

INSTRUCCIÓN 6 / 2003

DE: DIRECTOR GENERAL DE OSAKIDETZA/SERVICIO VASCO DE SALUD

A: DIRECTORES/AS GERENTES/AS ORGANIZACIONES DE SERVICIOS

ASUNTO: **Funciones y obligaciones del personal de Osakidetza/Servicio vasco de salud, con relación a la protección de datos de carácter personal. Procedimientos de actuación.**

Osakidetza/Servicio vasco de salud como parte fundamental del Sistema Sanitario de Euskadi, tiene como misión *"proveer los servicios sanitarios públicos de calidad a los ciudadanos de la Comunidad Autónoma, para satisfacer las necesidades de salud de la población, bajo los principios de equidad, eficiencia y calidad, mediante el desarrollo de actividades de promoción, prevención, cuidado y mejora de la salud"*. 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, es de aplicación a los datos de carácter personal registrados en cualquier soporte físico (papel, magnético o telemático) que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de los mismos. 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.

Los **"datos personales relativos a la salud"** están especialmente protegidos, y respecto a ellos, la Ley orgánica 15/1999, en su artículo 8, dice *"las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal y autonómica sobre Sanidad"*.

Dada la importancia de la definición adecuada de los términos relacionados con esta normativa, se utilizara la siguiente:

- **Contraseña**, información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
- **Documentación clínica**, soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial.
- **Fichero**, todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Incidencia**, todo suceso que pueda provocar vulneración de la confidencialidad, privacidad o seguridad de los datos de carácter personal, con independencia de cual sea su soporte de registro.
- **Información clínica**, todo dato cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla.
- **Responsable de autorización de accesos**, persona o personas responsables de establecer los mecanismos que permiten acceder a datos o recursos.
- **Responsable de fichero**, persona física o jurídica que decide sobre la finalidad, contenido y uso de los datos de carácter personal de un fichero.
- **Responsable de seguridad**, persona o personas a las que el responsable de ficheros ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
- **Sistema de información**, conjunto de ficheros automatizados, programas soportes y equipos empleados para el almacenamiento y tratamiento de carácter personal.
- **Soporte**, objeto físico susceptible de ser tratado en un sistema de información y sobre el que se pueden grabar o recuperar datos.
- **Usuario**, sujeto o proceso autorizado para acceder a datos o recursos.

Así, 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, tal como la Ley 15/1999 de protección de datos de carácter personal, el Real Decreto 994/1999 sobre medidas de seguridad de ficheros automatizados, la Ley 41/2002 básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, la Ley 8/1997 de Ordenación Sanitaria de Euskadi, la Ley 6/1989 de Función Pública Vasca, el Decreto 272/1986 que

regula el uso de la historia clínica en la Comunidad Autónoma del País Vasco (artículos 7 a 10), el Decreto 45/1998 sobre la Valoración, Conservación y Expurgo de la

Documentación del Registro de Actividades Clínicas y el Decreto 175/1989 por el que se aprueba la carta de derechos y obligaciones de los pacientes y usuarios de Osakidetza/ Servicio vasco de salud, se dictan las siguientes

I N S T R U C C I O N E S

1º.- DEBERES Y OBLIGACIONES

1.1- DEBER DE CONFIDENCIALIDAD

Todo el personal de Osakidetza/ Servicio vasco de salud que ejerce su labor en cualquiera de sus organizaciones de servicios, y que de manera directa o indirecta tenga acceso a datos de carácter personal, y/o a datos relativos a la salud (información clínica) tiene el deber de preservar la confidencialidad de los mismos, utilizarlos de forma adecuada, adoptar las medidas pertinentes para salvaguardar su confidencialidad y evitar su acceso a personal no autorizado.

El deber de secreto es independiente del tipo documental en que este recogida la información (soporte papel, magnético o telemático) y subsiste por tiempo indefinido, aún después de la finalización del contrato laboral.

Cuando por procesos de expurgo de archivo y documentación un soporte vaya a ser desechado o reutilizado, se aplicarán medidas adecuadas para salvaguardar la confidencialidad de los datos contenidos.

En el caso de empresas subcontratadas por Osakidetza/ Servicio vasco de salud y cuyo personal en el ejercicio de sus funciones, tenga acceso a datos de carácter personal, el contrato deberá incluir una cláusula específica respecto "al deber de secreto y al uso o manejo de la información estableciendo las medidas de seguridad adecuadas". En el **anexo I** figura **modelo de "cláusula sobre el deber de secreto y la confidencialidad para contratos con terceros"**.

El incumplimiento de estas obligaciones, en materia de confidencialidad y salvaguarda de la privacidad de la información, por parte del personal de Osakidetza/ Servicio vasco de salud dará lugar a la sanción que corresponda en función de la gravedad del caso (intencionalidad, perturbación del servicio, reiteración, reincidencia...), pudiendo llegar a ser causa de inhabilitación.

Si fuere detectada una violación del deber de secreto respecto a datos de carácter personal, la Dirección Gerencia de la organización de servicios correspondiente procederá a su investigación y correspondiente sanción si hubiere lugar.

1.2- DEBER DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Los datos de carácter personal, incluidos los datos clínicos, sólo se podrán recoger y/o utilizar cuando sean legítimos, adecuados y pertinentes, en relación con el ámbito, finalidad y motivo para el que hayan sido obtenidos. No podrán utilizarse para finalidades incompatibles con aquellas para las que los datos fueron recogidos, o cuyo uso no está contemplado por la normativa vigente.

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

- 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.

En el **anexo II**, se adjunta nota informativa de la Dirección de Asistencia Sanitaria informando a los ciudadanos del tratamiento de datos de carácter personal con la finalidad de elaborar la historia clínica informatizada, que debe estar en un lugar bien visible en las áreas de atención al cliente de las organizaciones de servicios de Osakidetza/ Servicio vasco de salud, y puede servir de **modelo para la información relativa a otros ficheros**.

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

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.

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 podrá ser objeto de tratamiento los datos carácter personal relativos a la salud *“cuando el tratamiento sea necesario 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.

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.

En relación a los **ficheros de carácter corporativo** las medidas se adoptarán por su correspondiente responsable desde la Organización Central de Osakidetza/ Servicio vasco de salud, sin embargo 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, así como velar por el cumplimiento de las medidas de seguridad establecidas para cada tipo de fichero (corporativos y propios).

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 y al deber de guarda respecto de los mismos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero, en su caso con el responsable del mismo.

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.

Si los datos pertenecen a un **fichero de carácter no corporativo**, cuando el responsable del fichero tenga necesidad de comunicar los datos de carácter personal objeto de tratamiento a un tercero, remitirá, por un medio que deje constancia del envío y de la fecha de recepción, notificación al interesado exponiendo los siguientes extremos:

- Identificación del responsable del fichero cedente.
- Datos de carácter personal del interesado en poder del responsable del fichero cuya comunicación a un tercero se pretende autorizar.
- Circunstancias en que se obtuvieron los datos que se pretende comunicar.
- Finalidad a la que se destinarán los datos cuya comunicación se pretende autorizar.
- Sujeción del cesionario, a las disposiciones de la Ley Orgánica de Protección de Datos de Carácter Personal.
- Advertencia, gráficamente destacada, de que si no se manifiesta lo contrario en el término de 15 días naturales contados a partir del día siguiente al de la recepción de la notificación, se entenderá que

presta su consentimiento a la comunicación de los datos personales expuesta.

- Igualmente destacado, el carácter revocable del consentimiento prestado.

Si los datos pertenecen a un **fichero de carácter corporativo**, los responsables de dichos ficheros en la Organización Central de Osakidetza/ Servicio vasco de salud serán los competentes para decidir sobre la posible cesión.

No se requerirá el consentimiento del interesado cuando la comunicación tenga por objeto datos de carácter personal relativos a la salud y sea necesaria para solucionar una urgencia o para realizar estudios epidemiológicos en los términos establecidos en la legislación sanitaria estatal o autonómica, debiendo utilizarse para esta finalidad datos disociados.

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.

Los interesados podrán solicitar **información acerca de sus datos** y la **rectificación de los datos erróneos o innecesarios** para el fin por el que hubieren sido recogidos. Estos derechos serán ejercidos por el afectado frente al responsable del fichero, para lo que será necesario que el afectado acredite su identidad ante el responsable del fichero. Podrá no obstante actuar el representante legal del afectado, cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de sus derechos.

La solicitud se acompañará de:

- Documento que acredite la identidad del interesado, como DNI u otro documento legal. Si la solicitud es del tutor o representante legal, se acompañará también la documentación que acredite esta representación.
- Exposición del motivo de la petición solicitada.
- Domicilio a efectos de notificación.
- Fecha y firma del solicitante.

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, quienes informarán debidamente a los interesados de sus derechos al respecto.

Las solicitudes se recogerán, registrarán y enviarán de manera urgente al Responsable de Seguridad nombrado en cada organización de servicios, siguiendo los circuitos y procedimientos definidos, y darán lugar a una respuesta por parte del **Responsable del Fichero**, con la aprobación o denegación motivadas, enviándole al interesado una "*notificación de resolución*". En caso de tratarse de **ficheros de carácter corporativo** (Gizabide, Osabide, etc..), la solicitud se enviara a los Responsables de los ficheros en la Organización Central de Osakidetza/ Servicio vasco de salud. En cualquier caso, dada la brevedad de plazos para responder (10 días en algunos casos), será fundamental coordinar dichas acciones a fin de que los plazos se cumplan.

En el **anexo III** se adjuntan los "**Modelos de solicitudes de acceso, de rectificación y de cancelación de datos de carácter personal de los ficheros de Osakidetza/ Servicio vasco de salud**".

El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros. Si la solicitud no reúne los requisitos expuestos en el apartado anterior, el responsable del fichero deberá requerir la subsanación de los mismos. En cualquier caso, para la respuesta se emplearán medios que permitan acreditar el envío y la recepción de la respuesta.

El responsable del fichero cuidará que el personal autorizado para acceder a los datos personales conozca y pueda prestar información a los interesados sobre sus derechos de acceso, rectificación y cancelación.

2.1- DERECHO DE ACCESO

El interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dicho datos, así como las comunicaciones realizadas o que se prevén realizar de los mismos.

El responsable del fichero resolverá sobre la solicitud de acceso en el **plazo** máximo de un mes a contar desde la recepción de la solicitud. En el caso de que no disponga de datos personales de los afectados deberá igualmente comunicárselo en el mismo plazo. Si la resolución fuese estimatoria, el acceso se hará efectivo en el plazo de los 10 días siguientes a la notificación de aquélla.

El **ejercicio del derecho de acceso** ofrecido por el responsable del fichero podrá hacerse mediante el procedimiento que sea adecuado a la configuración e implantación material del mismo (visualización en pantalla, escrito, copia o fotocopia remitida por correo...).

El responsable del fichero podrá **denegar el acceso** a los datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite interés legítimo al efecto, así como cuando la solicitud sea formulada por persona distinta del afectado.

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.

Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero **dentro de los diez días siguientes al de la recepción de la solicitud**. Si los datos rectificadas o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

La **solicitud de rectificación** deberá indicar el dato que es erróneo y la corrección que debe realizarse, debiendo ir acompañada de la documentación justificativa de la rectificación solicitada.

La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado, de terceros o cuando existiese una obligación de conservación de los datos. En este sentido y con carácter general, no procederá la cancelación de datos de la Historia Clínica en virtud del deber de conservación de la misma establecido en la legislación sanitaria.

Respecto a la **solicitud de cancelación**, el interesado deberá indicar si revoca el consentimiento otorgado en los casos en que la revocación proceda, o si por el contrario se trata de un dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa. Si el responsable del fichero considera que no procede atender la solicitud del afectado, se lo comunicará motivadamente dentro del plazo de los diez días siguientes al de la recepción de la misma.

La cancelación dará lugar al bloqueo de los datos conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales. Cuando acabe el plazo de prescripción de las posibles responsabilidades nacidas del tratamiento, deberá procederse al borrado físico de los datos.

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. Dicho responsable de seguridad deberá garantizar la custodia eficaz de la información y documentación generada, tal como establece la

normativa vigente en cuanto a medidas de seguridad de los datos de carácter personal.

A su vez, el responsable de seguridad de cada Organización de Servicios, actuará en coordinación con el responsable de seguridad de la Organización Central y con la Comisión Central de Seguridad de Osakidetza/ Servicio vasco de salud, con el fin de establecer y adoptar las medidas de seguridad más adecuadas a cada centro.

Las medidas de seguridad se establecerán de forma específica para cada sistema de información aplicando el nivel de seguridad exigible según el tipo de datos de carácter personal a tratar.

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, siendo responsable también de poner medidas para evitar el acceso a personas no autorizadas.

Las Organizaciones de Servicios deberán adecuar y adaptar el Documento de Seguridad del Ente Público Osakidetza/ Servicio vasco de salud, que define las medidas de seguridad que afectan a los ficheros de carácter corporativo existentes en el conjunto del Ente Público. Los Directores Gerente de cada organización de servicios a través del Responsable de Seguridad correspondiente, elaborarán e implantarán la

normativa de seguridad a través de un **Documento de seguridad de cada Organización de Servicios**, que será producto de añadir al documento de seguridad corporativo la normativa de seguridad relativa a los ficheros propios. Para ello es necesario inventariar los ficheros no corporativos de cada organización de servicios, registrarlos en el Documento de Seguridad propio, y proceder a su declaración a la Agencia de Protección de Datos. Este Documento de Seguridad de la Organización de Servicios será de obligado cumplimiento para todo el personal que acceda a los sistemas de información.

Por lo que se refiere a los ficheros corporativos, la Comisión de Seguridad de la Organización Central revisará y actualizará de forma periódica el **documento de seguridad del Ente Público Osakidetza/ Servicio vasco de salud**, constando la fecha de revisión en el mismo.

Los Directores Gerente crearán en cada organización de servicios, una estructura de seguridad, que actuando en coordinación con la Comisión de Seguridad de la Organización Central, se encargue de:

- incorporar al Documento de Seguridad de la organización de servicios las actualizaciones que se efectúen en el Documento de Seguridad de seguridad del Ente Público Osakidetza/ Servicio vasco de salud.

- revisar periódicamente el Documento de Seguridad de la organización de servicios en lo concerniente a los ficheros propios.
- chequear las medidas establecidas para todo tipo de ficheros y de elaborar el "informe de auditoria interna" con el fin de identificar áreas de deficiencias y las medidas correctoras necesarias.

4º.- MEDIDAS DE SEGURIDAD DE LOS ORDENADORES

Para garantizar el uso adecuado de los sistemas informatizados se han de cumplir las siguientes medidas, en todos los ordenadores de las organizaciones de servicios:

- Cada usuario con acceso a sistemas de Información soportados en sistemas informatizados, tendrá asignado de forma personal, confidencial e intransferible, un *código de acceso y una contraseña*, de cuyo uso se responsabilizara personalmente.
- Cualquier sospecha de difusión o uso indebido de las contraseñas, será comunicado al Responsable de Seguridad de su organización de servicios, para su modificación, generándose la correspondiente incidencia al verse afectada la seguridad de los datos. Las contraseñas se renovararán periódicamente y el archivo/soporte donde se almacenen estará protegido.
- La protección y el uso de los *ordenadores personales, y portátiles* es responsabilidad de cada persona a la que se autoriza su uso. Si se introducen o manejan ficheros con datos de carácter personal deberán someterse a las mismas medidas de seguridad que el resto de ficheros de la organización de servicios.
- Al final de cada jornada laboral, se *apagarán los ordenadores*, y sólo se podrán mantener encendidos de forma prolongada, mediante la autorización del Responsable de Seguridad de la organización de servicios correspondiente.

5º.- NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS

Incidencia es todo suceso que pueda provocar vulneración de la confidencialidad, privacidad o seguridad de los datos de carácter personal, con independencia de cual sea su soporte de registro.

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, debiendo recoger:

- Descripción de la incidencia
- Fecha y hora en la que se produce
- Centro o dependencia donde se ha producido
- Nombre y apellidos de la persona que notifica

El **anexo IV**, contiene el modelo de "**Informe de notificación de incidencias**" que se utilizara en estos casos.

A efectos operativos y de inspección, se guardarán o mantendrá el registro de las incidencias acaecidas en los últimos 12 meses. Cuando el tipo de incidencia, de lugar a una "*recuperación de datos*", se describirá el procedimiento usado para la recuperación y grabación.

Los responsables de seguridad de cada organización de servicios, una vez detectada una incidencia y en función de la gravedad de la misma, la comunicaran al Director Gerente de la misma y al Responsable de Seguridad de la Organización Central, para depurar las posibles responsabilidades.

Las Direcciones Gerencia de las organizaciones de servicios, a través de las direcciones que de ellas dependen y de las jefaturas de unidades, servicios o áreas de atención al cliente implicados, establecerán los mecanismos necesarios para el cumplimiento de esta Instrucción y para su difusión al personal de Osakidetza/ Servicio vasco de salud implicado.

En Vitoria-Gasteiz, a 2 de septiembre de 2003

Josu I. Garay Ibáñez de Elejalde
Director General de Osakidetza/ Servicio vasco de salud

ANEXO I. CLAUSULA SOBRE EL DEBER DE SECRETO Y CONFIDENCIALIDAD PARA CONTRATOS CON TERCEROS

En consideración al tipo de información procesada en el desempeño de su labor, el personal del adjudicatario está obligado a mantener la más absoluta confidencialidad sobre todos aquellos datos y documentos a que tengan acceso con motivo de esta adjudicación. A ellos accederán, exclusivamente, las personas estrictamente imprescindibles para el desarrollo de las tareas inherentes a la misma. Todas ellas serán advertidas del carácter confidencial y reservado de la información a la que tendrán acceso.

Todos los ficheros que se pongan a disposición del adjudicatario para la ejecución del contrato son propiedad de **Osakidetza** y están registrados y sometidos a la salvaguarda que establece la legislación vigente, en especial la relativa a la protección de datos personales. Toda cesión a terceros será perseguida en los tribunales.

Los citados datos o ficheros no podrán ser empleados ni tratados por la empresa xxx para fin distinto al previsto en el contrato de xxxx, estando especialmente prohibida su cesión o comunicación a terceros. Una vez cumplida la prestación contractual principal, los datos de carácter personal deberán ser destruidos por la adjudicataria.

Osakidetza se reserva el derecho de establecer cualquier tipo de marcaje de los ficheros que se dejarán al adjudicatario, de manera que sus características puedan constituirse como prueba que posibilite localizar el origen y los responsables de las eventuales cesiones.

Bajo ningún caso ni circunstancia, el adjudicatario podrá suministrar a terceros, ni utilizar para sí ni para otros, datos facilitados por **Osakidetza**, para fines distintos a los contemplados en el objeto del presente contrato.

El adjudicatario estará obligado a poner en conocimiento de **Osakidetza**, inmediatamente después de ser detectada, cualquier sospecha de eventuales errores que se puedan producir en el sistema de seguridad de la información.

El adjudicatario faculta a **Osakidetza** para que, al terminar el proyecto, pueda responsabilizarlo y/o repercutirle los costes derivados de posibles reclamaciones ocasionadas por negligencia y/o falta de confidencialidad del mismo.

ANEXO II- MODELO DE INFORMACION AL USUARIO SOBRE RECOGIDA DE DATOS DE CARÁCTER PERSONAL PARA SU INCORPORACION A FICHERO INFORMATIZADO

Mediante la presente "Nota Informativa", la Dirección de Asistencia Sanitaria de Osakidetza-Servicio vasco de salud pone en conocimiento de los ciudadanos que los datos personales que se les soliciten, serán objeto de tratamiento e incorporados a los ficheros de datos de carácter personal que existen en Osakidetza-Servicio vasco de salud.

La recogida y tratamiento de los datos personales solicitados por los profesionales sanitarios y no sanitarios de Osakidetza-Servicio vasco de salud tiene como finalidad la elaboración de la historia clínica de los pacientes para el seguimiento de su estado de salud, la gestión adecuada de los servicios sanitarios, la investigación científica y la actividad docente.

El responsable del fichero de historia clínica es la Dirección de Asistencia Sanitaria (c/ Alava, 45 - 01006 Vitoria-Gasteiz), órgano al que Vds. deberán dirigirse para ejercer los derechos de acceso, rectificación y cancelación.

Los datos que como titular Vd. facilite únicamente serán cedidos a otros organismos del sistema sanitario y organismos oficiales de estadística. Cualquier cesión fuera de las previstas requerirá su expreso consentimiento, salvo que se trate de solucionar una urgencia o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal y autonómica.

Es todo cuanto se comunica en cumplimiento del deber de información que impone el artículo 5 de la Ley 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

Atentamente,

**DIRECTOR ASISTENCIA SANITARIA
OSAKIDETZA-SERVICIO VASCO DE SALUD**

ANEXO III. FORMULARIO DE SOLICITUD DE ACCESO A DATOS DE CARÁCTER PERSONAL DE FICHEROS DE OSAKIDETZA/SERVICIO VASCO DE SALUD.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:
Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/D^a, mayor de edad, con domicilio en la C/....., n^o....., Localidad....., Provincia.....,CP....., con DNI, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con los artículos 15 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 12 y 13 del Real Decreto 1332/94.

SOLICITA:

- 1.- Que se le facilite gratuitamente acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiéndose que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos, en virtud del artículo 18 de la Ley Orgánica y 17 del Real Decreto.
- 2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.
- 3.- Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En, a.....dede 200

ANEXO III. FORMULARIO DE SOLICITUD DE RECTIFICACION DE DATOS DE CARÁCTER PERSONAL DE FICHEROS DE OSAKIDETZA/SERVICIO VASCO DE SALUD.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:

Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/D^a, mayor de edad, con domicilio en la C/....., n^o....., Localidad....., Provincia.....,CP....., con DNI, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con los artículos 16 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA:

- 1.- Que se proceda gratuitamente a la efectiva corrección en el plazo de diez días desde la recepción de la solicitud, de los datos inexactos relativos a mi persona que se encuentran en sus ficheros.
- 2.- Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.
- 3.- Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.
- 4.- Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En, a.....dede 200

ANEXO III. FORMULARIO DE SOLICITUD DE CANCELACION DE DATOS DE CARÁCTER PERSONAL DE FICHEROS DE OSAKIDETZA/SERVICIO VASCO DE SALUD.

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre:

Dirección de la oficina de acceso:

DATOS DEL SOLICITANTE

D/D^a, mayor de edad, con domicilio en la C/....., n^o....., Localidad....., Provincia.....,CP....., con DNI, del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con los artículos 16 de la Ley Orgánica de Protección de Datos de Carácter Personal, LO 15/1999, y los artículos 15 y 16 del Real Decreto 1332/94.

SOLICITA:

- 1.- Que se proceda a la efectiva supresión en el plazo de diez días desde la recepción de esta solicitud, de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros al no existir vinculación o disposición legal que justifique su mantenimiento.
- 2.- Que me comuniquen de forma escrita a la dirección arriba indicada la cancelación de datos una vez realizada.
- 3.- Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado, a fin de poder interponer la reclamación prevista en el artículo 18 de la Ley.

En, a.....dede 200

ANEXO IV. INFORME DE NOTIFICACIÓN DE INCIDENCIAS

INCIDENCIA N° _____ **Fecha** _____ **notificación:** _____

Nombre y Apellidos de quien notifica: _____

Cargo o puesto: _____

Tipo de incidencia: _____

Descripción (detallada): _____

Fecha y hora en la que se produjo: _____

Efectos que puede producir: (en caso de no subsanación o incluso independiente de ello)

Recuperación de datos: SI NO No Procede

Procedimiento realizado: _____

Datos restaurados: _____

Datos grabados manualmente: _____

Persona que ejecutó el proceso: _____

- Nombre:
- Apellidos:
- D.N.I.
- Firma:

Firma de quien notifica