PLAN DE SENSIBILIZACIÓN EN MATERIA DE PROTECCIÓN DE DATOS

Especialmente dirigido a
Personal Sanitario y
Administrativo del
Servicio Andaluz de Salud

martes, 24 de enero de 2012

PLAN DE SENSIBILIZACIÓN EN MATERIA DE PROTECCIÓN DE DATOS

ÍNDICE

INTRODUCCIÓN: La LEY

La Ley Orgánica de Protección de Datos 15/99 y el Reglamento de medidas de seguridad 1720/07, obligan a los responsables de los ficheros del Servicio Andaluz de Salud (Dirección-Gerencia, Secretaría General, Dirección General de Asistencia Sanitaria, Dirección General de Personal y Desarrollo Profesional y Dirección General de Gestión Económica) **a adoptar las medidas necesarias para que el personal que use los sistemas de información conozca las normas que afecten al desarrollo de sus funciones**. (Artículos 88.1 y 89.2 - RD 1720/2007).

Artículo 88. *El documento de seguridad.*

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los si

Artículo 89. *Funciones y obligaciones del personal.*

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

INTRODUCCIÓN: El Plan de Sensibilización - Objetivo

Los contenidos del PLAN, distribuidos por perfiles profesionales, se centran en el cumplimiento de la **Ley Orgánica de Protección de Datos**, la aplicación su **Reglamento de Desarrollo**, la **Ley de Autonomía del Paciente**, el conocimiento del **Manual del Empleado Público** de la Junta de Andalucía en el uso de los sistemas informáticos y redes de comunicaciones, así como la difusión de las **Instrucciones Internas** de la organización relacionadas con estas materias.

INTRODUCCIÓN: El Plan de Sensibilización - Objetivo

El objetivo principal es la sensibilización del 100% de la plantilla del SAS del 2008 al 2011, por lo que este tercer año se pretende alcanzar el 75%. Para ello se procederá a recabar la firma del alumnado como justificante de asistencia.

Esta presentación cubre el módulo de formación denominado:

- Sensibilización en materia de protección de datos (LOPD), 10/2033/0929/GE/P/AI

INTRODUCCIÓN: El Plan de Sensibilización - Coordinación

La coordinación y ejecución del PLAN se realiza desde la **Subdirección de Tecnologías de la Información** de la Secretaría General del SAS, a través de la **Unidad de Gestión de Riesgos Digitales**.

Esta Unidad lleva a cabo las siguientes actuaciones en materia de protección de datos:

- Plan de Auditorías
- Plan de Sensibilización de Centros
- Coordinación de los ejercicios de derechos de la LOPD
- Adecuación a la LOPD de los proyectos de Tecnologías de la Información
- Definición de Políticas y Procedimientos del SAS.
- Elaboración y actualización del Documento de Seguridad.
- Inspecciones de la Agencia Española de Protección de Datos.
- Inspecciones de la Consejería de Justicia y Administración Pública.

INTRODUCCIÓN: Contenidos implícitos de la sesión

- **Obligaciones** de la LOPD 15/99, RD 1720/07, LAP 41/02, M.C.E.P.
- **Instrucciones** Internas del SAS.
- **Consentimiento informado** en materia de protección de datos.
- Circuito de **incidencias, registros y acceso** a la información
- Ejercicio de los **derechos** de acceso, rectificación y cancelación.
- **Deberes del personal** en materia de protección de datos y seguridad.
- Documento de Seguridad de la información corporativa del SAS.

Estos contenidos serán expuestos como Casos Prácticos

TERMINOLOGÍA:

- **Datos de Carácter Personal:** cualquier información concerniente a personas físicas identificadas o identificables.
- **Fichero:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Tratamiento de datos:** operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- **Cesión o comunicación de datos:** toda revelación de datos realizada a una persona distinta del interesado.
- **Consentimiento:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

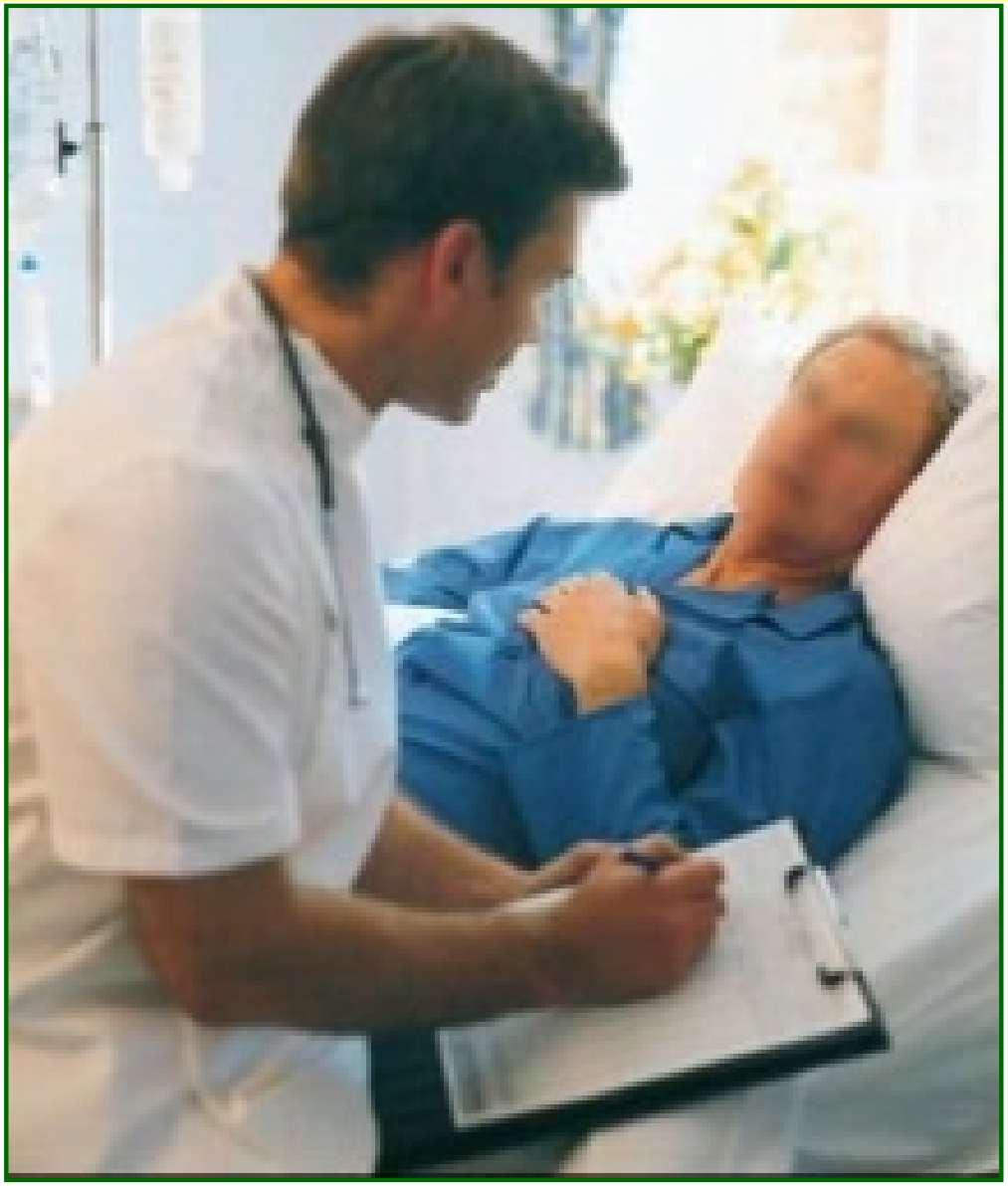
ACTORES:

Es importante reconocer las siguiente figuras que se recogen en el Documento de Seguridad del SAS.

- **Responsable del Fichero:** Director Gerente del SAS, Direcciones Generales y Directores de Centros.
- **Responsable de Seguridad:** Responsables de Tecnologías de la Información.
- **Responsable Funcional de Aplicación:** Directores, Subdirectores y Jefes de Servicio.

CASO PRÁCTICO 1: Publicación de fotografías

Un profesional de un centro hospitalario está pensando en hacer una publicación que contiene una foto donde aparece dicho profesional junto a un paciente encamado, en la foto se aprecia claramente el rostro de éste último.



CASO PRÁCTICO 1: Publicación de fotografías

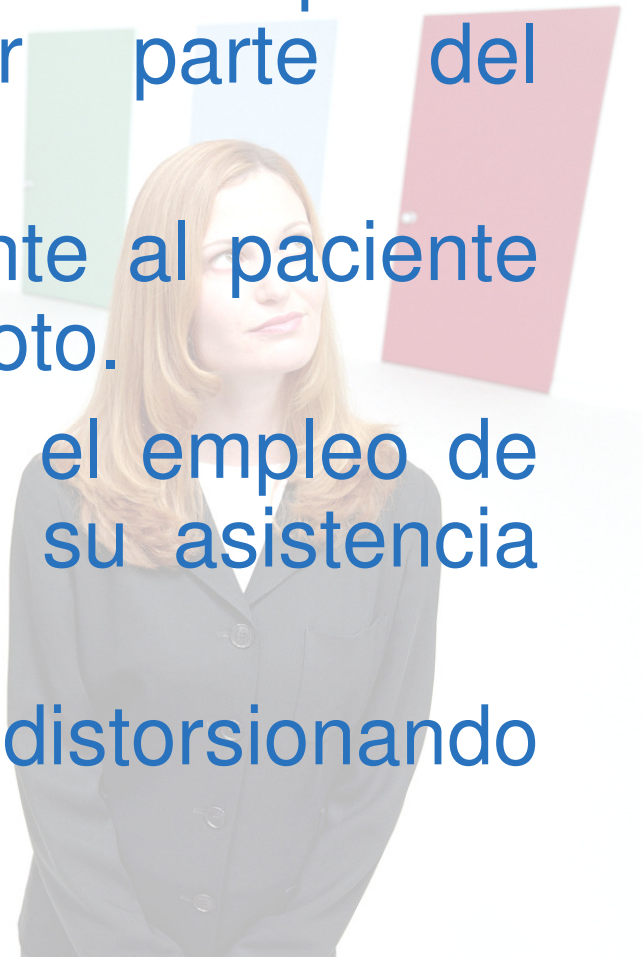
Opciones:

a) Se trata de un procedimiento habitual que no implica acción adicional por parte del profesional.

b) El profesional advierte verbalmente al paciente sobre su intención de publicar la foto.

c) El paciente consiente por escrito el empleo de dicha foto para fines distintos a su asistencia sanitaria.

d) El profesional hace uso de la foto distorsionando el rostro del paciente.



CASO PRÁCTICO 1: Publicación de fotografías

Dudas del profesional:

- **¿Quién me puede asesorar sobre cómo debo actuar?**
  El Responsable de Seguridad

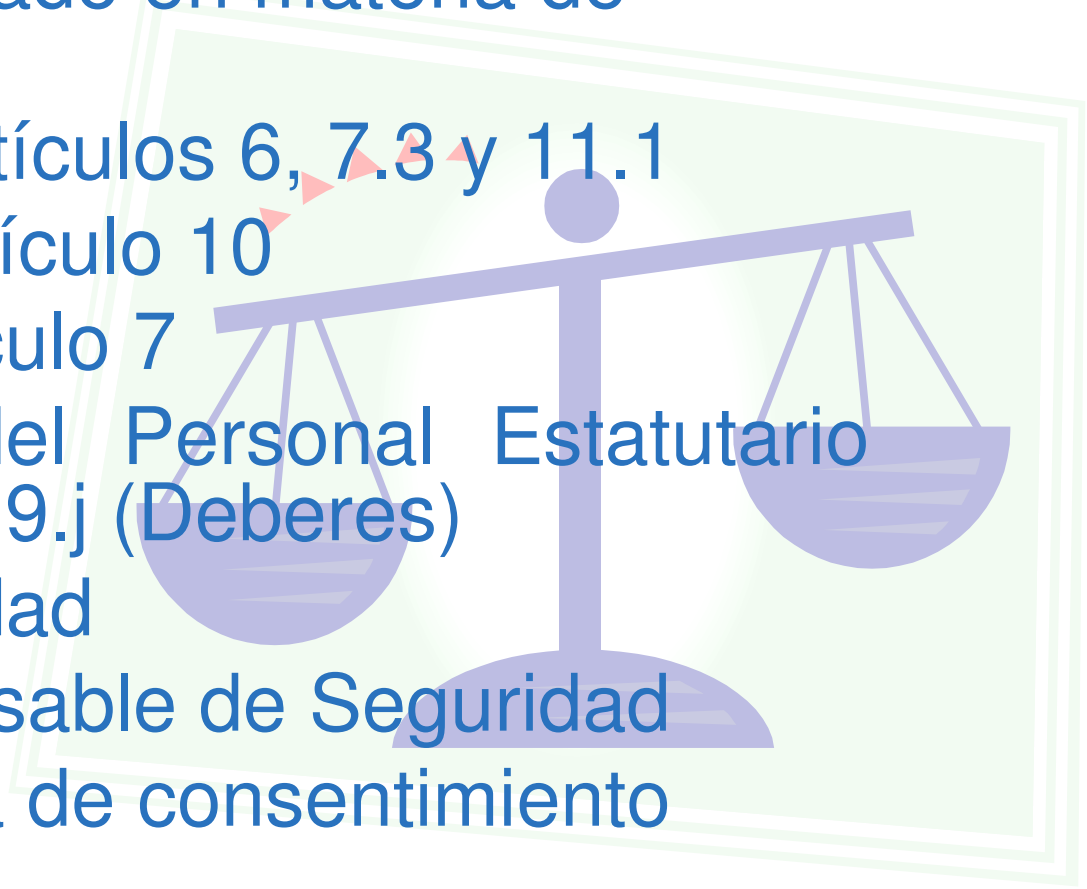
- **¿Dónde se encuentra el documento/plantilla de consentimiento/autorización que debo emplear?**
  En el Documento de Seguridad

- **¿Puedo usar imágenes del centro hospitalario libremente?**
  Normativa del centro sanitario

CASO PRÁCTICO 1: Publicación de fotografías

Normativa aplicable:

- Consentimiento informado en materia de protección de datos
  - LOPD 15/1999. Artículos 6, 7.3 y 11.1
  - RD 1720/2007. Artículo 10
  - LAP 41/2002. Artículo 7
  - Estatuto Marco del Personal Estatutario 55/2003. Artículo 19.j (Deberes)
- Documento de Seguridad
  - Figura del Responsable de Seguridad
  - Anexo con plantilla de consentimiento



CASO PRÁCTICO 1: Publicación de fotografías

Casos similares:

- Uso no asistencial de la radiografía de un paciente.
- Empleo de DCP de pacientes/profesionales para investigación, congresos, etc.
- Envíos publicitarios empleando DCP de la Historia Clínica o Contrato.
- Acceso a la Historia Clínica de un paciente por un médico no involucrado en su diagnóstico o tratamiento.
- Publicación web (centros, servicios, laboratorios, …) de DCP.
- Exposición de DCP por megafonía o pantallas de información públicas.
- Envíos de e-mails conteniendo direcciones de correo de personas distintas al destinatario.
- Cesión de DCP a terceros (consultoras, laboratorios, …) para su tratamiento.

CASO PRÁCTICO 1: Publicación de fotografías

Resumen:

Conceptos que hay que tener muy claros:

- Ante cualquier duda sobre el tratamiento de información, consultar al **Responsable Funcional de Aplicación o al Responsable de Seguridad**.
- Distinguir cuando se hace un **uso acorde a la finalidad** declarada de los datos de carácter personal.
- Los datos de carácter personal son **propiedad de su titular**, no de quien los custodia.
- El Responsable del Fichero debe **autorizar cualquier uso extraordinario de los datos**.
- El consentimiento y otros anexo interesantes está disponible en el **Manual de Seguridad Corporativa del SAS**.

CASO PRÁCTICO 1: Publicación de fotografías

Casos real:

EN DIRECTO OIR hora 14

CADENA SER .COM

Inicio | La SER | Noticias | Deportes | Escucha | Participa | El pulsómetro | Vídeos nuevo | Widgets

Estas en: Cadenaser.com » Noticias

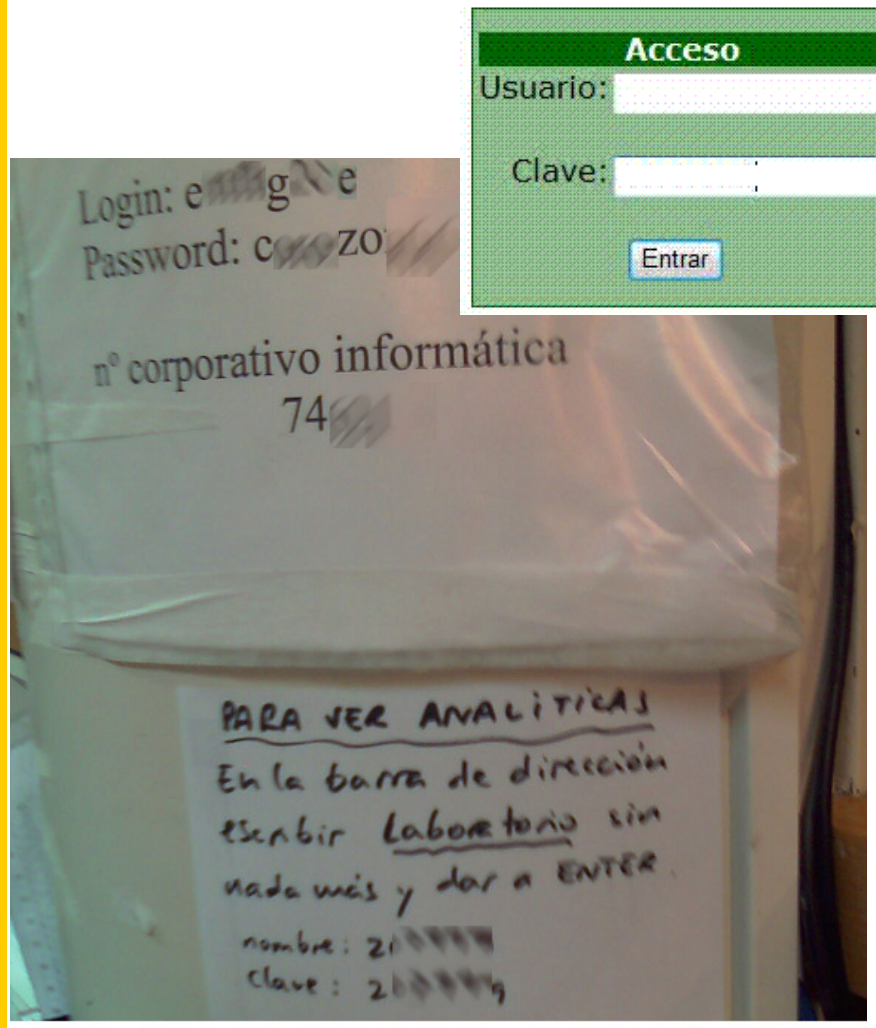
Sancionados por difundir imágenes tomadas en la calle

La Agencia Española de Protección de Datos ha sancionado por primera vez la grabación y posterior difusión de imágenes a través de YOUTUBE, tomadas el pasado octubre en la calle Montera de Madrid

CADENA SER/ AGENCIAS 22-07-2008

La Agencia Española de Protección de Datos (AEPD) ha multado con **601 euros** a los responsables de la grabación y publicación en el portal de vídeos "Youtube" de unas imágenes en las que se podía ver a una serie de personas mientras transitaban por la calle de Montera tras la investigación iniciada de oficio el pasado mes de octubre por la captación y difusión de imágenes de la citada vía.

CASO PRÁCTICO 2: Acceso a los Sistemas de Información



Un profesional de un centro sanitario que se ha incorporado recientemente pretende que su compañero de trabajo le diga su usuario y contraseña para poder entrar en el sistema informático. Este profesional se ha incorporado al trabajo y aún no dispone de usuario y contraseña de acceso.

CASO PRÁCTICO 2: Acceso a los Sistemas de Información

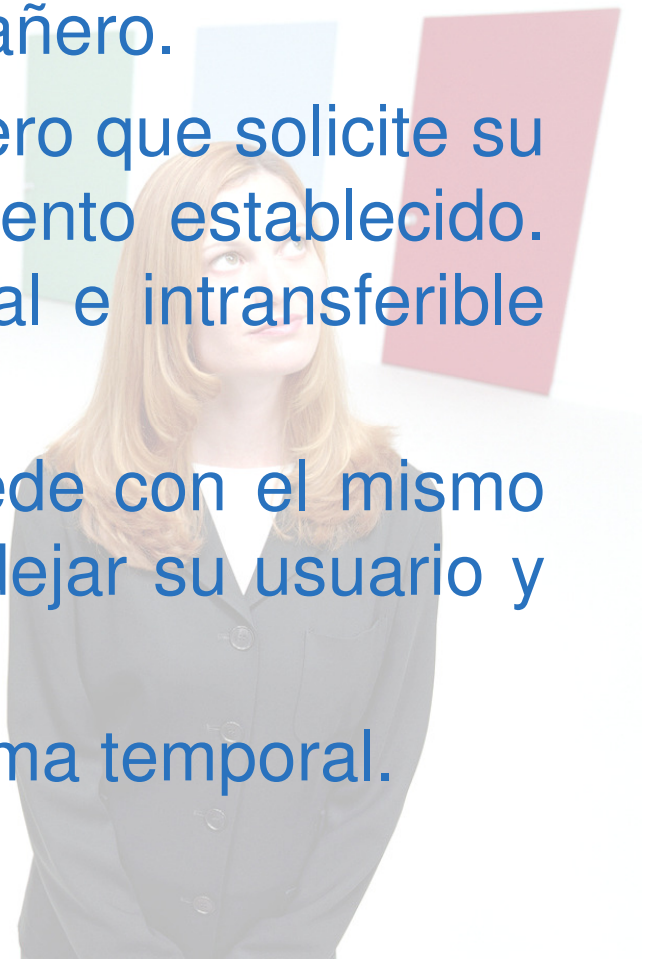
Opciones:

a) Conocedor del mecanismo de alta de usuarios, el profesional le crea una cuenta al compañero.

b) El profesional debe advertir al compañero que solicite su usuario y contraseña por el procedimiento establecido. Al tratarse de una información personal e intransferible opta por no dársela.

c) Al tratarse de un compañero que accede con el mismo perfil y a los mismos datos, le puede dejar su usuario y contraseña.

d) Le cede su usuario y contraseña de forma temporal.



CASO PRÁCTICO 2: Acceso a los Sistemas de Información

Dudas del profesional:

- **¿Quién me puede asesorar sobre cómo debo actuar?**
  - La persona **Responsable de su Servicio**.
  - En el departamento de **Informática** ó Sistemas de Información del centro.
  - El **Responsable de Seguridad**
- **¿Dónde puedo encontrar los formularios para solicitar usuario y contraseña?**
  - El procedimiento viene establecido en el **Documento de Seguridad**.
  - En el Departamento de **Informática** o de Sistemas de Información.
  - Solicítalos al **Responsable de Funcional de Aplicación o al Responsable de Seguridad**.
- **¿Puedo usar usuario y contraseña de otro compañero?**
  - **No**, es personal e intransferible.

CASO PRÁCTICO 2: Acceso a los Sistemas de Información

Normativa aplicable:

- RD 1720/2007 de 21 Diciembre. Artículo 91, 93
- Manual Comportamiento Empleados Públicos. Artículo 7.1
- Documento de Seguridad
  - Obligaciones de todo el personal
  - Figura del Responsable Funcional de Aplicación
  - Figura del Responsable de Seguridad
  - Anexo con plantilla de documento de acceso
- Obligaciones de la LOPD

CASO PRÁCTICO 2: Acceso a los Sistemas de Información

Resumen:

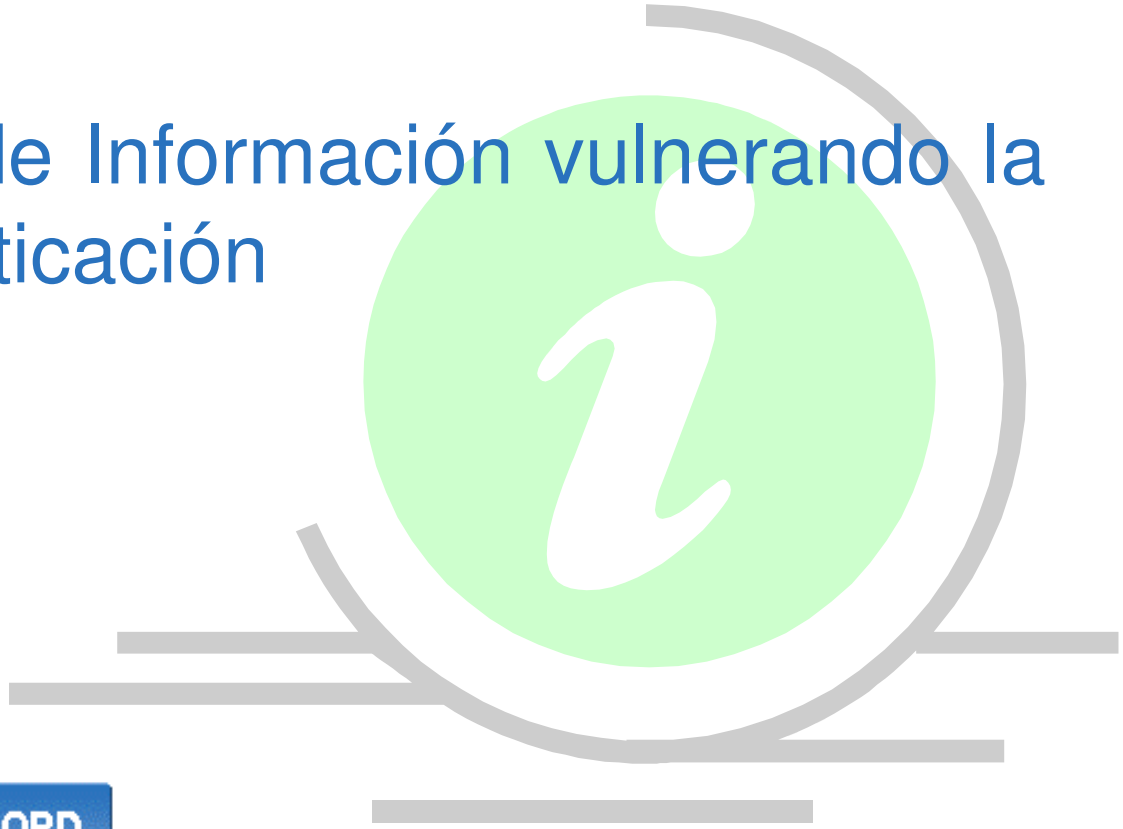
Conceptos que hay que tener muy claros:

- **Existe un procedimiento** para solicitar acceso a los Sistemas de Información
- Éste debe constar como **anexo del Documento de Seguridad** y debe estar actualizado por el centro.
- El **Responsable Funcional de Aplicación** debe ser la figura a la que el usuario/profesional consulte la mayoría de sus dudas respecto de los datos de carácter personal
- Las credenciales de un usuario lo vinculan con sus acciones en los Sistemas de Información. **Responsabilidades.**

CASO PRÁCTICO 2: Acceso a los Sistemas de Información

Casos similares:

- Utilización de **credenciales** de acceso **genéricas**
- Reutilización de **credenciales** de acceso **obsoletas**
- Acceso a Sistemas de Información vulnerando la identificación y autenticación



CASO PRÁCTICO 2: Acceso a los Sistemas de Información

Caso Real:

Primera sanción por no disponer de usuario y contraseña

Por Samuel Parra • 26 Mayo, 2008

Existe un gran desconocimiento respecto a las medidas de seguridad que un fichero con datos de carácter personal debe disponer, y aquí me estoy refiriendo a las medidas de seguridad que el ordenamiento jurídico impone (no a las voluntarias o recomendables)
Pocas son las empresas que las cumplen, y si hablamos de profesionales individuales, creo que el grado de cumplimiento tiende a 0.

Si a este desconocimiento de la legislación le sumamos la poca concienciación que existe en el ámbito empresarial de entender que el activo más valioso para cualquier profesional son los datos de sus clientes, nos encontramos con que la mayoría de los sistemas de información no cumplen unos requisitos mínimos de seguridad, como la del caso que vamos a examinar en relación a la **existencia de un mecanismo de identificación y autentificación, o lo que es lo mismo, de usuario y contraseña** (normalmente).

Porque en efecto, tanto la regulación actual como la anterior, imponen la obligación de que para acceder al fichero con datos de carácter personal exista un mecanismo de estas características.

En este caso el sancionado ha sido un **abogado**, por denuncia de un particular; para seguir leyendo haz click en

En agosto de 2004, la Agencia Española de Protección de Datos recibió una denuncia de un particular, en la que, entre otras cosas, informaba que el abogado D. I.I.I. tiene una base de datos con los clientes de su despacho, **sin las medidas de seguridad que exige la ley**.

CASO PRÁCTICO 3: Publicación de un estudio epidemiológico

Los miembros de un grupo de investigación de la Universidad, nos piden datos de pacientes para hacer un estudio epidemiológico.

Además, pretenden publicar los resultados del estudio en una revista científica.

CASO PRÁCTICO 3: Publicación de un estudio epidemiológico

Opciones:

a) Se trata de un procedimiento habitual que no implica acción adicional por parte del profesional.

b) El profesional advierte verbalmente al que le cede estos datos, para que sea cuidadoso con el manejo de estos datos y que guarde secreto.

c) El profesional se asegura que la entidad o persona a la que le cede los datos, ha sido previamente autorizada para dicha cesión.

d) El profesional, previa autorización del Responsable del Fichero, solo cede datos que no identifican a pacientes (o disociados), ya que para hacer el estudio o el servicio, no es necesario saber la identidad de un paciente.

CASO PRÁCTICO 3: Publicación de un estudio epidemiológico

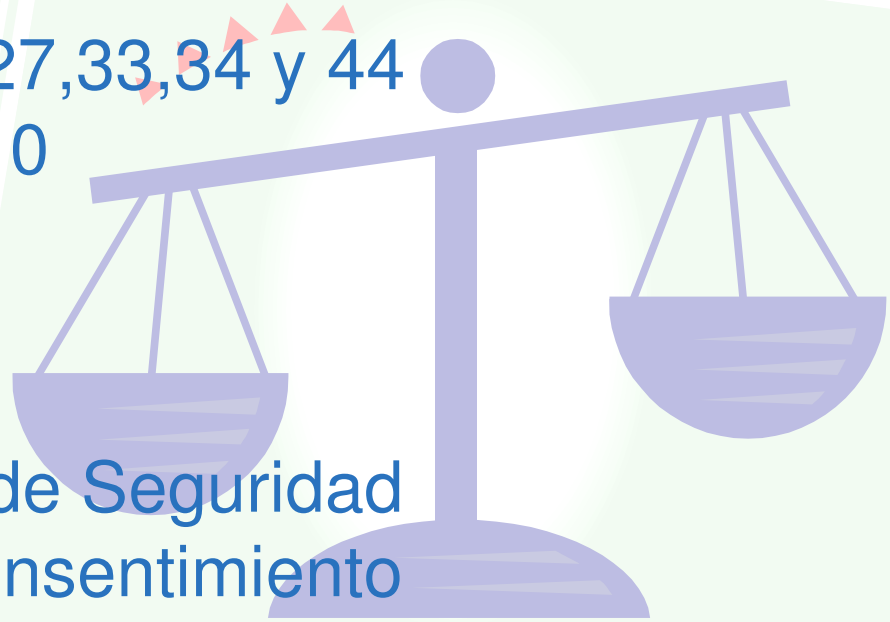
Dudas del profesional:

- **¿Quién me puede asesorar sobre cómo debo actuar?**
  - El **Responsable de Seguridad**
- **¿Puedo ceder libremente datos de mis pacientes, siempre y cuando estén disociados?**
  - Normativa Interna del centro y o Responsable Funcional de aplicación
- **¿Puedo Descargar, guardar o grabar datos para cederlos?**
  - **No**, excepto si contamos con la autorización del Responsable del Fichero o persona en quién delegue (Responsable de Seguridad).
- **¿Puedo ceder datos a otras Administraciones Públicas?**
  - Si a los **centros y servicios del Sistema Nacional de Salud** . (Sin el consentimiento del Paciente), No en otros casos (Nos haría falta el Consentimiento del Paciente).

CASO PRÁCTICO 3: Publicación de un estudio epidemiológico

Normativa aplicable:

- Cesión o comunicación de datos / Consentimiento informado en materia de protección de datos
  - LOPD 15/1999. Artículos 3.c,3.e,6,7.3,8,10,11,21,27,33,34 y 44
  - RD 1720/2007. Artículo 10
  - LAP 41/2002. Artículo 7
  - MCEP 6.2 y 6.11
- Documento de Seguridad
  - Figura del Responsable de Seguridad
  - Anexo con plantilla de consentimiento
  - Responsable Funcional de la Aplicación

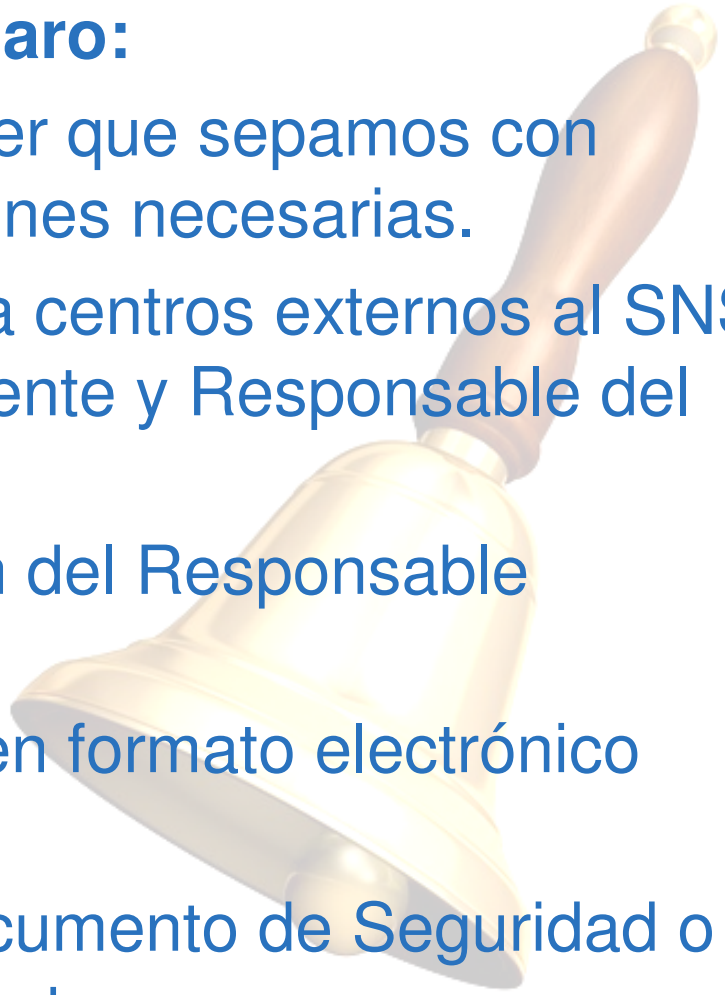


CASO PRÁCTICO 3: Publicación de un estudio epidemiológico

Resumen:

Conceptos que hay que tener muy claro:

- No ceder o comunicar datos, a no ser que sepamos con seguridad que tienen las autorizaciones necesarias.
- Para DCP No disociados enviados a centros externos al SNS: Necesidad de Autorización del Paciente y Responsable del fichero.
- Para datos Disociados: Autorización del Responsable funcional de aplicación
- Registrar la E/S de soportes, tanto en formato electrónico como en Papel
- Ante cualquier duda consultar el documento de Seguridad o al Responsable de Seguridad del centro



CASO PRÁCTICO 3: Publicación de un estudio epidemiológico

Casos similares:

- Fundaciones, ONG´s, Laboratorios.
- Familiares de pacientes que nos piden información sobre el estado de un paciente
- Periodistas o conocidos, que nos piden información sobre un famoso que se encuentra ingresado, o se le ha realizado alguna intervención.
- Clínicas o empresas privadas, que habitualmente nos hacen estudios radiológicos, analíticas u otros servicios o mantenimientos.

CASO PRÁCTICO 3: Publicación de un estudio epidemiológico

Caso Real:

AGENCIA

datospersonales.org

La revista de la Agencia de Protección de Datos de la Comunidad de Madrid
ISSN: 1988-1797

Consejo Editorial Número actual

>> APDCM : INFORMES Y RESOLUCIONES

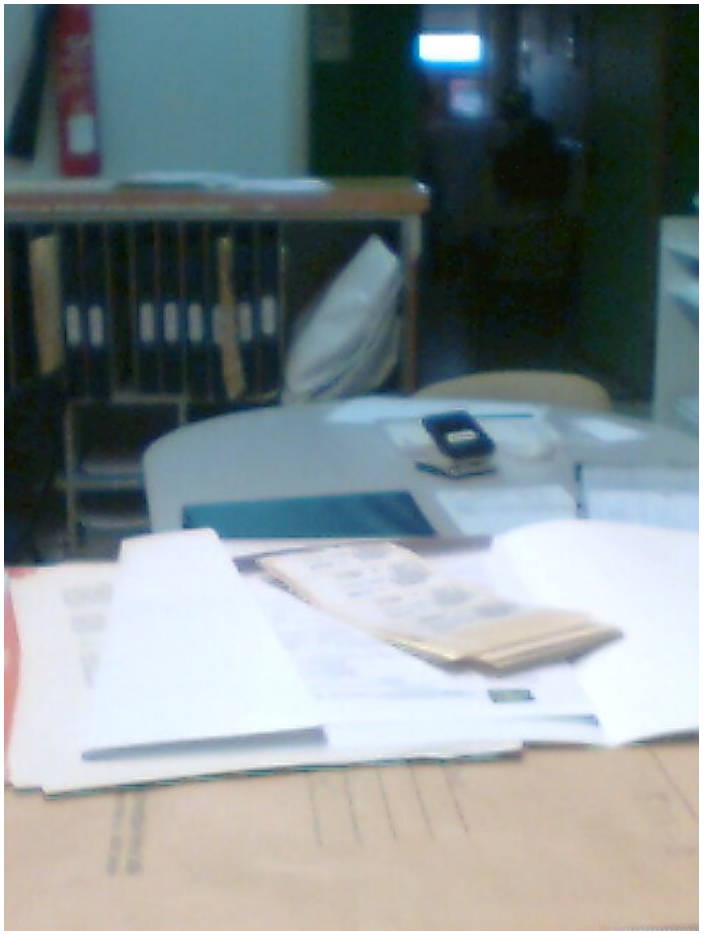
Volver a sección Página 1 de 1 Imprimir página

Cesión de listado comprensivo de pacientes ingresados por anorexia y bulimia.

Para poder facilitar la información demandada a la persona que realiza la solicitud, debería someterse ésta a un procedimiento de disociación, previo a la cesión, de forma que la información que obtenga no pueda asociarse a persona identificada o identificable.

Ha tenido entrada en el Registro de Documentos de ésta Agencia de Protección de Datos de la Comunidad de Madrid, escrito del Subdirector Médico del Hospital (...), solicitando se le indique la manera más adecuada de proceder ante una petición recibida, en la que se insta la entrega de "copia de la documentación oficial obrante en la base de datos correspondiente sobre el listado de los pacientes ingresados por anorexia y bulimia en el último año 2006 y sus correspondientes características anotadas en el referido registro oficial de datos, al objeto de poder realizar un estudio sociológico sobre cuantificación estadística del fenómeno de la población ingresada por estas patologías referidas a los trastornos alimentarios, y su distribución por diferentes áreas y diversas variables clasificatorias, apelando a la vigente legislación española sobre derechos de acceso de los ciudadanos a los documentos y archivos obrantes en la Administración que no estén expresamente protegidos por la regulación de secretos especiales u otras específicas".

CASO PRÁCTICO 4: Destrucción de documentos antiguos



Los armarios de la oficina están abarrotados de papeles, muchos de ellos antiguos o copias de trabajo de otros documentos con información que ya no se utiliza para nada. Una limpieza de las estanterías vendría muy bien para hacer espacio.....

CASO PRÁCTICO 4: Destrucción de documentos antiguos

Opciones:

a) Podemos poner los papeles en cajas y ponerlos en el pasillo para que lo recojan las limpiadoras.

b) Podemos ponerlo en las papeleras de reciclaje del hospital.

c) Solicitamos la autorización del responsable del fichero y destruimos el papel, luego lo enviamos a las papeleras de reciclaje.

d) Lo ponemos en los contenedores de papel de la calle, se los lleva el ayuntamiento para reciclarlos.

CASO PRÁCTICO 4: Destrucción de documentos antiguos

Dudas del profesional:

- **¿Qué debo hacer para deshacerme del papel inservible?**
  - Dependiendo de la información contenida en el papel podemos actuar de forma diferente.
  - Si el papel NO contiene DCP (p.e. estadísticos):
    - Podemos tirarlo directamente a la papelera sin ningún temor respecto a la ley de protección de datos.
  - Si el papel contiene datos personales de pacientes o trabajadores:
    - Es imprescindible destruir el papel por cualquier mecanismo que lo haga ilegible para otras personas antes de tirarlo a cualquier contenedor o papelera. Además es necesaria la autorización del Responsable del Fichero

CASO PRÁCTICO 4: Destrucción de documentos antiguos

Dudas del profesional:

➢¿Qué medidas debo tomar para el almacenamiento de documentos papel con datos de carácter personal?

- Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el **acceso esté protegido** con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

➢¿Qué medidas debo tomar para enviar un documento fuera de los locales donde se encuentran archivados?

- Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a **impedir el acceso o manipulación de la información** objeto de traslado. Además debe obtenerse la autorización necesaria del responsable del fichero (a través del responsable de aplicación o nuestro superior jerárquico) y **registrar la salida** en el registro de E/S de información.

CASO PRÁCTICO 4: Destrucción de documentos antiguos

Dudas del profesional:

- **Necesito hacer copias de una documentación, ¿A quien puedo encargar el trabajo de copia?**
  - La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del **personal autorizado** en el documento de seguridad.
  - Deberá procederse a la **destrucción de las copias o reproducciones desechadas** de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

CASO PRÁCTICO 4: Destrucción de documentos antiguos

Normativa aplicable:

- **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.
- **LEY 14/1986**, de 25 de Abril, **General de Sanidad**
- **LEY Orgánica 15/1999**, de 13 de Diciembre, de Protección de Datos de Carácter Personal. **(LOPD)**
- **REAL DECRETO 1720/2007**, de 21 de diciembre, por el que se aprueba el **Reglamento de desarrollo de la LOPD**
- **Documento de Seguridad**
  - Funciones y Obligaciones del Personal
  - Gestión de Documentos

CASO PRÁCTICO 4: Destrucción de documentos antiguos

Resumen:

Conceptos que hay que tener muy claro:

- Todos los datos personales, sin importar cual sea su soporte físico debe manejarse con las garantías exigidas en la ley, tanto para su utilización, archivo, custodia y traslado.
- Los documentos con datos personales deben encontrarse siempre **protegidos** (p.e. bajo llave)
- Sólo el **personal autorizado** puede tener acceso a los documentos en papel
- Para deshacerse de cualquier documento con datos personales hay que proceder a su **destrucción** previa de forma que se impida su recuperación posterior.
- El traslado de la documentación debe realizarse de forma que se **impida el acceso a la misma a personas no autorizadas**

CASO PRÁCTICO 4: Destrucción de documentos antiguos

Casos similares:

- Envío de información por correo electrónico (especialmente fuera de la red corporativa)
- Llevar información fuera de las instalaciones del SAS
  - en portátiles
  - pen-drives
  - CD's
  - o cualquier otro dispositivo de almacenamiento.
- Envío de imágenes radiológicas identificadas a otro destinatario distinto del propio paciente

CASO PRÁCTICO 4: Destrucción de documentos antiguos

Casos real:

elmundo.es

BÚSQUEDAS

60 segundos | Edición impresa | Opinión | Callejero | Servicios | Gráficos | Charlas | Tienda | Juegos

Fotos del día
Álbum
Vídeos
Mapa del sitio

ULTIMA HORA
España
Internacional
Sociedad
Economía
Deportes
Cultura
Cine
Ciencia
Tecnología
60 segundos
Especiales

EDICIÓN LOCAL
Madrid24horas
Catalunya
Baleares

SERVICIOS
El tiempo
Televisión
Hemeroteca
Callejero
Pág. blancas
Pág. amarillas
Diccionarios
Horóscopo
Traductor
Barra de navegación

SUPLEMENTOS
Magazine
Crónica

sociedad

Domingo, 28 de Julio de 2002
Actualizado a las 16:55 (CET) - Internet time @663 by swatch

MÁLAGA | DATOS CONFIDENCIALES

Una trabajadora de un centro de salud andaluz admite haber tirado 7.000 expedientes a la basura

El delegado del Servicio Andaluz de Salud se queja de la difusión pública del incidente

AGENCIAS

MÁLAGA.- Una trabajadora del centro de salud de **Los Boliches, de Fuengirola**, ha reconocido ser la responsable de que **7.000 expedientes con datos sanitarios y confidenciales** aparecieran el pasado viernes 26 al lado de unos contenedores de basura, informó el delegado provincial de Salud de la Junta, José Luis Marcos.

Periodistas del canal de la televisión local de Fuengirola encontraron los documentos junto al citado centro del Servicio Andaluz de Salud (SAS) y cuando el distrito sanitario tuvo conocimiento de este hecho se puso a trabajar para investigar lo ocurrido, momento en el que una trabajadora administrativa del centro admitió haber tirado la información a la basura.

Según explicó Marcos, la mujer "confesó que decidió coger esa información", que estaba archivada, y depositarla en la calle **para "hacer limpieza"**, y que incluso reconoció que **era consciente de que "no debería haberlo hecho"**.

CASO PRÁCTICO 5: Llevarse trabajo a casa

Un profesional de un centro sanitario tiene que trabajar en casa, para lo que necesita llevarse historiales clínicos de pacientes.

CASO PRÁCTICO 5: Llevarse trabajo a casa

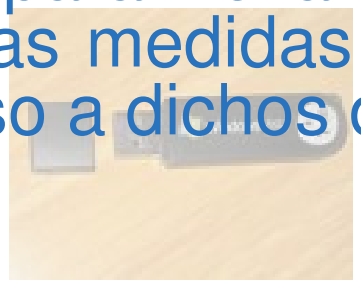
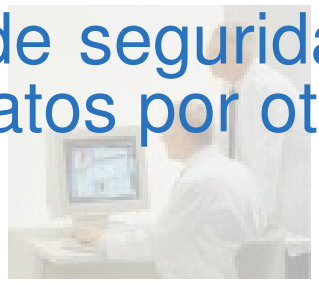
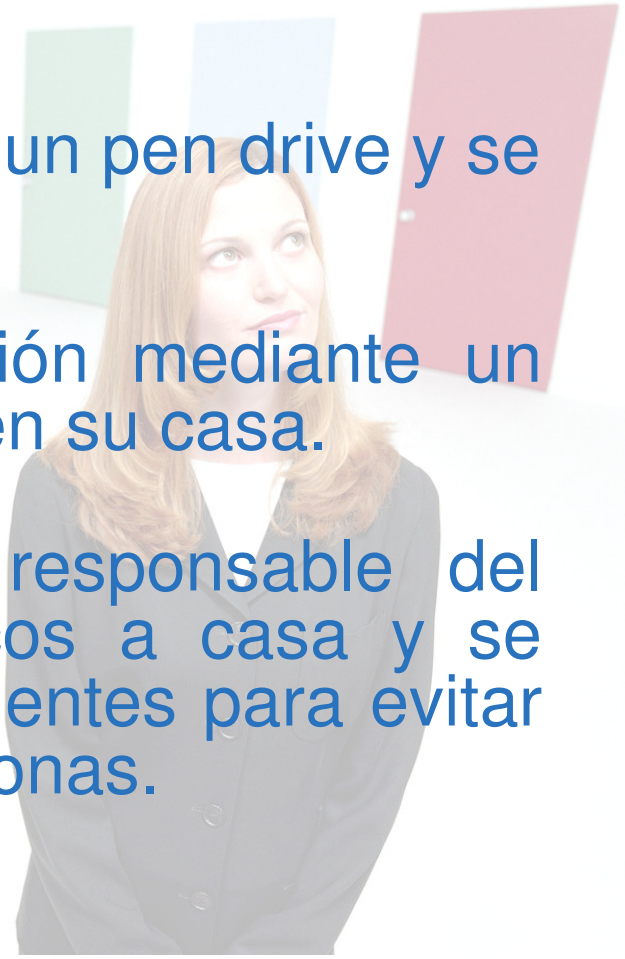
Opciones:

a) El profesional coge las carpetas de los historiales clínicos y se los lleva a su casa.

b) El profesional guarda la información en un pen drive y se lo lleva a su casa.

c) El profesional se manda la información mediante un correo electrónico, para luego abrirlo en su casa.

d) El profesional pide autorización al responsable del fichero para llevarse historiales clínicos a casa y se toman las medidas de seguridad pertinentes para evitar el acceso a dichos datos por otras personas.

CASO PRÁCTICO 5: Llevarse trabajo a casa

Dudas del profesional:

- **¿Qué procedimiento debe seguir el profesional para poder llevarse las historias clínicas a casa?**

  - Pedir la **autorización** al responsable funcional de la aplicación y después este se lo transmite al responsable del fichero, quien será el encargado de aprobar dicha solicitud.
  - Cumplir con el **procedimiento de seguridad** del centro en el caso de extracción de datos de salud que al menos deberá incluir las medidas de protección aplicables durante el transporte y en “la casa” y el registro de entrada/salida.

CASO PRÁCTICO 5: Llevarse trabajo a casa

Dudas del profesional:

- **¿Qué procedimiento hay que seguir en caso de pérdida de dicha información?**
  - **Comunicar la incidencia** al responsable funcional de la aplicación, el cual se encargará de comunicárselo al responsable de seguridad y este a su vez al responsable del fichero. El responsable de seguridad se encargará de realizar los trámites para denunciar la pérdida de datos a la Policía.
  - El profesional podrá rellenar la solicitud para **incluir la incidencia en el registro de incidencias** o bien comunicárselo al responsable funcional, y este se lo comunicará al responsable de seguridad quien será el que tome la decisión de incluir o no dicha incidencia en el registro de incidencias.

CASO PRÁCTICO 5: Llevarse trabajo a casa

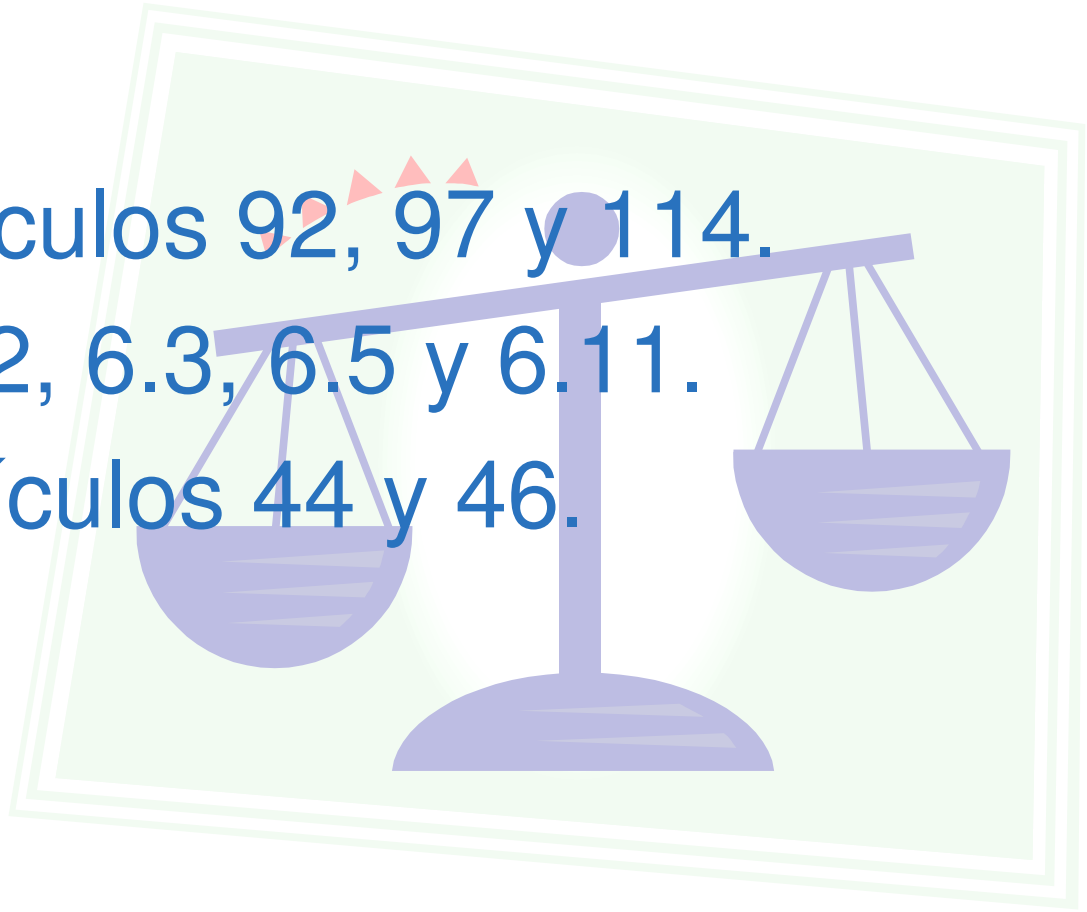
Dudas del profesional:

- **¿Qué ocurriría en el caso de no seguir este procedimiento?**
  - En este caso se cometería una **infracción grave**. Como medidas sancionadoras al cometer dicha infracción, la AGPD dictará una resolución estableciendo las medidas que procede adoptar para que se corrijan los efectos de la infracción.
  - La AGPD podrá también iniciar las **actuaciones disciplinarias**, si procedieran.
  - En el SAS, para depurar responsabilidades se podrá aplicar el **régimen disciplinario interno** como consecuencia de las actuaciones de la AEPD.

CASO PRÁCTICO 5: Llevarse trabajo a casa

Normativa aplicable:

- RD 1720/2007. Artículos 92, 97 y 114.
- MCEP. Artículos 6.2, 6.3, 6.5 y 6.11.
- LOPD 15/1999. Artículos 44 y 46.



CASO PRÁCTICO 5: Llevarse trabajo a casa

Resumen:

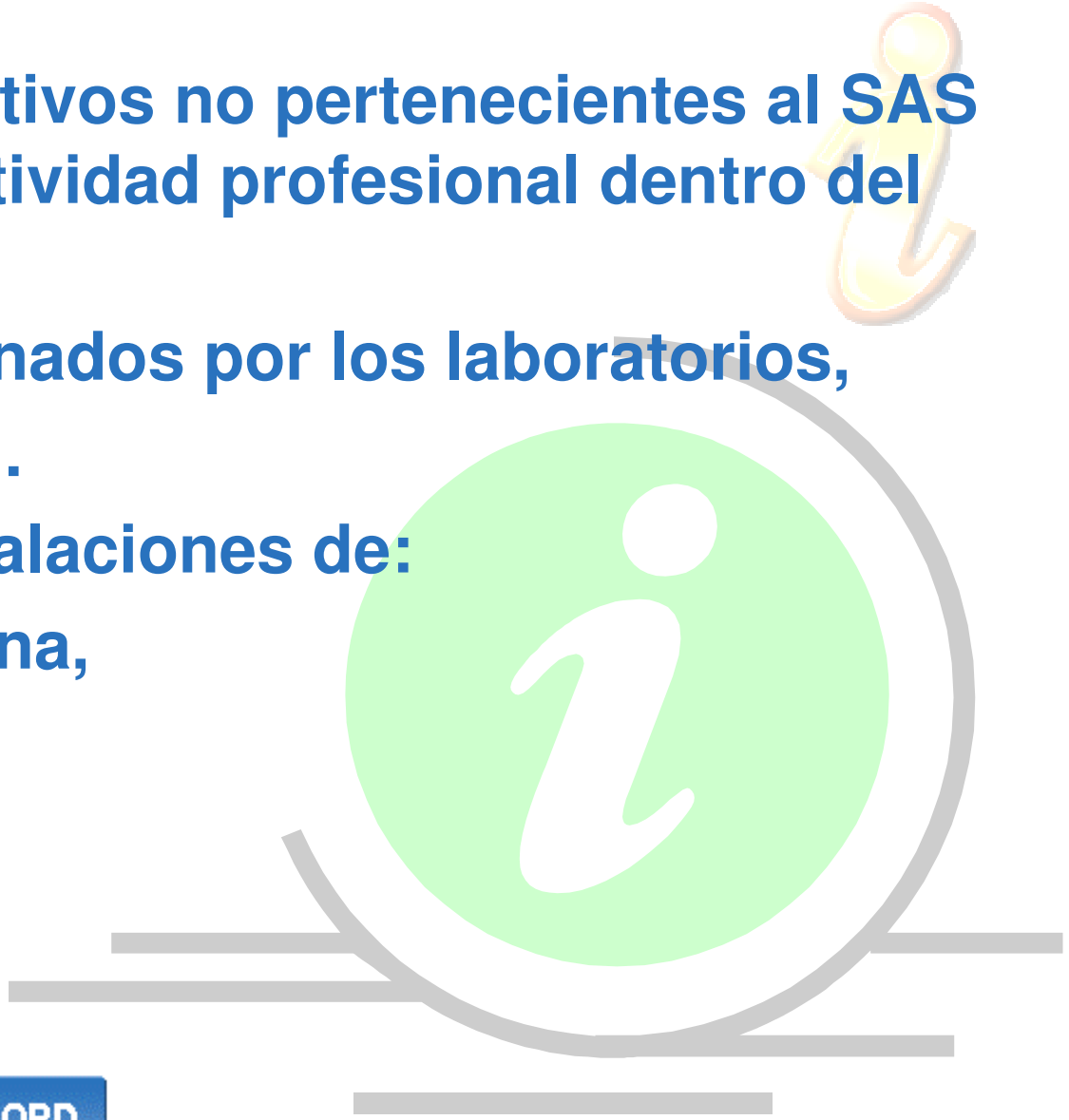
Conceptos que hay que tener muy claros:

- El tratamiento de datos de carácter personal fuera de los locales de ubicación del fichero debe ser **autorizado por el Responsable del Fichero**.
- Se deberá garantizar el **nivel de seguridad adecuado** según lo establecido en el Manual de Seguridad.
- La seguridad abarcará tanto a los **equipos del centro de trabajo como de la casa**, todos aquellos desde los que se accede o donde aparecen resultados visuales o impresos, así como en los procesos de transmisión de información.

CASO PRÁCTICO 5: Llevarse trabajo a casa

Casos similares:

- Usar equipos o dispositivos no pertenecientes al SAS para desempeñar la actividad profesional dentro del centro sanitario:
  - equipos proporcionados por los laboratorios,
  - equipos propios, …
- Trabajar desde las instalaciones de:
  - una empresa externa,
  - hotel,
  - cibercafé, ….



CASO PRÁCTICO 5: Llevarse trabajo a casa

Caso real:

Los escándalos de los archivos perdidos

La pérdida de una memoria portátil con información sobre miles de criminales es el último caso de una serie de extravíos o robos de información confidencial que dejan mal parada a la Administración británica.

- Expedientes de ayudas fiscales (noviembre de 2007).

Hacienda extravía dos discos de ordenador con los datos de las 7,25 millones de familias que han pedido ayudas fiscales por sus hijos. Las informaciones, que incluyen filiación, número de la seguridad social y cuentas bancarias, afectan a 25 millones de personas. Los discos fueron enviados por correo interno, sin las debidas garantías, a la Oficina Nacional de Auditoría. Pese a la búsqueda y a una recompensa de 20.000 libras, (25.000 euros) los discos no aparecieron.

- Exámenes de conducir (diciembre de 2007).

Una memoria externa con datos de tres millones de personas que se habían presentado al examen teórico de conducir se extravía en EE UU, en manos de la empresa encargada de su procesamiento. El Gobierno británico dice que la información no es accesible a terceros.

- Datos de reclutas (enero de 2008). El portátil de un oficial de la Marina, con información confidencial de 600.000 aspirantes a entrar en la Armada o la Fuerza Aérea, es robado de un vehículo en Birmingham. El caso destapa la existencia de centenares de robos de ordenadores del Ministerio de Defensa.

- Robo de otro portátil (abril de 2008).

El ordenador portátil de un capitán del Ejército es sustraído de debajo de su silla mientras comía en un McDonald's. La información no era "sensible" y estaba encriptada, dicen sus superiores. El Gobierno acababa de endurecer las normas para sacar ordenadores o memorias externas del Ministerio de Defensa.

- Documentos de Al Qaeda (junio de 2008). Un alto funcionario de inteligencia es sancionado después de olvidar un documento con la etiqueta "Top Secret" en un tren de cercanías. La carpeta contiene dos informes sobre Al Qaeda y la situación de las fuerzas de seguridad iraquíes. Este mismo mes, aparece en otro tren un documento del Tesoro sobre la red de financiación del terrorismo islamista.

- Caos en Defensa (julio de 2008). El Ministerio de Defensa confirma el extravío o el robo, desde 2004, de 747 portátiles y de 121 memorias externas, cinco de ellas con datos secretos

CASO PRÁCTICO 6: Envío de Datos Personales por Correo Electrónico

¿Se puede enviar la historia clínica de un paciente u otros datos personales del mismo por correo electrónico?

CASO PRÁCTICO 6: Envío de datos personales por correo electrónico

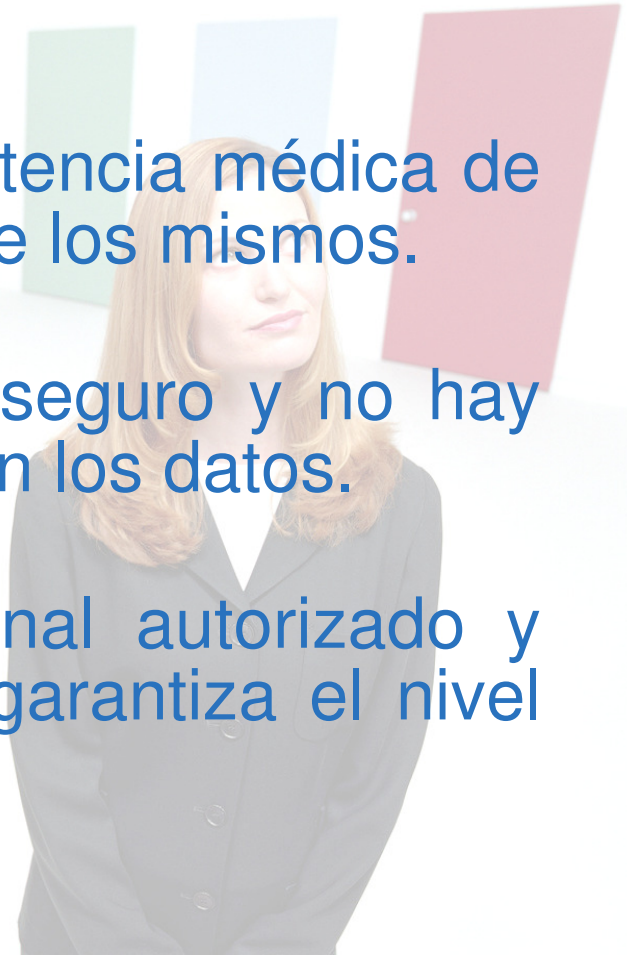
Opciones:

a) No. No pueden enviarse datos personales por correo electrónico en ningún caso.

b) Si, pero solo si es en relación a la asistencia médica de los afectados y con el consentimiento de los mismos.

c) No, pues el correo electrónico no es seguro y no hay garantía de que los destinatarios reciban los datos.

d) Si, pero solo podrá hacerlo el personal autorizado y cumpliendo la normativa vigente que garantiza el nivel de protección adecuado.



CASO PRÁCTICO 6: Envío de datos personales por correo electrónico

Dudas del profesional:

- **¿Puedo usar mi cuenta de correo particular para enviar o recibir información relacionada con mi trabajo?**
  - No, está **prohibido terminantemente** el uso de otras cuentas de correo distintas de las facilitadas por la Administración de la Junta de Andalucía.
- **¿Quién tiene que autorizarme para poder enviar los datos personales de pacientes?**
  - El envío tiene que ser **autorizado** por el Responsable del fichero o el Responsable Funcional de la Aplicación en quien este haya delegado
  - La solicitud debe dirigirse al Responsable Funcional de la Aplicación
  - El envío debe registrarse en el **Registro de Entrada/Salida** de soportes del centro. De esto se encargará el Responsable de Seguridad.

CASO PRÁCTICO 6: Envío de datos personales por correo electrónico

Dudas del profesional:

- **¿Necesito el consentimiento de los afectados para enviar sus datos personales?**
  - No si dicho envío está relacionado con su asistencia y/o tratamiento. Para cualquier otro fin es necesario el consentimiento.
  - Existen excepciones en las cuales no es necesario el consentimiento.
  - Siempre que sea posible se procederá a la disociación de los datos.

- **¿ Cómo puedo asegurarme de que solamente el destinatario del envío accede a los datos y que estos no han sido modificados en el camino?**
  - Mediante el uso de técnicas de cifrado y/o firma digital. **El cifrado es obligatorio** cuando se envían datos personales fuera de la red corporativa de la Junta de Andalucía-SSPA.
  - La preparación de los datos debe ser validada y autorizada por el Usuario Responsable de la Aplicación/Fichero.
  - Cualquier incidencia al respecto hay que comunicarla al Responsable de Seguridad.

CASO PRÁCTICO 6: Envío de datos personales por correo electrónico

Dudas del profesional:

- **¿ Tengo que tener en cuenta algún requisito adicional cuando se envían datos a un tercero para que este efectúe, por encargo, determinado tratamiento con los datos suministrados (por ejemplo un "mailing" para invitación a un evento)?**

  - Debe existir un **contrato escrito** que regule el tratamiento que realizará el tercero en cuestión y que indique las medidas de seguridad que este (el encargado del tratamiento) está obligado a implementar.

  - Una vez concluida la relación contractual **los datos deben ser destruidos o devueltos** al responsable del tratamiento.

CASO PRÁCTICO 6: Envío de datos personales por correo electrónico

Normativa aplicable:

- Manual de Seguridad Corporativa del SAS
- Ley 15/1999 de 13 de Diciembre (LOPD)
- RD 1720/2007 Reglamento Desarrollo LOPD
- Manual de Comportamiento de los Empleados Públicos en el uso de los Sistemas Informáticos y Redes de Comunicación de la JJ.AA.

CASO PRÁCTICO 6: Envío de datos personales por correo electrónico

Resumen:

Conceptos que hay que tener muy claros:

- El envío de datos personales por correo electrónico ha de ser **autorizado por el Responsable de Aplicación/Fichero** el cual debe actuar según la LOPD
- Debe quedar anotado en el **Registro de Entrada/Salida de soportes.**
- La información tiene que **enviarse cifrada.**
- **Cualquier incidencia de seguridad tiene que comunicarse** al Responsable de Seguridad.

CASO PRÁCTICO 6: Envío de datos personales por correo electrónico

Casos similares:

- **Envío o transferencia de información en soportes portátiles**
  - Pen-drive
  - CD/DVD
  - Disco duro externo
  - PDA
- **Envío o transferencia de ficheros a través de internet**
  - FTP
  - HTTP

CASO PRÁCTICO 6: Envío de datos personales por correo electrónico

Caso real:

Multa de 600 euros por dejar a la vista 42 direcciones de correo electrónico

Cuidado al mandar mensajes masivos: utiliza el campo CCO

ELPAIS.com - Madrid - 23/02/2007

Da igual que sea un despiste, pero todo aquel que en una actividad que no sea doméstica o personal deje a la vista las direcciones de correo electrónico de sus destinatarios está cometiendo una infracción multada hasta con 60.101, 21 euros por la Ley Orgánica de Protección de Datos (LOPD).

Doña A.G. S. sabe bien que no se trata de una amenaza, pues ha tenido que pagar 601,01 euros por haber dejado a la vista 42 direcciones de *email* al enviar un mensaje promocional de telefonía móvil por encargo de una pequeña empresa conocida como La Cremallera, que estaba llevando a cabo una campaña para Vodafone.

Uno de los destinatarios de este mensaje sintió que se violaba su intimidad al exponer su dirección y no utilizar la opción de copia oculta (CCO), y presentó una denuncia ante la Agencia Española de Protección de Datos (AEPD), quien inició el proceso.

El correo electrónico se considera un dato personal desde 1999, según explica en su blog dedicado al derecho y las nuevas tecnologías Samuel Parra, y sólo se puede utilizar para los fines que su propietario ha autorizado. Este punto echó por tierra la defensa de la denunciada, quien alegaba que la dirección de correo de su denunciante se podía encontrar en Internet en diferentes páginas web.

"Esto (se refiere a LOPD) nos deja cristalino que aunque la dirección aparezca en Internet, si no tenemos consentimiento del interesado no podremos utilizarla para ningún tipo de comunicación", explica Parra. La sentencia de la AEPD asegura que se ha violado el artículo 10 de la LOPD en el que se refiere al deber de secreto profesional. La agencia ha aplicado la menor multa contemplada para este tipo de infracción considerada leve.

En cualquier caso, la lección que se saca de esta multa es que en ningún momento se debe de copiar en el apartado CC (Copia Carbón) las direcciones de nuestros destinatarios si estamos realizando cualquier tipo de comunicación, que se salga del ámbito doméstico o personal.

CASO PRÁCTICO 7: Descargar música y software en el trabajo

El personal de un centro sanitario, aprovecha el equipo informático que tiene asignado para el desarrollo de sus tareas profesionales, para hacer descargas desde Internet de música, software, etc,…..

CASO PRÁCTICO 7: Descargar música y software en el trabajo

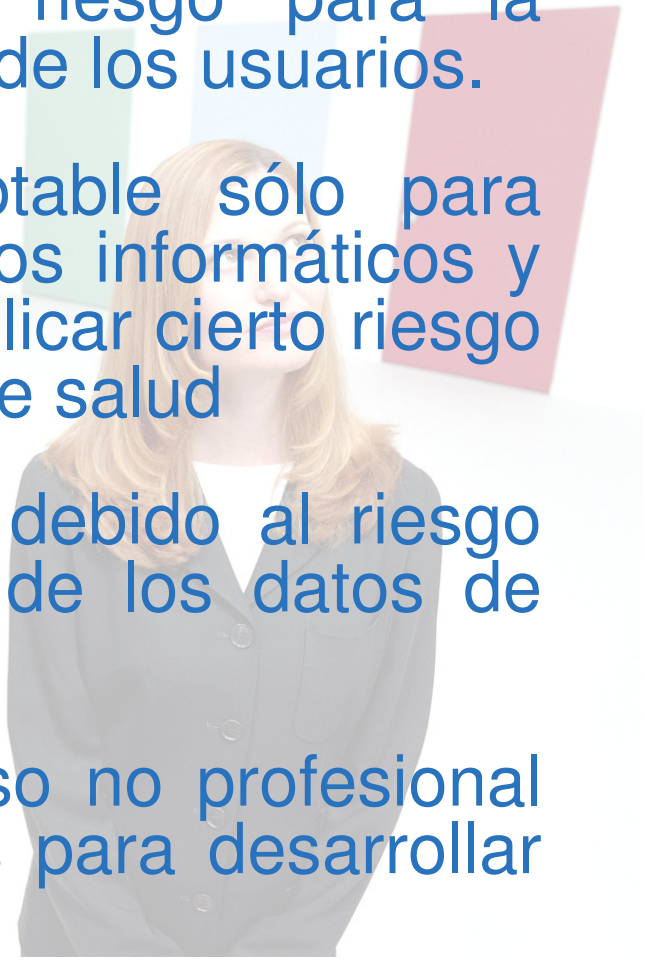
Opciones:

a) Se trata de un procedimiento habitual entre algunos empleados que no implica ningún riesgo para la confidencialidad de los datos de salud de los usuarios.

b) Se trata de un procedimiento aceptable sólo para aquellos usuarios con los conocimientos informáticos y técnicos adecuados ya que podría implicar cierto riesgo sobre la confidencialidad de los datos de salud

c) Se trata de una práctica inaceptable debido al riesgo que supone para la confidencialidad de los datos de salud

d) Está totalmente prohibido hacer un uso no profesional de los equipos informáticos asignados para desarrollar nuestro trabajo



CASO PRÁCTICO 7: Descargar música y software en el trabajo

Dudas del profesional:

¿Puedo instalar software por mi cuenta en el equipo informático que utilizo para trabajar?

- Los equipos informáticos sólo puede utilizarse con **fines profesionales**
- La utilización de **las aplicaciones informáticas tiene una finalidad profesional**.
- Sólo el **personal autorizado** puede **instalar, configurar o desinstalar** sistemas y aplicaciones informáticas.
- Sólo podemos utilizar aquellas aplicaciones informáticas para las que estemos autorizados expresamente.
- **Está expresamente prohibida la instalación de aplicaciones informáticas sin la correspondiente licencia o no adecuándose a la legislación vigente.**

CASO PRÁCTICO 7: Descargar música y software en el trabajo

Dudas del profesional:

¿Mi ordenador va un poco lento, puedo desinstalar el antivirus?

Los usuarios están obligados a utilizar los antivirus y sus actualizaciones u otros sistemas de seguridad, destinados a la prevención y protección de Sistemas de Información.

¿Puedo desinstalar aplicaciones corporativas instaladas de mi equipo?

Los usuarios en ningún caso podrán borrar o desinstalar las aplicaciones informáticas legalmente instaladas por la Administración de la Junta de Andalucía.

CASO PRÁCTICO 7: Descargar música y software en el trabajo

Dudas del profesional:

¿Podemos utilizar los equipos informáticos para usos personales?

¿Puedo tener mis datos, fotos, documentos personales en los equipos que utilizo para trabajar?

Los usuarios deberán hacer un uso de los equipos informáticos compatible con la finalidad de las funciones del servicio al que se encuentren adscritos y que correspondan a su trabajo.

CASO PRÁCTICO 7: Descargar música y software en el trabajo

Dudas del profesional:

¿Puedo instalar o conectar dispositivos hardware a mi equipo de trabajo?

- Los usuarios deberán cuidar los equipos informáticos que les sean facilitados, no procediendo a alterarlos o modificarlos.
- Los usuarios no tienen permitido conectar a los equipos informáticos otros equipos distintos de los que tengan instalados.
- En ningún caso se podrá acceder físicamente al interior de los PC's. Sólo personal autorizado podrá realizarlo para labores de reparación, instalación o mantenimiento.

CASO PRÁCTICO 7: Descargar música y software en el trabajo

Normativa aplicable:

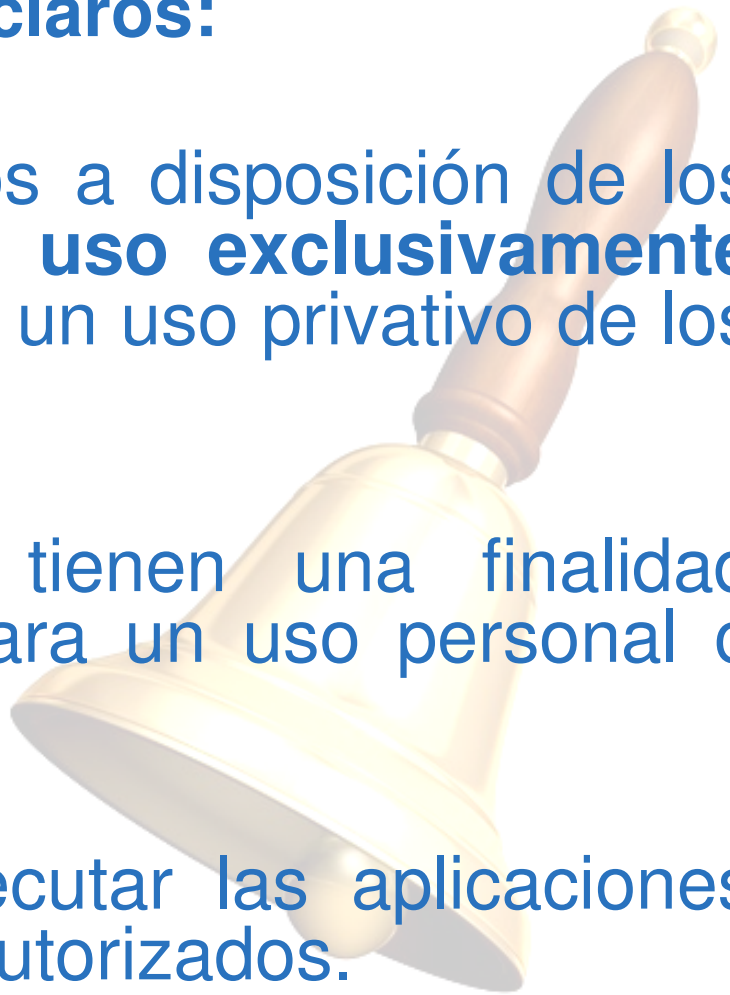
- **LOPD 15/1999.**
  - Artículo 9
- **Manual de Comportamiento de los Empleados Públicos en el uso de Sistemas.**
  - Artículos 4 y 5
- **Documento de Seguridad**
  - Funciones y Obligaciones del personal

CASO PRÁCTICO 7: Descargar música y software en el trabajo

Resumen:

Conceptos que hay que tener muy claros:

- Los equipos informáticos puestos a disposición de los usuarios están destinados a un **uso exclusivamente profesional** y éstos no gozan de un uso privativo de los mismos.
- Las aplicaciones informáticas tienen una finalidad profesional y no son idóneas para un uso personal o privado.
- Los usuarios se limitarán a ejecutar las aplicaciones informáticas para las que estén autorizados.



CASO PRÁCTICO 7: Descargar música y software en el trabajo

Casos similares:

- Instalación de Salvapantallas o fondos de escritorio con contenidos ofensivos, violentos u obscenos o que atenten contra la dignidad de las personas.
- Instalación de software de procedencia desconocida, software pirata…..
- Utilización de los sistemas de información corporativos para comprobar datos a petición de amigos o conocidos.
- Desactivación de los sistemas antivirus

CASO PRÁCTICO 7: Descargar música y software en el trabajo

Caso real:

La protección de datos

4.000 historias clínicas de abortos se filtran en la Red a través de eMule

Protección de Datos sanciona con 150.000 euros a un centro médico de Bilbao

MÓNICA C. BELAZA - Madrid - 25/04/2008

Descargarse música o películas desde el ordenador del trabajo a través de un programa de intercambio de archivos puede tener efectos trágicos y no sólo para quien quizá sólo pretendía meter en su MP3 una canción de David Bisbal. Un error de este tipo ha podido provocar que 11.300 historias clínicas, de ellas 4.000 de casos de aborto, acaben expuestos ante cualquier internauta.

El desconocimiento tecnológico de algún empleado de una clínica ginecológica pudo llevarle a poner a disposición del programa eMule (el más popular de intercambio de archivos entre particulares), y por lo tanto al alcance de millones de personas, todos estos datos, contenidos en una carpeta del disco duro de su ordenador. No se sabe con exactitud quién ha sido el culpable, ni las razones de la filtración, pero la Agencia Española de Protección de Datos (AEPD) acaba de sancionar a la clínica, el

Descargas en la Red

- Atención al marcar la casilla
- Domicilio y teléfono de afiliados sindicales
- Un becario que deja ver datos de clientes

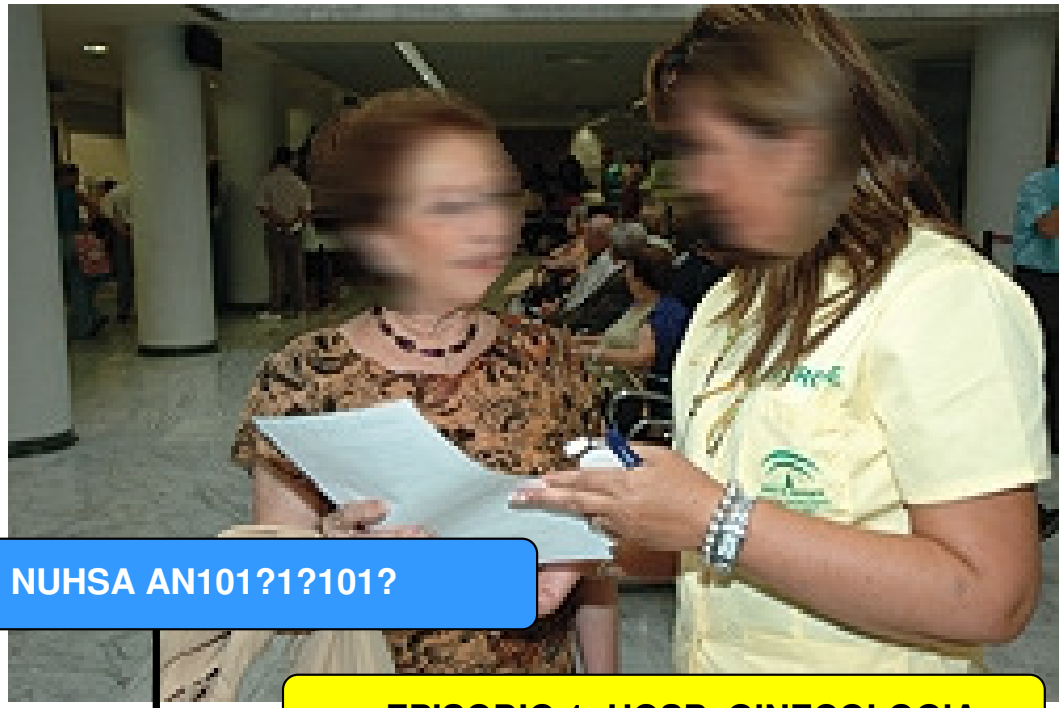
La noticia en otros webs

¿Te gustaría encontrar tu Historia Clínica en Internet?

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Un paciente se dirige a uno de nuestros mostradores para solicitar que se eliminen de su historial unos episodios de urgencias concretos.

El paciente asegura que en esas fechas no ha estado en urgencias y que esos episodios no le corresponden.



- NUHSA AN101?1?101?
  - EPISODIO 1: HOSP. GINECOLOGIA
  - EPISODIO 2: CCEE OFTALMOLOGÍA
  - EPISODIO 3: URGENCIAS
  - EPISODIO 4: URGENCIAS X

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

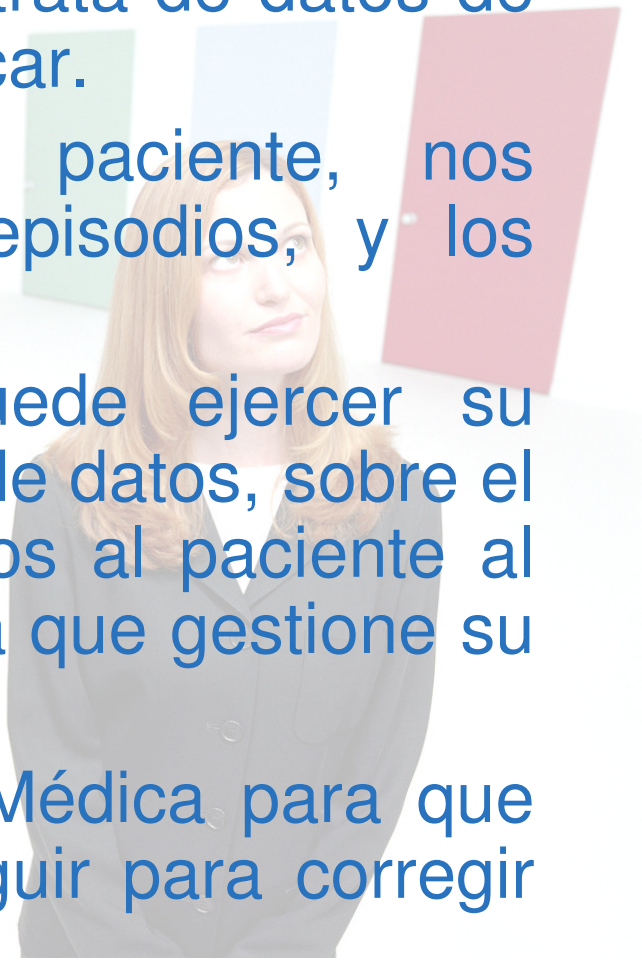
Opciones:

a) Informamos al paciente de que no es posible eliminar datos de su historial clínico ya que se trata de datos de salud y no se pueden eliminar ni modificar.

b) Tras comprobar la identidad del paciente, nos aseguramos de que existen esos episodios, y los eliminamos del sistema sin más

c) Informamos al paciente de que puede ejercer su derecho de rectificación y cancelación de datos, sobre el procedimiento para ejercerlo y dirigimos al paciente al Servicio de Atención al Ciudadano para que gestione su petición.

d) Enviamos al paciente a la Dirección Médica para que informen sobre el procedimiento a seguir para corregir sus datos.



CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Dudas del profesional:

- **¿ Y si el usuario que solicita el cambio no es el propio paciente?**

  Los derechos de acceso, rectificación, cancelación y oposición **son personalísimos** y será ejercidos por el afectado. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Dudas del profesional:

- **¿Y si la solicitud nos llega por otros medios distintos al servicio de Información del Centro, o presento su solicitud en un mostrador equivocado?**

  Debemos atender la solicitud aun cuando el usuario no hubiese utilizado el procedimiento establecido, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud y que esta cumpla los requisitos necesarios. Además, **cualquier personal con acceso a datos de carácter personal** tiene la obligación de conocer el procedimiento para el ejercicio de los derechos del usuario.

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Dudas del profesional:

- **¿Y si no tenemos datos de dicho paciente?**

  Tenemos la **obligación legal de contestar** a la solicitud independientemente de si tenemos datos personales del paciente o no

- **¿Y si la solicitud presentada no cumple con los requisitos exigidos por la ley?**

  Tenemos la **obligación legal de ponernos en contacto con el usuario** y requerir la subsanación de los errores detectados en su solicitud.

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Dudas del profesional:

- **¿Y si un paciente se acerca a información para pedir que le demos todos sus datos?**

  El paciente tiene el derecho de acceso a sus datos, el tratamiento de que está siendo objeto, el origen de dichos datos y las comunicaciones realizadas o previstas de sus datos.

- **¿Puede excluirse alguna información?**

  El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Dudas del profesional:

- **¿Puedo mostrarle al usuario sus datos usando una de nuestras pantallas para ello?**

Podemos dar la información solicitada al usuario mediante:

- Visualización en pantalla
- Escrito, copia o fotocopia remitida por correo, certificado o no
- Telecopia
- Correo electrónico u otros sistemas de comunicación electrónicos
- Cualquier otro sistema adecuado ofrecido por el responsable del fichero
- En cualquier caso, nos corresponde a nosotros demostrar la prueba de cumplimiento del deber de respuesta

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Dudas del profesional:

- **Pero tenemos tantos sistemas y ficheros.... ¿Tengo que darle todos los datos de todos los sistemas de información que disponemos?**

  El usuario puede solicitar el acceso a todos sus datos o a una parte de ellos. En circunstancias de especial complejidad que lo justifiquen, podremos solicitar del afectado la especificación de los ficheros respecto de los cuales quiere ejercitar su derecho. en cuyo caso, tendremos que facilitarle una relación de todos ellos.

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Dudas del profesional:

- **¿De cuanto tiempo disponemos para contestar a la solicitud de acceso a sus datos de un usuario?**

  El plazo máximo establecido por la ley es de **un mes** (de fecha a fecha), aún en el caso de no disponer de datos de carácter personal del usuario que lo solicita.

- **¿Y si el paciente lo que quiere es que elimine todos sus datos de nuestros sistemas?**

  La cancelación de los datos de carácter personal no procederá cuando éstos deban ser conservados durante los plazos previstos por la ley o debido a las relaciones contractuales entre las partes que justifican el tratamiento de los datos.

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Dudas del profesional:

- **¿Y cuando un paciente ingresado no desea que nadie conozca su estancia en el centro?**

  El paciente podrá ejercer su **derecho de oposición** como consecuencia de motivos legítimos y fundados, referidos a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Normativa aplicable:

- Consentimiento informado en materia de protección de datos
  - LOPD 15/1999. Títulos II y III
  - RD 1720/2007. Título III
  - LAP 41/2002. Art. 4, 5 y 18
  - LGS. Art. 10
- Documento de Seguridad
  - Figura del Responsable de Seguridad
  - Procedimiento para el Ejercicio de los Derechos de Oposición, Acceso, Rectificación o Cancelación de Datos de Carácter Personal

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Casos similares:

- Solicitudes de copias de historia clínicas
- Modificación o Eliminación de informes clínicos erróneos
- Solicitud de restricción de acceso a la información de un paciente hospitalizado
- Solicitud de accesos a la historia clínica de un paciente

CASO PRÁCTICO 8: Ejercicio del derecho de rectificación de datos

Resumen:

Conceptos que hay que tener muy claros:

- El usuario tiene los derechos de Acceso, Rectificación, Cancelación y Oposición (**ARCO**) que puede ejercer en cualquier momento
- La organización tiene la obligación de disponer y regular los procedimientos para el ejercicio de estos derechos por parte de los usuarios.
- Disponemos de **diez días hábiles** para responder a los derechos de rectificación, cancelación y oposición y de **un mes** para el derecho de acceso.
- El silencio administrativo no es posible en el ejercicio de estos derechos.

CASO PR… …e datos

Caso re…

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Procedimiento Nº: TD/00067/2008

RESOLUCIÓN Nº.: R/00608/2008

Vista la reclamación formulada por **D. J.J.J.**, contra el **Consorcio Hospital General Universitario de Valencia**, y en base a los siguientes,

HECHOS

En fecha 13 de diciembre de 2007, tuvo entrada en esta Agencia reclamación de D. J.J.J. contra el Consorcio Hospital General Universitario de Valencia por no haber sido debidamente atendido su derecho de acceso.

Realizadas las actuaciones procedimentales previstas en el artículo 17 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), se han constatado los siguientes

CASO PRÁCTICO 9: Videovigilancia

La Comisión de Dirección de un centro sanitario está pensando en instalar cámaras de videovigilancia para proteger las instalaciones, el equipamiento y garantizar la seguridad de las personas.

CASO PRÁCTICO 9: Videovigilancia

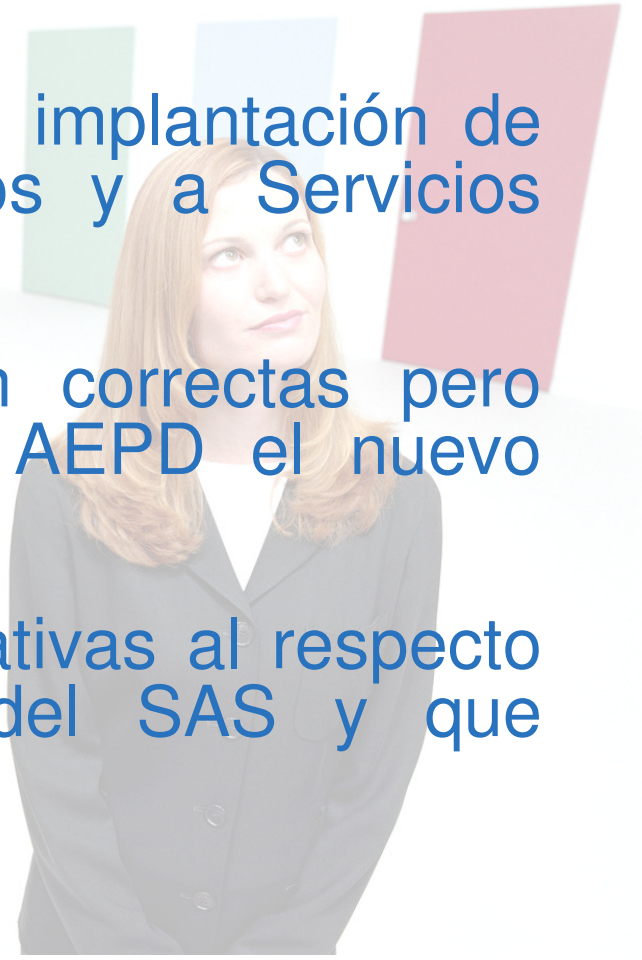
Opciones:

a) Delegar la implantación y gestión a la empresa privada de seguridad contratada por el centro.

b) Encargar al Servicio de Informática la implantación de los dispositivos y recursos necesarios y a Servicios Generales su gestión.

c) Tanto la opción a) como la b) son correctas pero además habría que comunicar a la AEPD el nuevo fichero.

d) Proceder acorde a las normas corporativas al respecto que marca la Secretaría General del SAS y que desarrolla la UGRD.



CASO PRÁCTICO 9: Videovigilancia

Dudas del profesional:

¿Hay condiciones a considerar antes de implantar un sistema de videovigilancia?

- Toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.
- El uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

CASO PRÁCTICO 9: Videovigilancia

Dudas del profesional:

¿Qué pasos debo seguir para actuar correctamente?

- Contactar con la UGRD para asesoramiento e información.
- Las videocamaras deben estar homologadas por la CEE.
- La empresa de seguridad instaladora/gestora debe estar autorizada por el Ministerio del Interior si el sistema conecta con central de alarmas.
- Se debe informar a los empleados de la intención de instalar cámaras y de quien es el responsable del fichero.
- Comunicar a los representantes de los trabajadores esta decisión.
- Tener a disposición de los interesados impresos informativos e impresos para el ejercicio de sus derechos.
- Instalar distintivos/carteles según formato de la AEPD.
- Realizar copias de respaldo de las imágenes grabadas al menos semanalmente.
- Mensualmente deberán cancelarse (bloquearse) los datos grabados.

CASO PRÁCTICO 9: Videovigilancia

Dudas del profesional:

¿Quién se encarga de publicar en BOJA el fichero de videovigilancia?, ¿quién lo notifica a la AEPD?

- La UGRD elaborará un borrador de documento para su publicación.
- La Subdirección de Ordenación y Organización de la Secretaría General del SAS formaliza el borrador y emite los informes correspondientes.
- Secretaría General aprueba y traslada la publicación a la Dirección Gerencia del SAS.
- Dirección Gerencia aprueba y traslada la publicación a la Consejera de Salud quien finalmente firma la publicación.
- La notificación a al AEPD la lleva a cabo la UGRD por delegación del Responsable del Fichero a través del sistema NOTA.

CASO PRÁCTICO 9: Videovigilancia

Dudas del profesional:

¿Qué implicaciones tiene el hecho de que las videocámaras sólo captaran imágenes para su reproducción?

- Cuando sólo se reproducen las imágenes captadas en tiempo real, sin proceder a la grabación o almacenamiento de las mismas, no es necesario publicar y notificar el fichero.
- Al no existir fichero, no proceder el ejercicio de los derechos ARCO.

- **¿Es necesario informar sobre la ubicación de las videocámaras atendiendo a LOPD?**

- No, solo se establece que debe colocarse un distintivo informativo en lugar visible, tanto en espacios abiertos como cerrados.

CASO PRÁCTICO 9: Videovigilancia

Dudas del profesional:

¿Es necesario el consentimiento escrito de los profesionales que aparecen en las imágenes grabadas?

- El Estatuto de los Trabajadores (ET) faculta al "empresario" para adoptar las medidas oportunas de vigilancia para verificar el cumplimiento de las obligaciones laborales, guardando la consideración debida a la dignidad humana...

- El ET legitima el tratamiento de imágenes sin consentimiento sólo si el trabajador ha sido debidamente informado mediante al menos un distintivo informativo en lugar visible e impresos a disposición de los trabajadores en los que se detalle la información del art. 5.1 - LOPD.

- Además, los datos no podrán ser utilizados para fines distintos a los antes descritos.

CASO PRÁCTICO 9: Videovigilancia

Dudas del profesional:

¿En algún momento se han de borrar las imágenes grabadas?

- El plazo máximo que se establece para la "cancelación" de los datos es de un mes. Esto debe entenderse como un bloqueo y no como un borrado.
- La eliminación real de la información estará sujeta a los plazos de prescripción de responsabilidades (20 años como máximo para delitos penales) en el caso de que estas hubieran surgido durante el periodo de conservación de las imágenes.
- La copia de respaldo de la grabación está sometida a los mismos plazos para la supresión de los datos que el original.

CASO PRÁCTICO 9: Videovigilancia

Dudas del profesional:

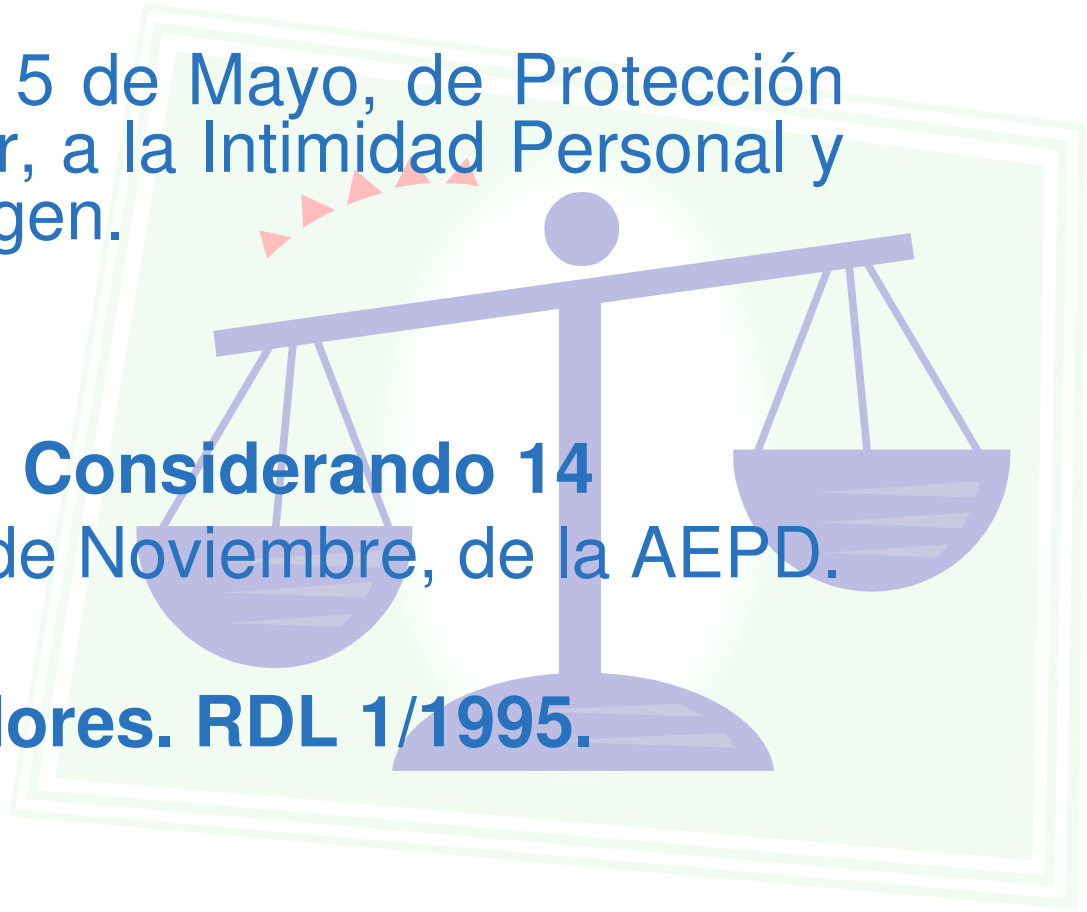
¿Puede grabarse cualquier lugar dentro del espacio de trabajo?

- No, la instalación deberá atenerse a la verificación del cumplimiento de las obligaciones, a razones de seguridad laborales y en especial velar porque se garantice la intimidad.

- Estará terminantemente prohibida la grabación en aquellos espacios del lugar de trabajo donde pudiera vulnerarse la dignidad del sujeto grabado, como pudieran ser vestuarios, baños, duchas,...

CASO PRÁCTICO 9: Videovigilancia

Normativa aplicable:



- **Ley Orgánica 1/1982** de 5 de Mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.
- **LOPD 15/1999.**
  - Artículo 3. Definiciones
- **Directiva 95/46/CE en su Considerando 14**
- **Instrucción 1/2006** de 8 de Noviembre, de la AEPD.
- **Ley 25/2009** (Ómnibus)
- **Estatuto de los Trabajadores. RDL 1/1995.**
  - Artículo 20.3

CASO PRÁCTICO 9: Videovigilancia

Resumen:

Conceptos que hay que tener muy claros:

- Actuar según normas corporativas. Consultar a la UGRD.
- Verificar la homologación de las videocamaras.
- Verificar la autorización de la empresa de seguridad encargada si hay conexión con central de alarmas.
- Establecer un contrato de encargado de tratamiento.
- Informar a empleados y representantes de los mismos.
- Disponer de impresos para el ejercicio de derechos.
- Instalar distintivos en los lugares adecuados
- Cumplir con los procedimientos y plazos de grabación y copia de respaldo.

CASO PRÁCTICO 9: Videovigilancia

Caso real:

EL PAÍS edición impresa | ANDALUCÍA — Jueves, 16/4/2009

Primera Internacional España Economía Opinión Viñetas

Vida&artes Sociedad Cultura Tendencias Gente Obituarios Deportes Pantallas Última

ELPAIS.com > Edición Impresa > Andalucía >

Protección de Datos cuestiona la videovigilancia del Virgen del Rocío

La Agencia estatal abre un proceso contra el SAS por dos infracciones graves

REYES RINCÓN - Sevilla - 27/03/2009

Vota ☆☆☆☆☆ | Resultado ★★★★★ 0 votos

La Agencia Española de Protección de datos ha abierto un procedimiento de infracción contra el Hospital Virgen del Rocío de Sevilla por incumplir la normativa de videovigilancia en las cámaras instaladas en el centro. Según el acuerdo de la agencia estatal, fechado el pasado 16 de marzo, el Servicio Andaluz de Salud (SAS), podría haber cometido dos infracciones que la Ley Orgánica de Protección de Datos tipifica como graves. La administración tiene 15 días para presentar alegaciones.

La noticia en otros webs
webs en español
en otros idiomas

La investigación de la Agencia llegó tras la denuncia presentada en junio de 2007 por dos trabajadores del Virgen del Rocío, a los que la dirección del hospital abrió un expediente, tras identificarlos, a través de las cámaras de seguridad, como responsables de unos incidentes enmarcados en las movilizaciones que entonces mantenían los médicos de Urgencias por la falta de medios. Los expedientados denunciaron que las grabaciones incumplían la ley y la agencia tiene indicios de que llevaban razón.

El SAS supuestamente incumplió el artículo 20 de la ley estatal, que hace referencia a que la creación de ficheros de titularidad pública o el inicio de recogida de datos personales debe anunciarse antes en el Boletín Oficial del Estado o de la Comunidad. Según el acuerdo de la Agencia Estatal, cuando representantes de este organismo se desplazaron al Virgen del Rocío para inspeccionar el sistema de videovigilancia, los responsables del hospital les explicaron que todavía se estaba elaborando la disposición legal que acreditaba la creación del fichero en el que se almacenan las imágenes de las cámaras. Es decir, el sistema empezó a funcionar sin que se hubiera cumplido este paso legal.

Asimismo, la agencia considera que pudo incumplirse el artículo 6.1 de la ley, que señala que el tratamiento de los datos personales "requerirá el

PARA SUSCRIPTORES edición en PDF
Descubre nuestro visor de la edición impresa. Permite visualizarla y descargarla
ver demo > SUSCRÍBASE

la tienda EL PAIS.com
Litografía Subirachs. Edición Limitada.
Precio 450 €

Lo más visto | ...valorado | ...enviado
La talentosa 'friki' que hace llorar a Demi Moore
Sarkozy: "Puede que Zapatero no sea muy inteligente"
Una dramática subida del mar que podría repetirse
La amenaza de la extrema derecha se extiende en EE UU
Cercas: "El Rey hizo cosas en el 23-F que no debería haber hecho"

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Una chica de 15 años acude sola al Servicio de Urgencias de un centro sanitario para solicitar asistencia médica.

La joven, en apariencia consciente de sus actos, presenta una herida leve en la cabeza.

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

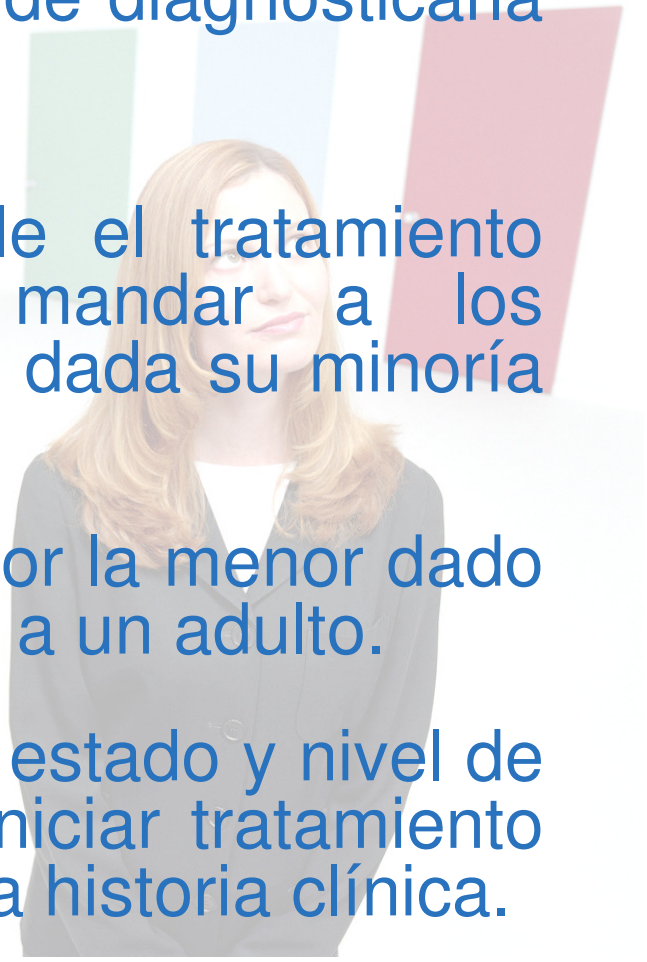
Opciones:

a) El profesional alude la necesidad de llamar a los padres o tutores de la menor (15 años) antes de diagnosticarla y tratarla.

b) Diagnosticar a la menor y prescribirle el tratamiento correspondiente y posteriormente mandar a los padres/tutores informe de la asistencia dada su minoría de edad.

c) Proporcionar el tratamiento requerido por la menor dado que su edad, según la LAP, la equipara a un adulto.

d) Entrevistarse con la menor, verificar su estado y nivel de madurez, informarle y recomendarle, iniciar tratamiento si procede de lo anterior y registrar en la historia clínica.



CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

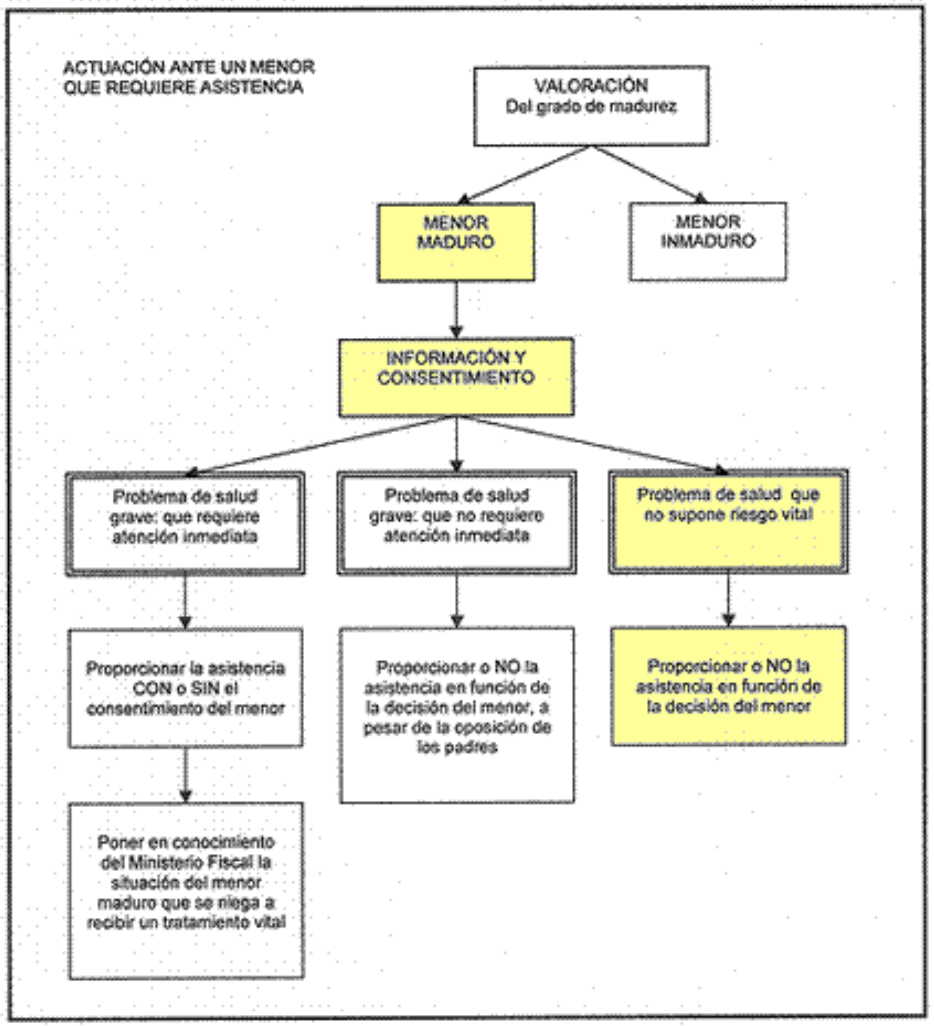
Dudas del profesi

¿Cómo debo [illegible] ue requiere asistencia?

Esquema 1

Actuación ante un menor que requiere asistencia

(Modificado de: Servicio de Responsabilidad Profesional del Colegio de Médicos de Barcelona. Asistencia a Menores, adolescentes y Malos Tratos. Diario Médico. 2003)



CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Dudas del profesional:

¿Cómo determino la MADUREZ del menor en cuestiones que afecta a su salud (p.e. realización de diagnósticos o tratamientos médicos?

- Entre los 12 y 16 años procede la valoración de madurez.
- Los criterios que han sido propuestos para establecer el grado de madurez incluyen: comprensión adecuada de la información dada y de su situación, capacidad de fundamentar de modo razonable los motivos de su decisión y de ponderar los riesgos y beneficios de la misma .
- Si existen dudas, se puede obtener la opinión de otro profesional sanitario (psicólogos, psiquiatras,…)

Scielo España

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Dudas del profesional:

¿Cómo determino la MADUREZ en cuestiones que afecta al tratamiento de datos de carácter personal (p.e. derechos ARCO o cesiones de datos)?

- El ordenamiento jurídico español reconoce en los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil.
- …la minoría de edad no supone una causa de incapacitación, por lo que aquélla habrá de ser analizada en cada caso concreto a los efectos de calificar la suficiencia en la prestación del consentimiento en atención a la trascendencia del acto de disposición y a la madurez del disponente.

- Por tanto, los mayores de 14 disponen de las condiciones de madurez para prestar el consentimiento al tratamiento. Los menores de 14 precisan evaluación de madurez.

AEPD – Informe 2008-0114

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Dudas del profesional:

¿Puedo informar a los padres/tutores del menor maduro?

- Disponer de la información sanitaria de los hijos es fundamental para poder velar adecuadamente por la salud de los mismos, por ello, la AEPD entiende que el Código Civil (art. 154) habilita la cesión de la información sanitaria a quienes ostenten la patria potestad (no a cualesquiera familiares).

  AEPD – Informe 2008-0114

- Hay que actuar de forma diferente ante la sospecha, con datos objetivos, de maltratos o abusos. Asesoramiento Servicios Sociales.

- Mientras hay un proceso de separación, puede que uno de los padres pida información sobre su hijo/a para utilizarla en el procedimiento legal. Tanto si el menor es maduro como si es inmaduro, se dará la información estrictamente necesaria a los tutores (habitualmente los dos padres), evitando, entrar en dinámicas que faciliten convertir el/la menor en excusa para la disputa.

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Dudas del profesional:

¿Qué consecuencias puedo tener si actúo acorde a los criterios del menor maduro?

- Dado que el menor de edad puede prestar su consentimiento en el tratamiento o utilización de fármacos una vez considerado maduro por el médico, éste queda exento de consecuencia jurídica alguna siempre que:
  - actúe con arreglo a lo establecido en la LAP, artículos:
    - 8 sobre el consentimiento informado
    - 9 sobre límites del consentimiento informado y representación.
    - 10 sobre condiciones de la información y consent. escrito …
  - y anote en la historia clínica los criterios objetivos que le sirvieron para considerar la madurez del menor de 16 años.

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Dudas del profesional:

¿El consentimiento médico del menor maduro es aplicable también a la IVE (interrupción voluntaria del embarazo)?

No, cierto es que la reforma de la ley del aborto o ley de plazos suprime el permiso paterno para que una joven mayor de 16 años pueda abortar.

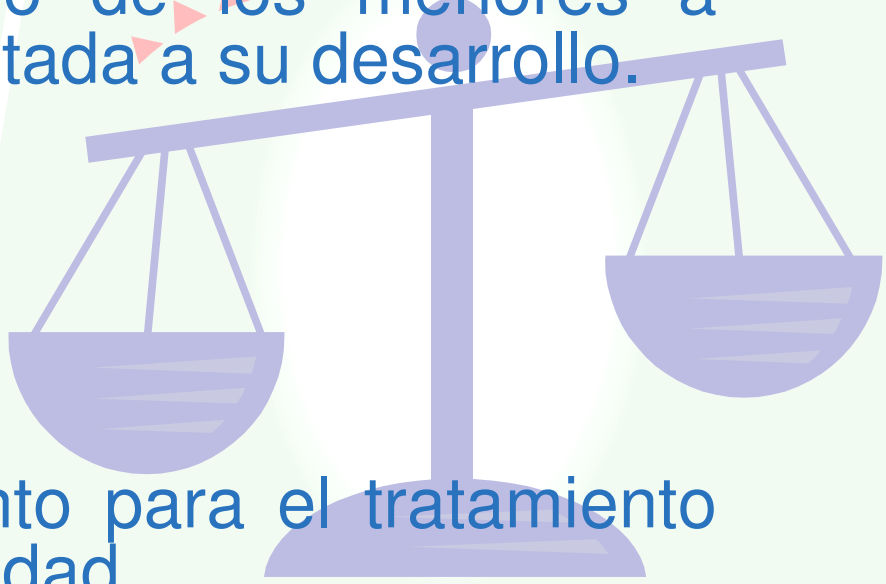
¿Y a los ensayos clínicos?

En estos temas, el consentimiento médico se rigen por lo establecido con carácter general sobre la mayoría de edad y por las disposiciones especiales de aplicación. Según el Código Civil, la mayoría de edad se alcanza a los 18 años.

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Normativa aplicable:

- **Código Penal y Código Civil**
- **Ley de Protección Jurídica del Menor**
- **Decreto 246/2005,** derecho de los menores a recibir atención sanitaria adaptada a su desarrollo.
- **Ley General de Sanidad**
- **Constitución Española**
  - Artículo 10.1
- **RD 1720/2007**
  - Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.
- **LAP 41/2002.**
  - Artículo 5, 3.



CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Casos similares:

- PROBLEMAS DE SALUD QUE NO SUPONE RIESGO VITAL
  - Heridas o traumas leves.
  - Chequeos médicos.
  - Análisis de embarazo positivo.
  - Alergias
  - Contagios

- PROBLEMAS DE SALUD GRAVE QUE NO REQUIEREN ATENCIÓN INMEDIATA
  - Tumor
  - VIH

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Resumen:

Conceptos que hay que tener muy claros:

- La edad del menor es muy relevante en estos casos.
- Debe existir un procedimiento claro dentro del centro de actuación ante asistencia a menores.
- El menor maduro tiene capacidad de consentir tratamiento de DCP y tratamiento sanitario.
- Es posible informar a los padres o tutores, bien por iniciativa del profesional o bien por el ejercicio del derecho de acceso de estos.
- No todos los procesos asistenciales se rigen por estas pautas. Abortos, ensayos clínicos y técnicas de reproducción asistida.

CASO PRÁCTICO 10: Menor agredida atendida en Urgencias

Caso real:

AGENCIA ESPAÑOLA DE PROTECCIÓN

Gabinete Jurídico

madrid.org

Tamaño texto -a a +a

Agencia de Protección de Datos de la Comunidad de Madrid

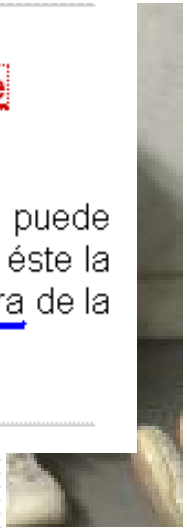
La Agencia | Derechos Ciudadanos | Consultas | Registro Ficheros | Servicios | Actualidad | Legislación | Resolu
Publicaciones

APDCM > Resoluciones

La carencia de medidas de gestión adecuadas de datos de carácter personal puede suponer una conculcación de la finalidad perseguida por el artículo 1 LOPD

La APDCM declara la existencia de una infracción grave al apreciar que, si bien no se puede imputar una pérdida de datos al responsable del fichero, sin embargo, sí le es imputable a éste la carencia de medidas organizativas en relación con las necesarias indicaciones a la pediatra de la menor para el adecuado acceso al contenido íntegro de la historia clínica de ésta.

que "El tutor está obligado a velar por el tutelado y, en particular (...) a educar al menor y procurarle una formación integral".



CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

En un Centro Médico de Atención Primaria, dos agentes de la Unidad de Policía Judicial de la Policía Autonómica, solicitan varios datos administrativos y de salud de un paciente.

Los agentes no disponen de mandamiento judicial ni requerimiento previo del Ministerio Fiscal.

CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

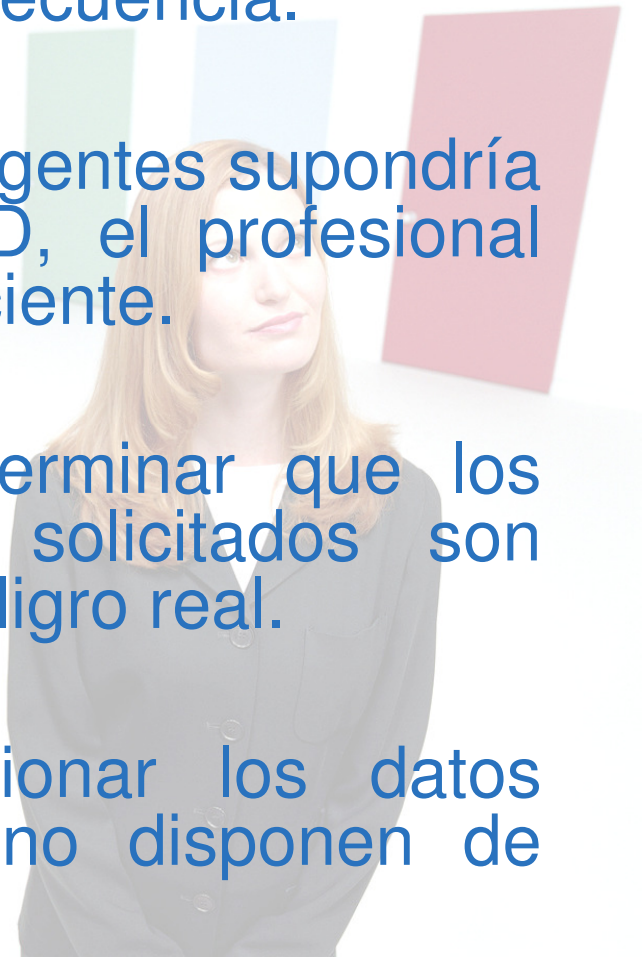
Opciones:

a) Tras consultar a su Responsable Funcional de Aplicación, el profesional actúa en consecuencia.

b) Puesto que atender la solicitud de los agentes supondría una cesión de datos según la LOPD, el profesional solicita el previo consentimiento del paciente.

c) Proporcionar la información tras determinar que los supuestos y categorías de datos solicitados son necesarios para la prevención de un peligro real.

d) El profesional se niega a proporcionar los datos solicitados puesto que los agentes no disponen de mandato judicial.



CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

Dudas del profesional:

¿Qué debo tener en cuenta antes de entregar los datos?

- Debe quedar acreditado que la obtención de los datos resulta necesaria para la **prevención de un peligro** real y grave para la seguridad pública o para la **represión de infracciones penales**.
- Tratándose de datos especialmente protegidos, estos deben ser **absolutamente necesarios** para los fines de una investigación concreta.
- Se debe tratar de una **petición concreta y específica**, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.
- La petición se debe efectuar con la **debida motivación**, que acredite su relación con los supuestos que se han expuesto.

Informe 133/2008 de la AEPD

CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

Dudas del profesional:

¿Qué sucede con los datos una vez en poder de la Unidad de Policía Judicial?

- Los datos deben ser **cancelados** "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".

- La Policía Judicial está obligada a dar cuenta de los hechos a la Autoridad Judicial y Fiscal de forma inmediata (art. 549.1 de la Ley Orgánica del Poder Judicial), por tanto la cancelación de datos se tornará en **destrucción** una vez producida esa comunicación (cesión).

- Conforme dispone el artículo 11.2 d) de la Ley Orgánica 15/1999, **procederá la cesión** si ésta tiene por destinatario al Ministerio Fiscal o los Jueces o Tribunales.

CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

Dudas del profesional:

Entonces, ¿estoy obligado a dar información a la Unidad de Policía Judicial siempre?

- No, sólo en relación con aquellos supuestos en los que la Policía Judicial requiere la cesión de los datos con el fin de ejercitar las funciones de averiguación del delito y detención del responsable, y no existir en ese caso mandamiento judicial o requerimiento del Ministerio Fiscal que dé cobertura a la cesión.

¿La Policía Nacional o Local y la Guardia Civil merecen la misma consideración que la Policía Judicial?

- En este caso, a juicio de la AEPD, nos encontramos ante el ejercicio por los efectivos de la Policía Judicial de funciones que, siéndoles expresamente reconocidas por sus disposiciones reguladoras, se identifican con las atribuidas, con carácter general, a todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

Dudas del profesional:

Concretamente, ¿debo facilitar a la Unidad de Policía Judicial copia de los partes de lesiones extendidos a ciudadanos que son presentados por la policía para reconocimiento médico?

- En el supuesto planteado el parte de lesiones es recabado por la policía con el objeto de elaborar el atestado con las diligencias practicadas, que debe remitirse a la autoridad judicial en un plazo máximo de 24 horas, según el artículo 295 de la Ley de Enjuiciamiento Criminal. Por lo tanto, el requisito de la existencia de una investigación concreta queda cumplido y, de acuerdo con esto, los centros de salud deben facilitar a la policía judicial una copia de los partes de lesiones.
- Debe recordarse que, si bien la LOPD facilita a las Fuerzas y Cuerpos de Seguridad el tratamiento de los datos necesarios en el ejercicio de sus funciones, no ampara el mantenimiento indefinido de los mismos.

CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

Dudas del profesional:

Concretamente, ¿debo facilitar a la Unidad de Policía Judicial copia de los partes de lesiones extendidos a ciudadanos que son presentados por la policía para reconocimiento médico?

- En relación a esta copia, y con el fin de agilizar el trámite de recepción en el Órgano Judicial, la Ley Orgánica 8/2002, de 24 de Octubre, complementaria de la Ley de reforma parcial de la Ley de Enjuiciamiento Criminal, sobre procedimiento para el enjuiciamiento rápido e inmediato de determinados delitos y faltas y de modificación del procedimiento abreviado ("Ley de juicios rápidos") establece en su artículo 796.1.1ª que "la Policía Judicial solicitara del facultativo o personal sanitario que atendiere al ofendido, copia del informe relativo a la asistencia prestada para su unión al atestado policial", no suponiendo la entrega del parte una inobservancia del deber de sigilo profesional, tratándose de un claro ejemplo de secreto derivado.

El Médico. Formación Práctica en Bioética en Atención Primaria

(2 de 2)

CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

Dudas del profesional:

¿Qué procedimientos del Documento de Seguridad estoy obligado a cumplir?

Además de las consideraciones anteriores se debe cumplir con:

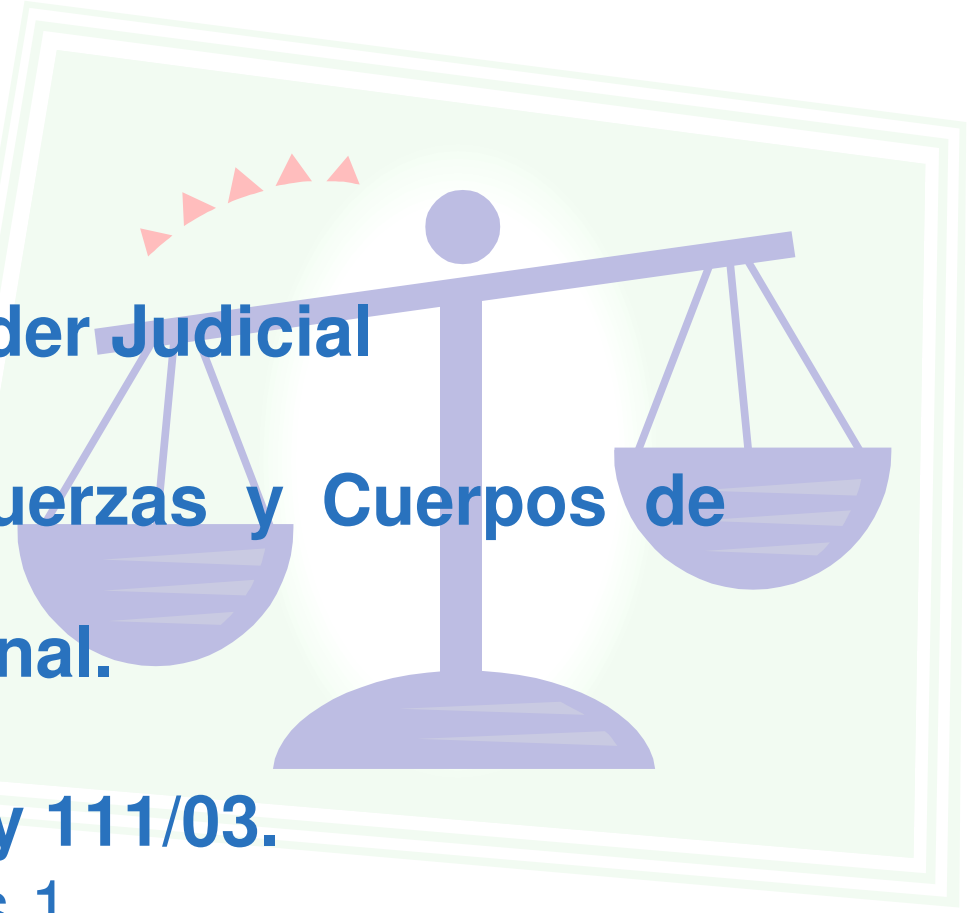
- El **procedimiento para la cesión de datos**, haciendo uso del formulario para la cesión de datos a las Fuerzas y Cuerpos de Seguridad.

- El **procedimiento de gestión de soportes**, resaltando el apartado de entrada/salida y el registro asociado donde debe hacerse constar información relativa a: *tipo de soporte, fecha y hora de entrada o salida, emisor, destinatario, identificación del soporte, descripción breve del contenido y forma de envío.*

CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

Normativa aplicable:

- **LOPD 15/1999**
  - Artículos 11.2 y 22.2
- **RD 1720/2007**
  - Artículo 10
- **Ley Orgánica 6/1985 del Poder Judicial**
  - Artículo 549.1
- **Ley Orgánica 2/1986 de Fuerzas y Cuerpos de Seguridad.**
- **Ley de Enjuciamiento Criminal.**
  - Artículos 295, 796.1.1ª
- **Resoluciones SAS 0023/01 y 111/03.**
  - Instrucción octava, puntos 1.



CASO PRÁCTICO 11: Solicitud de datos por la Policía Judicial

Casos similares:

El presente caso, dada la especificidad del mismo, sólo da cobertura a las solicitudes de datos provenientes de las Fuerzas y Cuerpos de Seguridad, a saber:

- Fuerzas y Cuerpos de Seguridad del Estado, dependientes del Gobierno de la nación
  - **Guardia Civil**
  - **Cuerpo Nacional de Policía**
- Cuerpos de Policía dependientes de las Comunidades Autónomas
  - **Policía Autónoma** (Ertzaintza, Policía Foral, Mozos de Escuadra, BESCAM)
- Cuerpos de Policía dependientes de las Corporaciones Locales
  - **Policía Local, Municipal o Guardia Urbana**

TIPO DE DATO	COMISIONADOS[1]	CUERPO POLICIAL	UNIDAD DEL CUERPO POL.	COMPETENCIAS DE LA UNIDAD	REQUISITOS
De Salud	NO	Policía Nacional	Policía Judicial	Investigar cualquier delito	Acreditar la absoluta necesidad de los datos para los fines de una investigación concreta.
		Guardia Civil	Policía Judicial	Investigar cualquier delito	
		Policía Autonómica	Policía Judicial[2]	Investigación por: - Violencia de género - Violencia familiar - Violencia escolar - Protección de menores	
		Policía Local	Policía Judicial[2]	Investigar cualquier delito	
			Atestados	Tráfico y seguridad vial: - Análisis de alcohol en sangre y orina. Test de alcoholemia	
	SI	Todos	Policía Judicial	Las que expresamente les encomiende la resolución de comisionamiento dictada	Aportar orden judicial o requerimiento previo del Tribunal o el Ministerio Fiscal
Administrativo	NO	Policía Nacional	Todas	- Prevención de un peligro real y grave para la seguridad pública - Represión de infracciones penales	- Acreditar la prevención de un peligro real y grave para la seguridad pública o la represión de infracciones penales - Justificar investigación
		Guardia Civil			
		Policía Autonómica			
		Policía Local			
	SI	Todos	Todas	Las que expresamente les encomiende la resolución de comisionamiento dictada	Aportar orden judicial o requerimiento previo del Tribunal o el Ministerio Fiscal

[1] Funcionarios policiales que actúan como representantes de las autoridades judiciales o fiscales.
[2] La función de Policía Judicial corresponde sólo a las Fuerzas de Seguridad del Estado. La Policía autonómica y local ejerce como colaboradora.

CASO PRÁC licía Judicial

Caso real:

Solicitudes de datos
judicial o requerimien

Se ha planteado por di
efectuadas por miemb
funciones de Policía Ju
jurisdiccional o requer
datos, llevando a cab
superior jerárquico.

En este caso nos enc
Judicial de funciones
disposiciones regulad
general, a todos los r
Estado, por lo que resu
el artículo 22.2 de
automatizado para fin
Fuerzas y Cuerpos
afectadas, están limit
resulten necesarios p
seguridad pública o p
almacenados en fich
clasificarse por categor

El citado artículo habili
y tratamiento de los da
de la cesión instada, si

a) Que quede debidar
necesaria para la pre
pública o para la repre
especialmente protegi
una investigación conc

b) Que se trate de una
lo señalado anteriorme

c) Que la petición se ef
con los supuestos que

d) Que, en cumplimi
cancelados "cuando nc
su almacenamiento".

Con referencia a la últ
tratándose de actuacio
consagradas en el apa
Judicial, la Policía Judi
la Autoridad Judicial y

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

Informe jurídico 0133/2008

La consulta plantea si la Agencia Española de Protección de Datos resulta competente para sancionar la actuación descrita en la misma conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

Se le comunica que la Agencia carece de competencia para sancionar la actuación descrita en la consulta, dado que no encaja en ninguno de los tipos de infracciones previstas en el artículo 44 de la citada Ley Orgánica.

No obstante, la Agencia se ha pronunciado en numerosas ocasiones sobre la obligación de comunicar los datos a la Policía Judicial, en relación con aquellos supuestos en los que la Policía Judicial requiere la cesión de los datos con el fin de ejercitar las funciones de averiguación del delito y detención del responsable, y no existir en ese caso mandamiento judicial o requerimiento del Ministerio Fiscal que dé cobertura a la cesión.

En este caso nos encontramos, a nuestro juicio, ante el ejercicio por los efectivos de la Policía Judicial de funciones que, siéndoles expresamente reconocidas por sus disposiciones reguladoras, se identifican con las atribuidas, con carácter general, a todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

Resultará, en consecuencia, aplicable a este segundo supuesto lo dispuesto en el artículo 22.2 de la Ley Orgánica 15/1999, según el cual "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad"

c. Jorge Juan 6
28004 Madrid
www.agpd.es

1

binete Jurídico

culo 22.2 de
.2 d) de la

sión de los
ulo 11.2 d),
este último
anifestadas

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

La Sección Sindical de CC.OO. de un Área de Gestión Sanitaria dirige escrito a la Dirección Económico-Administrativa en el que **solicita la plantilla de personal**, por categorías y servicios, ZBS, o dispositivos de apoyo, especificando el tipo de vinculación y fecha desde la que la persona se encuentra vinculada con contratos sucesivos al AGS sin cese efectivo.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

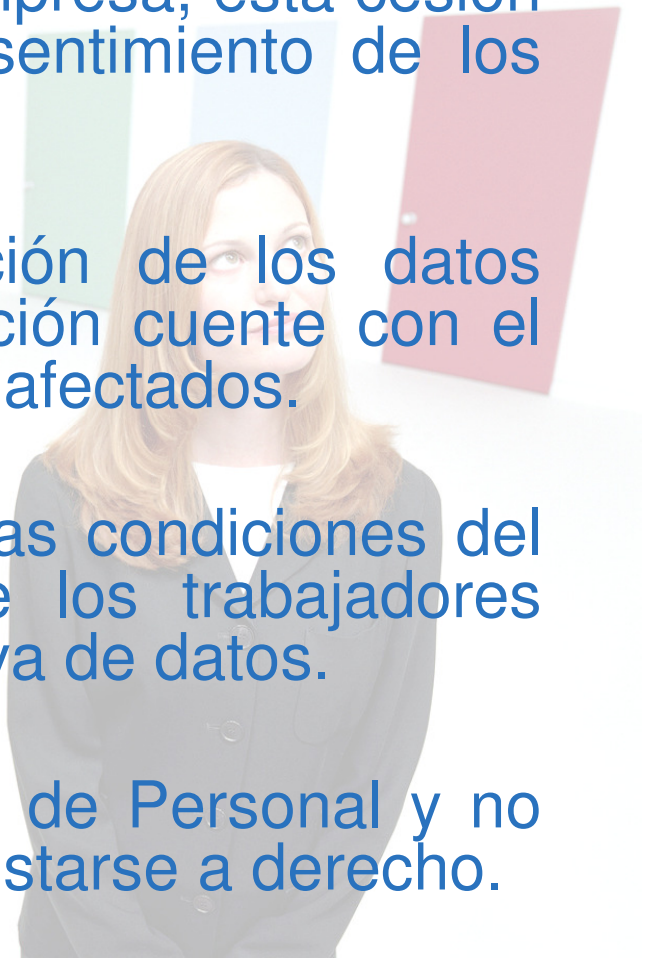
Opciones:

a) Atendiendo al Estatuto de los Trabajadores, al art. 64 que recoge las competencias del Comité de Empresa, esta cesión estaría habilitada sin necesidad del consentimiento de los afectados.

b) Es posible llevar a cabo la comunicación de los datos solicitados siempre y cuando la organización cuente con el consentimiento de todos y cada uno de los afectados.

c) La función de vigilancia y protección de las condiciones del trabajo propia de los representantes de los trabajadores puede llevarse a cabo sin una cesión masiva de datos.

d) La solicitud debe ser emitida por la Junta de Personal y no por la Sección Sindical de CC.OO. para ajustarse a derecho.



CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

¿Qué cesiones de datos de trabajadores están previstas cuando el trabajador del sindicato tiene la condición de personal funcionario de los Servicios de Salud?

- La única cesión prevista sería la derivada de las facultades atribuidas a los representantes de los trabajadores (los *Delegados de Personal* y la *Junta de Personal*, según el Estatuto Básico del Empleado Público).

¿Cuáles son esas facultades?

- Entre ellas está, además de la recepción de información, "vigilar el cumplimiento de las normas vigentes en materia de condiciones de trabajo, prevención de riesgos laborales, seguridad social y empleo, y ejercer, en su caso, las acciones legales oportunas ante los organismos competentes"

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

¿Cómo debo llevar a cabo la cesión de datos?

- La función de vigilancia y protección de las condiciones de trabajo, atribuida a las Juntas de Personal por la Ley 7/2007 puede llevarse a adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en el Órgano o Dependencia correspondiente. Sólo en el supuesto en que la vigilancia o control se refieran a un sujeto concreto, que haya planteado la correspondiente queja ante la Junta de Personal, será posible la cesión del dato específico de dicha persona.

- En caso de haber sido formalmente solicitada, procederá la cesión de los datos solicitados, siempre que los mismos sean cedidos de forma **disociada**, sin poder referenciar los datos a personas identificadas o identificables. En caso contrario, deberá recabarse el consentimiento de los interesados.

Informe Jurídico de la AEPD 2009-0118

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

Entonces, ¿son públicas las Relaciones de Puestos de Trabajo?

- Sí, pero las mismas no contendrán los datos del personal concreto que ocupe un determinado puesto de trabajo, sino exclusivamente las características de cada uno de los puestos de trabajo existentes en cada Dependencia Administrativa, siendo los datos personales referidos a cada funcionario público, de acceso restringido a éste último.

Ley 30/1984 de Medidas para la Reforma de la Función Pública.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

¿Aplica la disociación de datos a los listados del complemento de productividad?

- El Complemento de Productividad destinado a retribuir el especial rendimiento, la actividad extraordinaria y el interés o iniciativa con que el funcionario desempeñe su trabajo.

- La disociación de datos de los trabajadores únicamente quedará exceptuado en lo referente al complemento de productividad:

  "…en todo caso, las cantidades que perciba cada funcionario por este concepto serán de conocimiento público de los demás funcionarios del Departamento u Organismo interesado así como de los representantes sindicales".

Ley 30/1984 de Medidas para la Reforma de la Función Pública, artículo 23.3c.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

¿Aplica la disociación de datos a los listados del complemento de productividad?

- El la actualidad no existe base legal alguna para la cesión a los representantes sindicales de los datos referentes a las cantidades que perciben los funcionarios por complemento de productividad sin el consentimiento de los mismos.
- La entrada en vigor de la Ley 7/2007 EBEP, artículo 40, ha derogado el último párrafo del artículo 23.3c) de la Ley 30/1984 y el artículo 9.4.c) de la Ley 9/1987. Dejando sin efecto la obligación de informar a los representantes sindicales de los funcionarios las cantidades de productividad que percibe cada uno, pudiendo sólo conocer los criterios que se han tenido en cuenta en relación con los puestos de trabajo para conceder o no la productividad.

AEPD - Informe Jurídico 0275/2009, AEPD - Informe Jurídico 0343/2009, AEPD - Informe Jurídico 0137/2010.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

Respecto del cobro de la cuota sindical vía nómina, ¿qué procedimientos debe adoptar la organización?

- Es recomendable disponer de procedimientos de captación del consentimiento como impresos o modelos de solicitud en los que el trabajador autorice de modo expreso y por escrito el tratamiento. (El consentimiento es obligatorio)

- Es muy importante limitar el uso de estos datos a la finalidad para la que se han recabado: cobrar la cuota y transferir las cantidades a la organización sindical.

- Debe recordarse que si el tratamiento se da exactamente en los términos y para las finalidades aquí descritas el nivel de seguridad será básico.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

¿Los delegados sindicales pueden ver el parte de baja de un trabajador?

- El parte de baja es un documento susceptible de contener información sobre las enfermedades del trabajador.
- Para que un delegado sindical pueda consultar el parte de baja de un trabajador debe existir el consentimiento expreso del titular.

(Estos límites están recogidos en la Ley Orgánica 15/1999 que establece un régimen especial para el tratamiento y la comunicación de los datos de salud y, por otro lado, en la Ley 7/2007 reguladora del Estatuto del Empleado Público, que entre las funciones de los órganos de representación de los trabajadores no prevé que los delegados sindicales tengan acceso a dicha información.)

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

¿Porqué recibo información sindical en mi cuenta profesional de correo electrónico?

- Esta actividad requiere el tratamiento de datos personales puesto que una dirección electrónica es un dato personal.
- El envío de este tipo de mensajes de correo electrónico constituye un derecho de los sindicatos amparado por el derecho fundamental la libertad sindical. Sentencia del Tribunal Constitucional 281/2005
- Deben darse ciertas condiciones: la empresa debe disponer del servicio de correo electrónico y los envíos deben realizarse de modo proporcional y sin perjudicar el normal funcionamiento de la organización.
- Existen procedimientos automatizados (p.e.: listas de correo) que pueden permitir la satisfacción del derecho a la libertad sindical sin necesidad de realizar una cesión y, por tanto minimizando los riesgos y las obligaciones de cumplimiento normativo para el empresario y el sindicato.
- La celebración de elecciones sindicales legitima las cesiones de los datos censales necesarios para permitir al sindicato remitir información electoral y participar en el proceso electoral.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

¿Es lícita la publicación de datos personales en tablones?

- La Ley Orgánica de Libertad Sindical reconoce un derecho a disponer de un tablón de anuncios (que puede ser virtual) que permita facilitar información sindical a los trabajadores.
- Será responsable del tratamiento de datos en el tablón de anuncios (…), aquél órgano u organización que decida sobre su uso y finalidad y sitúe materialmente la información en él.
- Debe considerarse el espacio físico o virtual concreto en el que se situará el tablón con la finalidad de que la información personal sólo resulte visible a los usuarios legitimados para consultarla.
- Es fundamental que los tablones sindicales online se sitúen en las intranet de la organización, nunca en Internet.
- Debe tenerse muy en cuenta el principio de calidad desde el punto de vista de la proporcionalidad de los tratamientos y su finalidad.
- Es recomendable considerar la posibilidad de que los tablones impidan el acceso a la información por terceros no autorizados.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Dudas del profesional:

¿Cuándo debo informar a los representantes de los trabajadores?

- En principio el deber de información del art. 5 LOPD tiene como destinatario al afectado o interesado.
- No obstante, en aquellos tratamientos que repercuten sobre el conjunto de los trabajadores resulta muy recomendable informar con carácter previo a la representación de éstos ya que facilita el conocimiento y la comprensión general de los mismos.

  - Ej. Esta necesidad se manifiesta de modo particular en el caso del desarrollo de controles empresariales, como la videovigilancia, los controles sobre la navegación en internet, o el uso de controles biométricos para registrar la entrada, salida o presencia en el puesto.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Normativa aplicable:

- **Ley Orgánica 15/199** de Protección de Datos de Carácter Personal.
- **Real Decreto 1720/2007** que aprueba el Reglamento de Desarrollo de la LOPD 15/99.
- **Ley Orgánica 11/1985,** de Libertad Sindical
- **Ley 2/1991,** sobre derecho de información de los representantes de los trabajadores en materia de contratación
- **Ley 7/2007,** del Estatuto Básico del Empleado Público.
- **Ley 9/1987,** de Órganos de Representación, Determinación de las Condiciones de Trabajo y Participación del Personal al Servicio de las Administraciones Públicas.
- **Ley 30/1984** de Medidas para la Reforma de la Función Pública
- **Ley 8/1980** sobre el Estatuto de los Trabajadores

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Casos similares:

El presente caso, dada la especificidad del mismo, sólo da cobertura a las cesiones de datos destinadas a representantes de los trabajadores en calidad de miembros de organizaciones sindicales, a saber:

- Sección Sindical
- Delegados de Personal
- Junta de Personal

No obstante, los principios fundamentales en los que se funda, consentimiento y disociación de datos, ya han sido tratados en anteriores casos prácticos de esta presentación.

CASO PRÁCTICO 12: Cesión de datos a la Sección Sindical

Resumen:

Conceptos que hay que tener muy claros:

- Sólo los representantes de los trabajadores (Delegados de personal o Junta de Personal) pueden ser destinatarios de una cesión de DCP vinculada a organizaciones sindicales.
- El cumplimiento de las funciones de los representantes de los trabajadores puede llevarse a cabo con datos disociados.
- Para datos no disociados es preciso solicitar el consentimiento al trabajador.
- El correo electrónico y el tablón de anuncios son medios válidos para realizar comunicaciones a los trabajadores con las debidas medidas de seguridad.
- En aquellos tratamientos que repercuten sobre el conjunto de los trabajadores resulta muy recomendable informar con carácter previo a la representación de éstos.

CASO PI
dical

Caso re

PROTECCIÓN DE DATOS

1/11

leydeproteccióndedatos.com

00466/2008

[redacted]?

[redacted]

la Agencia
Españo
FEDER
por D. H
JADORES -
presentada

Conflicto entre los derechos fundamentales a la protección de datos y la libertad sindical

Sentencia de la

Abr
11

La Audiencia Na
lución de la Age
sancionaba con
datos personale
consentimiento.

La Audiencia Na
derecho a la pro
sindicato para di
sarios para el en
sindical y limitac

recaudac

c. Jorge Juan

de 2008

na reso-
que se
ublicado
a sin su

sobre el
ción del
te nece-
ctividad

a y Ocio.

de cada

agpd.es

AEPD sanciona a CC.OO. con 6.000 € por filtrar 20.000 ficheros

La Agencia Española de Protección de Datos (AEPD) ha sancionado al sindicato CC.OO. con 6.000 € porque uno de sus trabajadores filtró, accidentalmente, 20.000 ficheros con datos personales a través del eMule.

Se trata de la **primera vez** que la AEPD sanciona a una entidad por la difusión en Internet de datos personales filtrados a través de un software de intercambio de archivos como el eMule, que permite el acceso al contenido de los ordenadores de otros usuarios.

La AEPD decidió instruir el expediente por no haber sido cuidadosos con los datos y por no tener medidas de protección, pero ya ellos en esos dos años habían hecho una campaña de formación e información masiva a todos sus trabajadores que hizo que la Agencia reconsiderara su decisión inicial de sancionarles por una falta grave (de 60.000 a 600.000 €). Aunque la consideración de la falta es grave, la sanción, es la aplicable a una leve (6.000 €), que no recurrirán.

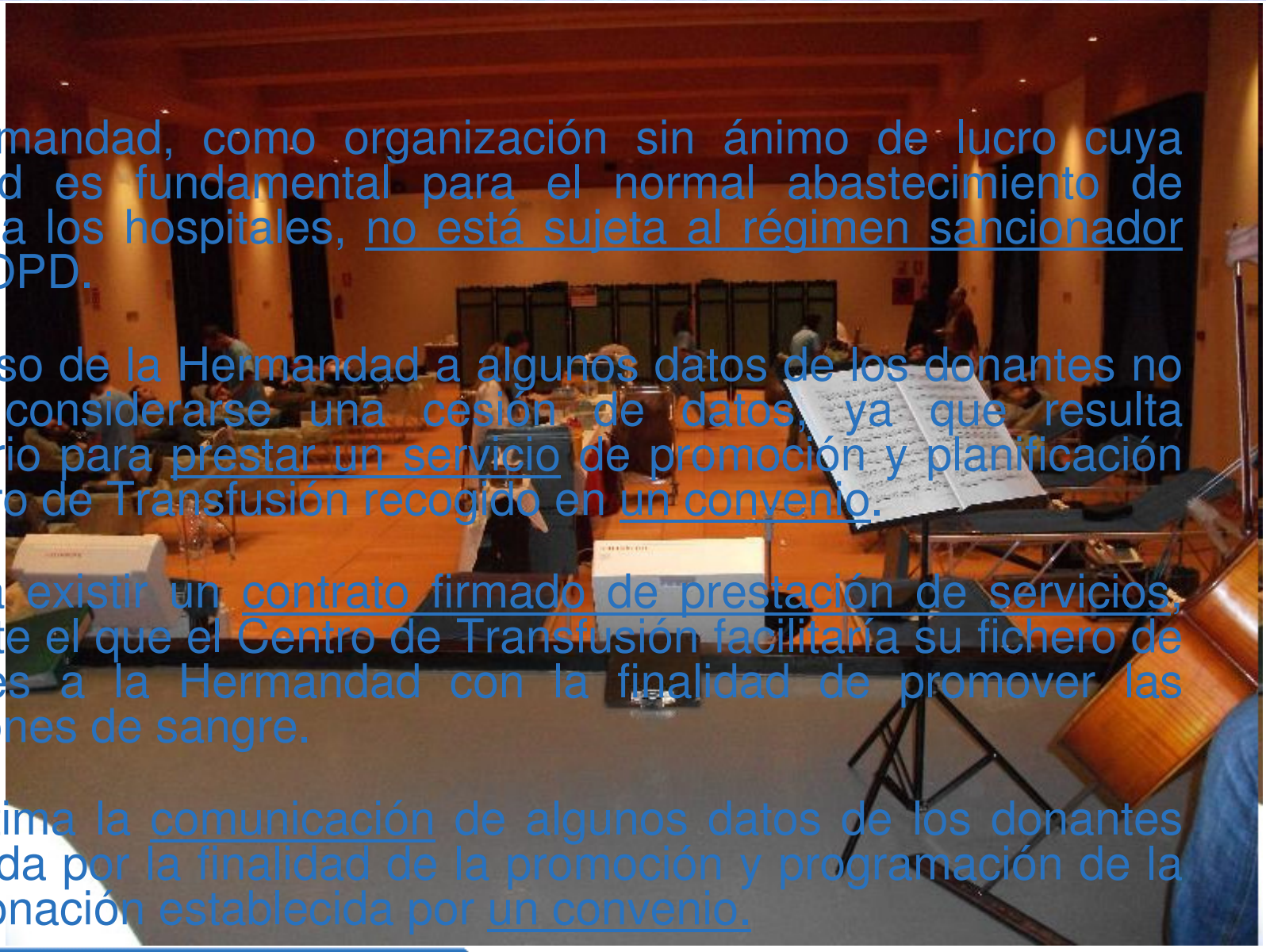
CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Un donante de sangre, que estima que solo el Centro de Transfusión Sanguínea debería disponer

de sus datos relativos a las donaciones, recibe un escrito remitido por la Hermandad de Donantes, solicitando nuevas donaciones y en el que se le informa que sus datos se los ha facilitado el Centro de Transfusión Sanguínea.

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Opciones:



a) La Hermandad, como organización sin ánimo de lucro cuya actividad es fundamental para el normal abastecimiento de sangre a los hospitales, no está sujeta al régimen sancionador de la LOPD.

b) El acceso de la Hermandad a algunos datos de los donantes no puede considerarse una cesión de datos, ya que resulta necesario para prestar un servicio de promoción y planificación al Centro de Transfusión recogido en un convenio.

c) Debería existir un contrato firmado de prestación de servicios, mediante el que el Centro de Transfusión facilitaría su fichero de donantes a la Hermandad con la finalidad de promover las donaciones de sangre.

d) Es legítima la comunicación de algunos datos de los donantes justificada por la finalidad de la promoción y programación de la hemodonación establecida por un convenio.

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Dudas del profesional:

¿Qué cesiones de datos de donantes pueden dirigirse a las Hermandades de Donantes de Sangre que colaboran en la provincia?

- Ninguna, salvo que se cuente con el consentimiento de los donantes titulares de los datos objeto de la comunicación.
- Necesidad de disponer de algún medio de prueba válido en Derecho, donde conste el consentimiento prestado por el afectado.

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Dudas del profesional:

¿Una Hermandad puede llevar a cabo promociones de la donación accediendo al fichero de donantes del CRTS?

- Sólo si se ha formalizado un contrato de prestación de servicios entre esta y el Centro de Transfusión donde la primera asume el papel de Encargado del Tratamiento.
- El acceso a los datos debe limitarse exclusivamente a los necesarios para llevar a cabo las funciones de promoción y planificación.

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Dudas del profesional:

¿Cuál es la infracción cometida por el Centro de Transfusión Sanguínea y la Hermandad de Donantes?

- Artículo 44.4. Son infracciones muy graves:

b) Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 (salud) y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Dudas del profesional:

¿El CRTS puede recopilar datos de los donantes en nombre de la Hermandad?

- Ello colocaría al CRTS como Encargado del Tratamiento de la Hermandad.

¿La Hermandad puede recopilar datos de los donantes?

- El donante puede comunicar sus datos personales a la Hermandad mediante los formularios o fichas que ésta disponga al efecto, y en las que se comunique la finalidad de dichos datos.

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Dudas del profesional:

¿En que situaciones el CRTS debe informar al donante en los términos del artículo 5.1 de la LOPD?

ANEXO I

PARTE A

Información mínima que se habrá de proporcionar a los posibles donantes de sangre o componentes sanguíneos

(…)

3. Información sobre la protección de datos personales. No se revelará sin la correspondiente autorización el nombre del donante, los datos concernientes a su salud ni el resultado de los análisis efectuados.

(…)

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Dudas del profesional:

¿Cómo deben tratarse los ficheros de convocatorias de los donantes?

- Los ficheros de convocatoria de los donantes estarán protegidos para preservar su integridad conforme a lo establecido en la LOPD.
- Dichos ficheros serán accesibles sólo a las personas autorizadas, y utilizados exclusivamente para los fines autorizados por el donante.
- Las tareas que se realicen externamente se definirán por escrito en un contrato específico.

(RD 1343/2007, artículo 5.2)

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Dudas del profesional:

¿Qué garantías tienen los titulares de los datos inscritos en el sistema de registro de donantes?

- Se garantizará a los donantes de sangre la confidencialidad exigida en la LOPD respecto de:
  - toda la información relacionada con su salud,
  - de los resultados de los análisis de sus donaciones,
  - así como de la trazabilidad futura de su donación.

- Dicha información sólo será facilitada al personal autorizado.

(RD 1088/2005, artículo 5.1)

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Dudas del profesional:

¿Qué debo tener en cuenta para manejar los datos del sistema de registro de donantes?

- Los datos de carácter personal del sistema de registro tendrán carácter confidencial.
- Estarán a disposición de los interesados y, en su caso, de la autoridad judicial.
- Su utilización se limitará a fines asistenciales o en interés de la salud pública.
- Quienes usen los datos están obligados a respetar la intimidad y la vida privada.

(RD 1088/2005, artículo 5.4)

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Normativa aplicable:

- **Real Decreto 1088/2005**, de 16 de septiembre, por el que se establecen los requisitos técnicos y condiciones mínimas de la hemodonación y de los centros y servicios de transfusión.
- **Real Decreto 1343/2007**, de 11 de octubre, por el que se establecen normas y especificaciones relativas al sistema de calidad de los centros y servicios de transfusión.
- **Ley Orgánica 15/99** de Protección de Datos de Carácter Personal.
- **RD 1720/2007** de 21 Diciembre.

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Resumen:

Conceptos que hay que tener muy claros:

- Informar en la recogida de datos
- Pedir el consentimiento para las cesiones previstas
- Formalizar los acuerdos de prestación de servicios contemplando la figura del Encargado del Tratamiento.
- Aplicar las medidas de seguridad de nivel alto
- Permitir el ejercicio de los derechos ARCO

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Casos similares:

El presente caso, dada la especificidad del mismo, sólo da cobertura a las cesiones de datos destinadas a Asociaciones Hermandades de Donantes de Sangre en calidad de asociaciones de carácter altruista destinadas al fomento de la donación de sangre.

El caso expuesto habla específicamente de los **CRTS** como posibles cedentes de datos pero en general es aplicable a cualquier **Banco de Sangre**.

CASO PRÁCTICO 13: Cesión de datos a Hermandad Donantes

Caso Real:

Memoria de la AEPD del 2002

Resolución respecto de una denuncia de un donante formulada en 2001

La Resolución del procedimiento declaró que el tratamiento de datos del denunciante realizado por la Hermandad de Donantes y la cesión de los mismos por parte del Banco de Sangre quedaban al margen de los supuestos permitidos en los artículos 6, 7 y 11 de la LOPD, resolviendo el Director imponer al Banco de Sangre una multa de 60.101,21 euros por una infracción del artículo 11.1 de la citada norma, tipificada como muy grave, e imponer a la Hermandad de Donantes de Sangre una multa de 60.101,21 por una infracción del artículo 7.3 de la misma, tipificada como muy grave en el artículo 44.4.c) de dicha norma.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

El asistente social de un Centro de salud solicita acceder a la Historia Clínica de un paciente.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Opciones:

a) Es razonable y está justificado el acceso a la Historia Clínica completa del paciente debido a la variabilidad y complejidad de los casos.

b) Debe otorgarse acceso a aquella información que pueda ser adecuada, pertinente y no excesiva, según la finalidad que persigue la asistencia social a los enfermos por los trabajadores sociales integrados en los equipos de atención primaria.

c) Sería recomendable que el parte de interconsulta incluyera un texto informativo conforme a lo establecido en el artículo 5 de la LOPD y se aprovechara para que quedara constancia del consentimiento del enfermo.

d) Las funciones propias de los trabajadores sociales dentro de la prestación socio-sanitaria legitiman a estos para acceder a aquellos datos de los pacientes a los que deben atender necesarios para la actuación social.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Cuál es el desarrollo y alcance de la Historia Social?

- La historia social es un buen ejemplo de tratamiento de datos de carácter personal, aunque no ha sido objeto de desarrollo legal, a diferencia de la historia clínica, que sí lo ha sido a través de 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, y diferentes Leyes autonómicas.

- La historia social es un instrumento documental en el que se registran exhaustivamente los datos personales, familiares, sanitarios, de vivienda, económicos, laborales, educativos y cualesquiera otros significativos de la situación sociofamiliar de un usuario, la demanda, el diagnóstico y subsiguiente intervención y la evolución de tal situación.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Se ha publicado y notificado el Fichero específico que da cobertura a la Historia Social?

- No.
- Atendiendo a la naturaleza de los datos que contienen las historias sociales, que se corresponden con los definidos en la LOPD como especialmente protegidos, deberán adoptarse las medidas correspondientes al mayor nivel de seguridad exigible cuando se proceda al tratamiento de dichos datos personales.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Podrían registrarse los datos referentes a la situación personal y social del paciente en la Historia Clínica?

- En aquellos centros en los que, además de la asistencia social, se dé también asistencia sanitaria, se tendrá especial cuidado en diferenciar y separar el archivo y custodia de los datos que componen la Historia Social de aquellos que tienen un fin específicamente asistencial sanitario y que se integrarán en la historia clínica del usuario.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Qué datos de salud podría tener La Historia Social?

- La historia social, siempre que se cuente con el consentimiento expreso del usuario o de su representante legal, podrá recoger aquellos datos de salud que reflejen situaciones de incapacidad o minusvalía, física o psíquica, reconocida legalmente o de hecho, o cualquier otro dato de salud que pueda afectar y repercutir en la situación personal y social del usuario o beneficiario de la prestación social.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Quién puede acceder a la Historia Social?

- A la Historia Social de un usuario podrán acceder aquellos profesionales sociales que participen en su proceso asistencial y siempre que el acceso sea necesario para el ejercicio de sus funciones.

- Los profesionales que prestan la asistencia social al interesado tienen acceso a la historia social completa de éste, como instrumento fundamental para su adecuada asistencia.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿El paciente puede acceder a los datos obrantes en el fichero?

- Derechos de acceso, rectificación, cancelación y oposición.
- Procedimiento de tutela de derechos ante la AEPD.
- Sí, además debe realizarse sin ningún coste para el usuario.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Los profesionales sanitarios pueden acceder a la Historia Social de un paciente?

- Sólo podrán acceder a aquellos datos de circunstancias sociales del paciente que tengan una relación directa con el posible diagnóstico o tratamiento de la salud del interesado, cuando esos datos resultan necesarios para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o la gestión de servicios sanitarios.

- Código Deontológico de la Profesión de Diplomado en Trabajo Social. Artículo 36:

  "El diplomado en trabajo social/asistente social debe guardar secreto de todo lo que los usuarios/clientes le transmitan y confíen, así como de lo que conozca en su ejercicio profesional. Tanto la recogida como la comunicación de datos debe ser restringida a las necesidades de la intervención profesional."

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Debe atenderse la solicitud de datos de un usuario/paciente realizada por los Servicios Sociales Municipales? [Regla general - 1/2]

- Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

- Ley habilitante: 6/1995 de Garantía de los Derechos de la Infancia y la Adolescencia.
  - Art. 52.1.b: competencia para poder solicitar informes de cuantas personas u organismos puedan facilitar datos relevantes para el conocimiento y la valoración de la situación socio familiar del menor.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Debe atenderse la solicitud de datos de un usuario/paciente realizada por los Servicios Sociales Municipales? [Menores - 2/2]

- **Ley 1/98 de los derechos y la atención al menor (Andalucía), artículo 10.6:**

  Los titulares de los servicios de salud y el personal sanitario de los mismos están especialmente obligados a poner en conocimiento de los organismos competentes de la Administración de la Junta de Andalucía en materia de protección de menores, de la Autoridad Judicial y del Ministerio Fiscal aquellos hechos que puedan suponer la existencia de situaciones de desprotección o situaciones de riesgo para los menores, así como a colaborar con los mismos para evitar y resolver tales situaciones en interés del menor.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿Se puede acceder a los datos de menores para un trabajo de investigación?

- Regla general, consentimiento o disociación.
- Aplicar los criterios del caso práctico 3 "publicación de un estudio epidemiológico".

¿Es obligatorio ceder datos de usuarios a la Policía?

- Sí, pero la petición debe ser motivada ajustándose al principio de calidad de datos.
- Aplicar los criterios del caso práctico 11 "solicitud de datos por la policía judicial".

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Dudas del profesional:

¿El Asistente Social del Ayuntamiento puede compartir datos de un usuario con profesionales sanitarios en una Comisión de Seguimiento de Casos?

- Código Deontológico. Artículo 40:

  No se vulnera el secreto profesional en los siguientes supuestos:

  b) En la relación y colaboración del diplomado en trabajo social/asistente social con otros profesionales de distinto ámbito técnico o de otras disciplinas, siempre que dicha colaboración se produzca en el marco de la intervención profesional.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Normativa aplicable:

- **Ley Orgánica 15/99** de Protección de Datos de Carácter Personal.
- **RD 1720/2007** de 21 Diciembre.
- **Recomendación 1/2005**, de 5 de agosto, de la Agencia de Protección de Datos de la Comunidad de Madrid.
- **Código Deontológico** de la Profesión de Diplomado en Trabajo Social
- **Circular 1/87 de la Consejería de Salud**, que regula las funciones de los Trabajadores Sociales en el ámbito de la Atención Primaria de Salud .
- Normativa Servicios Sociales

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Resumen:

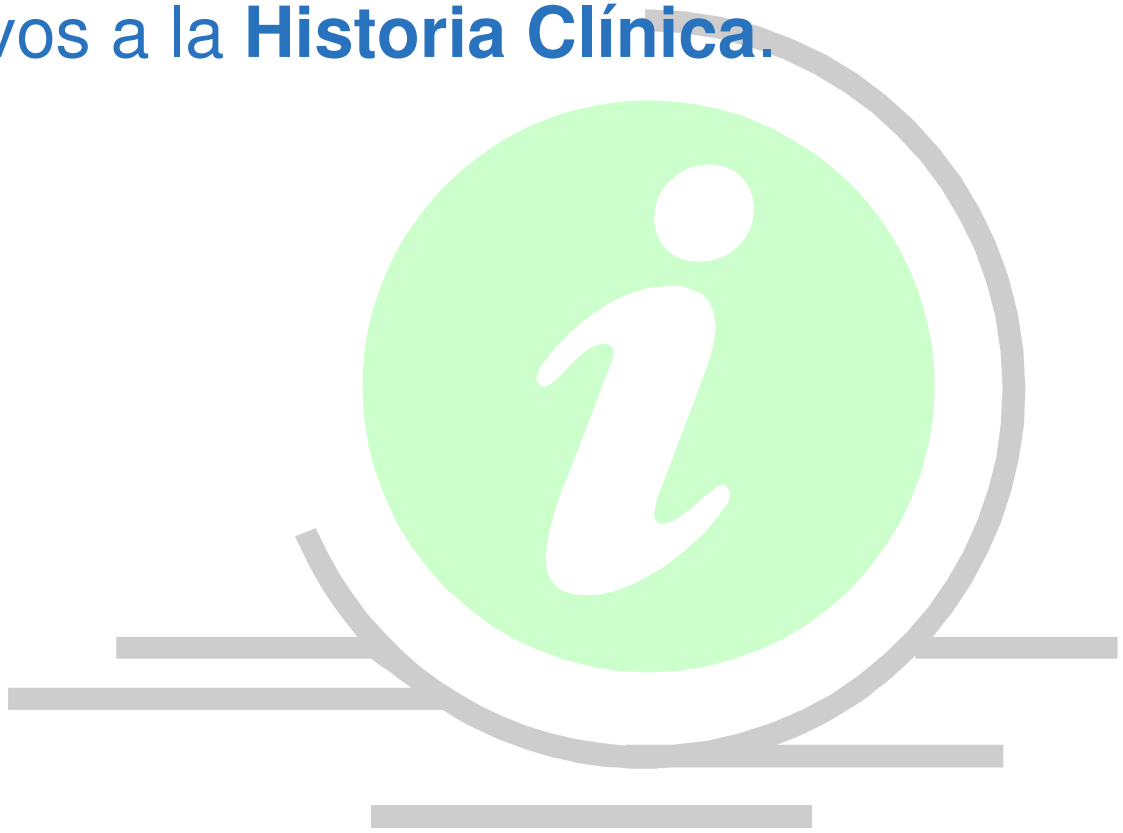
Conceptos que hay que tener muy claros:

- El acceso del trabajador social a la Hª Clínica y del personal sanitario a la Hª Social debe ser proporcional.
- Deben aplicarse a la Hª Social los "mismos" criterios de protección de datos que a la Hª Clínica (archivo, conservación, custodia, acceso, ejercicio de derechos,…)
- Debe diferenciarse la Hª Social de la Hª Clínica.
- "Posibilidad" de cesiones de datos a los Servicios Sociales
- Los usos de la Hª Social con fines de investigación, docencia o similar, deberán hacerse con datos disociados.

CASO PRÁCTICO 14: La Hª Social en las Instituciones Sanitarias

Casos similares:

El tratamiento de datos de carácter personal relativos a la **Historia Social** es similar al tratamiento de datos de carácter personal relativos a la **Historia Clínica**.



CASO P... ...itarias

Caso I...

Blog Cart@ de Protección de Datos

Todas las novedades sobre la protección de datos personales: actualidad, buenas prácticas, consejos...

Inicio | PractiLetter PROTECCION de DATOS

La Agencia madrileña propone que los datos de los servicios sociales estén "especialmente protegidos"

Publicado 17 de Junio de 2011 Sin comentarios

La Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) quiere que el marco normativo considere como "**especialmente protegidos**" los datos que gestionan los servicios sociales, al igual que ocurre con los datos que maneja el sector sanitario. El director de la Agencia, Santiago Abascal, pidió durante la sexta edición de las jornadas de protección de datos en los servicios sociales que se apruebe una ley que regule la historia social, a imagen y semejanza de la regulación actual de la historia clínica.

El acto, en el que se ha contado con cerca de 200 asistentes, ha tenido como principal objetivo identificar las dificultades más habituales que se presentan en los centros de servicios sociales y plantear soluciones a los problemas del trabajo diario, poniendo de manifiesto la posibilidad de conciliar una gestión eficaz con un escrupuloso respeto a los derechos de los ciudadanos.

CONCLUSIONES/DECÁLOGO

1	RECUERDA QUE LOS DATOS SON DE LAS PERSONAS
2	PARA EMPEZAR, COMPRUEBA QUE EL FICHERO ESTÁ CREADO
3	INFORMA Y PIDE EL CONSENTIMIENTO
4	SOLICITA Y TRATA SÓLO DATOS ADECUADOS, PERTINENTES Y NO EXCESIVOS
5	CUMPLE LAS MEDIDAS DE SEGURIDAD
6	FACILITA EL EJERCICIO DE DERECHOS “ARCO” A LAS PERSONAS A LAS QUE SE REFIEREN LOS DATOS
7	CUMPLE CON TU DEBER DE SECRETO
8	NO CEDAS DATOS SIN AUTORIZACIÓN
9	COMPRUEBA QUE EXISTE UN CONTRATO CON EMPRESAS QUE TRABAJAN PARA TU ADMINISTRACIÓN
10	CUANDO NO SEAN NECESARIOS CANCELA LOS DATOS DE FORMA ADECUADA

CONSECUENCIAS

La adecuación de los centros a la Ley Orgánica de Protección de Datos, además de ser una obligación legal, permite:

- **Cumplimiento del Contrato Programa 2005-2008**
- **Acreditación de Servicios (ACSA)**
- **Acreditación de Centros (ACSA)**

Hemos de considerar las denuncias e inspecciones de las que fuimos objeto:

- **Agencia Española de Protección de Datos:**

AÑO	CENTRO	AÑO	CENTRO
2010	Solicitud de informe on-line a los hospitales	2006	Denuncia A.G.S. Campo de Gibraltar
2008	Denuncia Hospital Reina Sofía	2006	Denuncia D.S.A.P. Málaga
2007	Denuncia Hospital Virgen del Rocío	2005	Denuncia Hospital Carlos Haya

- **Consejería de Hacienda y Administración Pública**
  - 2008 Inspección en Servicios Centrales del SAS
  - 2007 Inspección en Distrito Sanitario Almería...

FUENTES DE INFORMACIÓN ADICIONALES

- Agencia Española de Protección de Datos
- Agencia Madrileña de Protección de Datos. Consultas Servicios Sanitarios
- Unidad de Gestión de Riesgos Digitales
- Instituto Nacional de Tecnologías de la Comunicación
- Curso LOPD on-line. Consjería de empleo
- BOE / BOJA