar la LOPD al desarrollo de las actividades diarias de los psicólogos. Se puede ampliar esta información y acceder a modelos e instrucciones para inscribir los ficheros y adaptarse a la LOPD, consultando la zona privada para colegiados en la página Web del Colegio (www.copmadrid.org)

También se puede ampliar esta información en la página web de la Agencia Española de Protección de Datos (www.agpd.es) y de la Agencia de Protección de Datos de la Comunidad de Madrid (www.madrid.org/apdcm) donde, además de modelos de documentos de seguridad, documentación, consultas y recomendaciones sobre protección de datos en general, se encuentra información sobre archivo, uso y custodia de historias clínicas y sociales no informatizadas.

Las dudas de los colegiados en materia de protección de datos serán atendidas a través del correo electrónico: prot_datos@cop.es.

M.ª Dolores Manzano

1 **Datos de Carácter Personal:** Cualquier información concerniente a una persona física que, combinada o por sí misma, permita conocer a una persona concreta, desde el nombre, correo electrónico, DNI, etc, hasta datos de salud.

2 **Identificación y autentificación:** Reconocimiento y comprobación de la identidad de la persona que accede a los datos.

3 **Control acceso lógico:** Mecanismo que, en función de la identificación ya autenticada, permite acceder a los datos.

4 **Soportes:** Objeto físico susceptible de ser tratado en un sistema de información (programa, equipos) y sobre el cual se puede grabar o recuperar datos.

5 **Cifrado:** Transformación de un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que desconocen la clave.