

**ASUNTO: RESUMEN de la Instrucción 6/2003 del Director General de Okakidetza sobre funciones y obligaciones del personal de Osakidetza/Servicio vasco de salud, con relación a la protección de datos de carácter personal. Procedimientos de actuación.**

## **INTRODUCCIÓN.**

El personal que trabaja en las Organizaciones de Servicios de Osakidetza/Servicio Vasco de Salud, como fruto de sus relaciones laborales, tiene acceso de forma total o parcial a diferentes tipos de datos: datos identificativos, datos profesionales y datos clínicos.

El contenido de esta Instrucción está dirigido a todo el personal que desarrolla su trabajo en cualquiera de las organizaciones de servicios de Osakidetza/Servicio vasco de salud, y que en el ejercicio de sus funciones, maneja sistemas de información de cualquier índole con datos de carácter personal, como: 3S-Osabide, e-Osabide, Aldabide, Gizabide, o cualquier otra aplicación informática o base de datos. La finalidad es instar a todo el personal a conocer la normativa actual en materia de protección de los datos de carácter personal disponibles en Osakidetza/Servicio Vasco de Salud, y a manejar éstos de forma confidencial y adecuada, garantizando el ejercicio de los derechos del ciudadano en esta materia.

La Ley Orgánica 15/1999, de 13 de diciembre, relativa a la Protección de Datos de Carácter Personal, define los **“datos de carácter personal”** como cualquier información concerniente a personas físicas identificadas o identificables y el **“tratamiento de datos”** como las 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.

Con el fin de hacer efectivos los derechos del ciudadano, en cuanto a protección de datos y confidencialidad de la información, establecidos en la normativa actual, se dictan las siguientes

## INSTRUCCIONES

### 1ª DEBERES Y OBLIGACIONES

#### 1.1- DEBER DE CONFIDENCIALIDAD

Todo el personal de Osakidetza, que de manera directa o indirecta tenga acceso a datos de carácter personal y/o a datos relativos a la salud, tiene el deber de preservar la confidencialidad de los mismos.

#### 1.2- DEBER DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Los interesados a los que se les soliciten datos personales deberán ser previamente informados de modo expreso:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

#### 1.3- OBLIGACIÓN DE RECABAR EL CONSENTIMIENTO DEL AFECTADO PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Los datos personales relativos a la salud están especialmente protegidos y cuentan con un régimen específico para su tratamiento, en atención a su destino. Así, conforme al apartado 6 del art. 7 de la LOPD, y por lo que aquí interesa, los datos de carácter personal relativos a la salud podrán ser objeto de tratamiento sin consentimiento del afectado *“cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto”*. También *“para salvaguardar el interés vital del afectado o de otra persona”*, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Para el tratamiento de datos de carácter personal que no estén especialmente protegidos, se exige el consentimiento inequívoco del afectado, salvo las excepciones dispuestas en la legislación.

#### **1.4- DEBER DE ADOPTAR MEDIDAS DE SEGURIDAD**

El **responsable del fichero** deberá adoptar las medidas de índole técnica y organizativa que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Para los **ficheros de carácter no corporativos** existentes en cada organización de servicios, deberá de ser el director gerente, por medio de él o los responsables de seguridad y de autorizaciones de accesos, el encargado de articular dichas medidas

#### **1.5- DEBER DE SECRETO**

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, están obligados al secreto profesional.

#### **1.6- OBLIGACIÓN DE RECABAR EL CONSENTIMIENTO DEL INTERESADO PARA LA CESIÓN DE DATOS DE CARÁCTER PERSONAL**

La comunicación de datos de carácter personal a terceros sólo podrá realizarse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, y con el previo consentimiento del interesado.

#### **2º.- DERECHOS Y GARANTÍAS DE LOS AFECTADOS**

**La solicitud de acceso, rectificación, oposición y cancelación de datos de carácter personal** son derechos del ciudadano recogidos en la ley 15/1999, de protección de datos de carácter personal.

Las solicitudes podrán tramitarse a través de los Servicios de Atención al Paciente y Usuario o de las Áreas de Atención al Cliente de los centros.

#### **2.1- DERECHO DE ACCESO**

El interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento.

## 2.2- **DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN**

Si los datos de carácter personal del afectado son inexactos, incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, la cancelación de los mismos.

## 3º.- **MEDIDAS DE SEGURIDAD EN LAS ORGANIZACIONES DE SERVICIOS**

En cada Organización de Servicios, el director gerente nombrará un **Responsable de Seguridad** de cuantos Sistemas de Información estén ubicados o se generen en su ámbito de actuación.

Cada sistema de información tendrá un **Responsable de Autorización de Accesos**, nombrado por el Director Gerente de la organización de servicios, que será el encargado de diseñar el sistema de accesos y tener actualizado el listado de usuarios.

## 4º.- **MEDIDAS DE SEGURIDAD DE LOS ORDENADORES**

- Cada usuario con acceso a sistemas de Información tendrá asignado de forma personal, confidencial e intransferible, un *código de acceso* y una *contraseña*, de cuyo uso se responsabilizará personalmente.
- Las contraseñas se renovarán periódicamente y el archivo/soporte donde se almacenen estará protegido.

## 5º.- **NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS**

**Incidencia** es todo suceso que pueda provocar vulneración de la confidencialidad.

Las incidencias que puedan acontecer durante la explotación de los sistemas de información de Osakidetza/Servicio vasco de salud, y que traten datos de carácter personal, deberán quedar registrados en un **libro de incidencias** por medio del llamado **informe de incidencias**, comunicándose al Responsable de Seguridad de la organización de servicios.