



Guía de adecuación a la Ley de Protección de Datos



Comisión de Ejercicio Profesional
Ilustre Colegio Oficial de
Odontólogos y Estomatólogos de la 1ª Región





Introducción: ¿Qué supone la Ley de Protección de Datos?

La Ley Orgánica 15/1999 de Protección de Datos de carácter personal (en adelante LPD) y su Reglamento (1720/2007) establecen una serie de obligaciones para aquellos que manejen datos personales, como es el caso de los odontólogos y estomatólogos. Los datos de salud tienen en la LPD, junto con los referidos a ideología o religión, el nivel más alto de protección. Esto supone que debemos adoptar una serie de medidas de seguridad para salvaguardar la intimidad de los pacientes.

Los pasos fundamentales que se deben dar para adecuarse a la LPD son:

1. Informar a la Agencia de Protección de Datos (en adelante AGPD) de la existencia del fichero y registrarlo. Este trámite podemos hacerlo de diferentes maneras:

- Vía Telemática: (la más cómoda): a través de Internet, en la página <https://www.agpd.es/portalweb/index-ides-idphp.php> en la que podremos acceder a un formulario, encontrando en la misma página instrucciones claras de cómo rellenarlo y enviarlo directamente a través de la web [en el Capítulo II de la presente guía se incluye un tutorial de cómo rellenar el formulario de la AGPD]
- Vía personal: es necesario descargar y rellenar antes el formulario llamado NOTA (se obtiene en la misma web que el anterior) y enviarlo impreso y en soporte digital para agilizar el trámite a la Agencia de Protección de Datos.

2. Adopción de medidas de seguridad y redacción del Documento de Seguridad.

Tanto las medidas de seguridad como el Documento son imprescindibles e inexcusables en el tratamiento de nuestro historial clínico. Existe una guía de redacción del documento a disposición del responsable de seguridad en la web de la AGPD [consultar Documento de Seguridad en el Capítulo I: Terminología y Capítulo III: medidas de seguridad].

3. Auditorias bianuales: será necesario realizar auditorias cada 2 años para determinar si son adecuadas y si se cumplen las medidas de seguridad recogidas en el Reglamento de la LPD (Título VIII). Esta auditoria puede ser interna o externa y concluirá con un informe en el contenga los siguientes puntos:

- Adecuación de las medidas y controles a lo dispuesto en el Título VIII del Reglamento.
- Identificación de deficiencias y propuesta de medidas correctoras o complementarias.
- Datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Análisis del responsable de seguridad, que elevará sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.
- Deberá quedar a disposición de la Agencia Española de Protección de Datos.

Tener un documento de seguridad en regla no nos garantiza que estemos bajo el amparo de la Ley, es necesario cumplir lo que en el libro pone, es decir, debemos respetar escrupulosamente las medidas de seguridad y hacer que los demás las cumplan. **La ignorancia de la ley no exime de su cumplimiento.**



Terminología

1. Obtención de datos

La LPD otorga a los pacientes los derechos de: conocer para que se usen sus datos, conocer que existe un fichero con sus datos y saber quién es el responsable del fichero y su dirección.

Los datos que recabamos de los pacientes siempre deben ser cedidos previa autorización de los mismos, es decir, los pacientes deberán firmar un documento que indique que se están recabando sus datos para poder realizar un diagnóstico y tratamiento correcto. El consentimiento expreso u oral para datos de salud está contemplado en la Ley y se permite (art. 7.3), si bien es aconsejable recabar esta autorización por escrito ya que en caso de cualquier incidencia será obligación del responsable del fichero demostrar que ese consentimiento existe (art. 12.3).

En la historia clínica podemos añadir un pequeño anexo que incluya la autorización a la cesión de datos con un espacio para que el paciente firme (incluyendo DNI). En esa autorización debemos incluir los apartados que señala el artículo 5 de la LPD y el 12.2 de su Reglamento. (ANEXO I)

El tratamiento de datos sin consentimiento esta considerado como una infracción grave (art. 44).



ANEXO I

Ejemplo de «Autorización a la cesión de datos»

Yo..... con DNI.....
. he sido informado de la existencia del fichero o tratamiento de datos de carácter personal de la Clínica... (incluir aquí la denominación que tiene el fichero), de su finalidad y de los destinatarios de la información. Así mismo he sido informado del carácter obligatorio o facultativo de la respuesta a las preguntas que me han sido planteadas; de las consecuencias de la obtención de los datos y de mi posible negativa a suministrarlos. Se me ha informado de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y de la identidad y dirección del responsable del tratamiento (puede incluirse aquí la identidad y dirección en concreto).

Fecha y Firma

2. Derechos de los pacientes

Los derechos de los que dispone el paciente sobre sus datos son:

- **Derecho de acceso:** derecho a solicitar y obtener información de sus datos sometidos a tratamiento y de las comunicaciones realizadas o que se prevean hacer con sus datos. El paciente puede pedirlo, sin justificación, cada 12 meses (y en menor plazo si alega interés legítimo). Se le debe contestar en 1 mes, pudiendo ejercer su derecho hasta 10 días después de la notificación de estimación de solicitud.
- **Derecho de rectificación:** derecho a que se actualicen sus datos si son inexactos o incompletos. Plazo: 10 días.
- **Derecho de cancelación:** derecho a que se borren o supriman sus datos si son inexactos o se han tratado ilegítimamente. Plazo: 10 días.

(Nota: los datos no se borrarán, sino que se bloquearán, por si es preciso conservarlos en atención a posibles responsabilidades durante el plazo de prescripción de éstas. Una vez transcurrido el plazo se borrarán).

- **Derecho de oposición:** derecho a solicitar que no se traten sus datos.

Siempre se debe contestar al solicitante (aunque no se tengan datos suyos) por medios que permitan acreditar el envío y la recepción de la notificación (ej. correo certificado).

Todos estos derechos no son absolutos. El responsable del fichero puede denegarlos cuando concurra causa legal para ello.

3. Responsable del fichero

Aquel que decide sobre la finalidad y el uso del tratamiento de los datos personales (un autónomo o empresario individual será responsable del tratamiento de los datos personales de sus clientes/pacientes). Existe una Guía del Responsable de Ficheros elaborada por la Agencia de protección de datos que contiene información de interés.¹

Obligaciones:

- notificar el fichero ante el Registro General de Protección de Datos para que se proceda a su inscripción.
- Asegurarse de la autenticidad de los datos, de que se han obtenido legítimamente y que se tratan para la finalidad para la que se han obtenido.
- Garantizar el cumplimiento de los deberes de secreto y seguridad
- Informar a los pacientes de la recogida de los datos y obtener su consentimiento.
- Facilitar y garantizar el derecho gratuito a los pacientes a acceder, rectificar, oponerse y cancelar sus datos.
- Asegurar que en sus relaciones con terceros que le presten servicios y que comporte el uso de datos de pacientes (protésico, gestor) se cumpla lo dispuesto en la LPD.

¹ En la página principal de la AGDP ir a Documentación (en la barra naranja superior) – Publicaciones. En Publicaciones aparece la "Guía del responsable de fichero".

4. Encargado del tratamiento

Es aquel que solo o conjuntamente con otros, trate personalmente datos personales por cuenta del responsable del fichero como consecuencia de una relación jurídica que le vincule con el mismo. El encargado del tratamiento es ajeno a la organización del responsable del fichero (como podría ocurrir entre odontólogos que realizan prestación de servicios a otro dentista). No están incluidos en esta figura aquellos que tengan acceso a datos por su condición de empleado del responsable del fichero (Ej. auxiliar de clínica contratada por el dentista, recepcionista, dentista en régimen laboral...). El encargado del tratamiento y el responsable del fichero deberán firmar un contrato escrito que permita acreditar la existencia del fichero y su contenido.

5. Documento de seguridad

Documento que aglutina todas las medidas que el responsable del fichero debe cumplir para adecuar su fichero de datos (y su consulta) a la LPD y su reglamento. El documento debe guardarse en la clínica y debe actualizarse cada vez que se produzca una incidencia. En el mismo se incluirán los acuerdos con terceros que supongan manejo de datos (protésico, gestor), así como los compromisos de confidencialidad con el encargado del tratamiento y los empleados. El documento de seguridad tiene diferente contenido según tenga nuestro fichero carácter automatizado o no automatizado (es decir, con soporte informático o en papel). La Agencia de protección de datos pone a nuestra disposición un modelo en la Guía del Documento de Seguridad¹ (página 11) que incluye las modificaciones pertinentes según nuestro fichero sea automatizado o no.

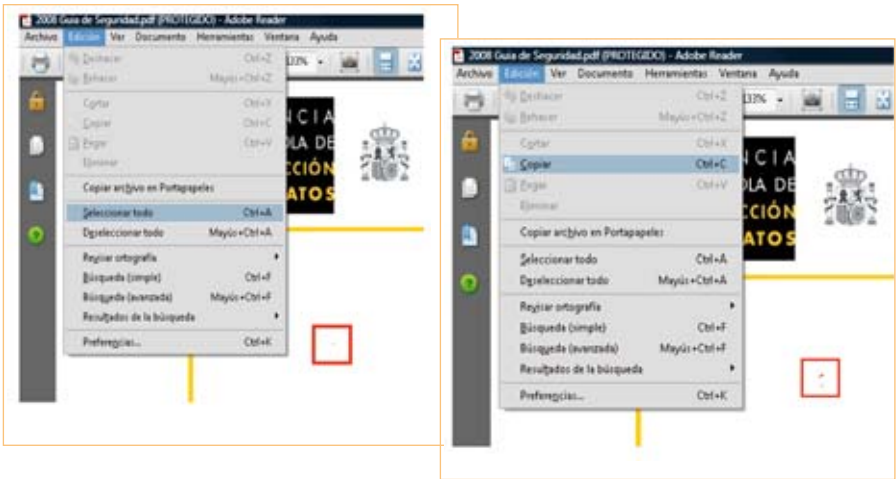
¹ En la página principal de la AGDP ir a Resp. Ficheros (en la barra naranja superior) – Guía Documento de Seguridad. En la página que aparece tenemos un enlace abajo para ir al documento pdf que contiene el modelo de documento de seguridad.

En caso de querer usar este documento como base seguiremos los siguientes pasos:

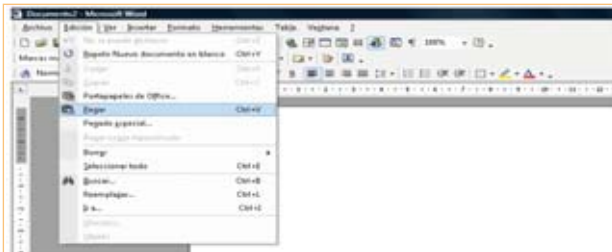
- descargaremos el archivo a nuestro disco duro [guardando el archivo pulsando sobre el icono del disquete señalado con el círculo rojo].



Se abrirá un cuadro de diálogo que nos preguntará donde guardarlo. Una vez guardado, lo abriremos y pulsaremos en "Edición-Seleccionar todo" (1). Volveremos a pulsar en "Edición" y pinchamos en "Copiar" (2).



Una vez realizados estos pasos, abriremos nuestro editor de texto (Microsoft Word, por ejemplo) y en un documento en blanco pincharemos en Edición-Pegar



Nos aparecerá todo el texto del documento en el archivo Word, así podremos modificar lo que queramos del documento tipo (que empieza a partir de la página 11, con el índice). En la Guía del Documento se nos indica los campos que hay que modificar, y que nos encontraremos entre "< >". También nos indicará si debemos completar o no una parte del documento según nuestro tipo de fichero (automatizado o no). Es **muy aconsejable** leer la introducción y las notas previas al modelo de documento en sí.

6. Auditoria

La LPD obliga a realizar una **auditoria bianual** de nuestro fichero, en la que se debe hacer constar el estado del mismo, el cumplimiento de las medidas de seguridad y las medidas a adoptar en caso de encontrar deficiencias. Se deben notificar al responsable del fichero las deficiencias encontradas para que este las solucione. El informe de la auditoria debe estar a disposición de la Agencia de Protección de Datos en caso de que esta lo solicite.

La LPD no indica que la auditoria deba ser obligatoriamente realizada por un auditor externo, existiendo la posibilidad de realizar una auditoria interna.

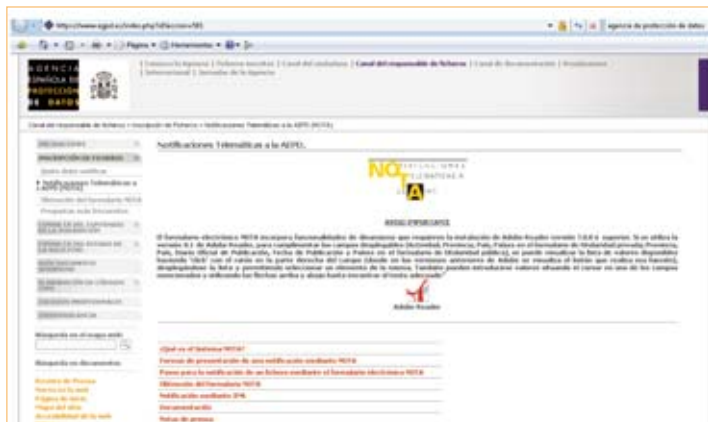
TUTORIAL DE INSCRIPCIÓN DE FICHERO EN LA AGENCIA DE PROTECCIÓN DE DATOS

1. Abrir Internet Explorer (o el navegador que tengamos instalado) e ir a la dirección de la agencia de protección de datos: <https://www.agpd.es/portalweb/index-ides-idphp.php>

Una vez en esta web, pincharemos en donde pone Notificaciones telemáticas a la APD. Inscripción de ficheros (señalada en rojo en la fig.1).



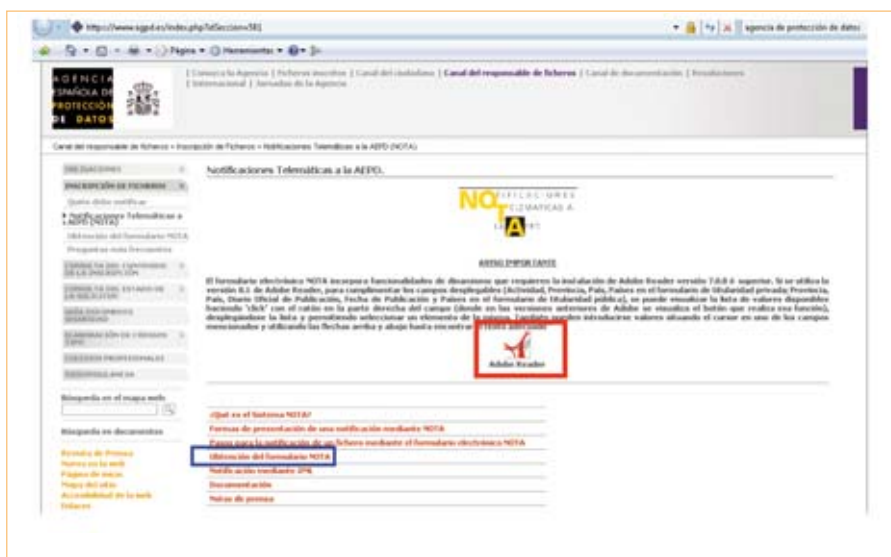
2. Al pinchar en esta zona nos llevará a otra página (fig. 2).



□ 3. Antes de continuar es conveniente saber si tenemos instalado el Acrobat Reader en nuestro ordenador, si no lo tenemos instalado pincharemos en el icono de Acrobat Reader que aparece en la misma página (recuadro rojo en fig.3). Al hacerlo saltará una ventana que nos lleva a la página de Adobe desde la que nos podemos descargar (gratuitamente) el Acrobat Reader.

(nota: si tenemos bloqueado el acceso a ventanas emergentes en el navegador es posible que el Acrobat Reader no se ejecute, por tanto habrá que autorizar a la página a hacerlo, aparecerá, si se bloquea, un mensaje que si se pincha en él podremos autorizar a la página a abrir ventanas emergentes).

En caso de tenerlo instalado (o si ya lo teníamos) pincharemos en "Obtención del formulario nota" (recuadro azul en fig. 3)



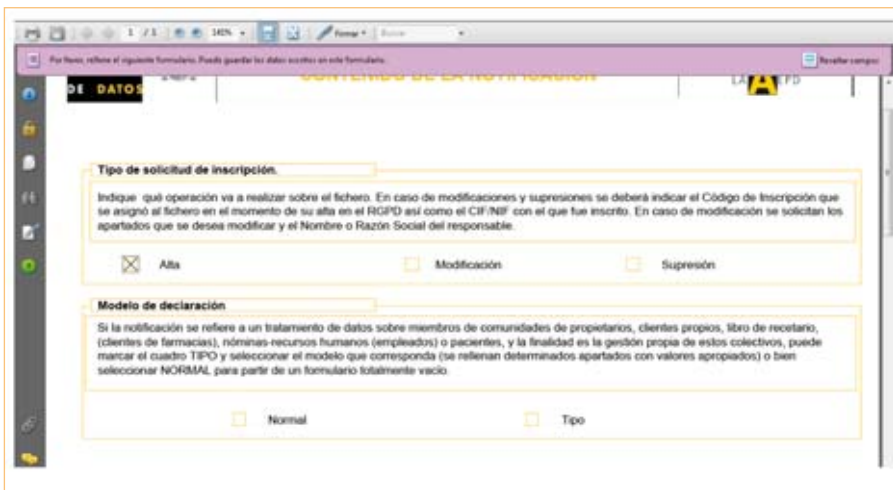
□ 4. Al pinchar sobre "obtención del certificado NOTA" nos llevará a otra página, al final de la cual, en el apartado "Descargas disponibles" debemos pinchar sobre: "Formulario NOTA de titularidad privada" (en rojo en fig. 4)

	Fecha de última actualización
Formulario NOTA de titularidad pública. (Consulte AVISO IMPORTANTE para la versión de Adobe Reader).	7/2/2006
Formulario NOTA de titularidad privada. (Consulte AVISO IMPORTANTE para la versión de Adobe Reader)	7/2/2006
Guía rápida del formulario NOTA	06/06/2007
Manual del formulario electrónico de notificación de ficheros de Titularidad Pública	07/05/2007
Manual del formulario electrónico de notificación de ficheros de Titularidad Privada	07/05/2007
Preguntas más frecuentes	06/06/2007

5. Volverá a saltar una ventana en la que se abrirá un documento PDF (razón por la que debemos tener instalado el Acrobat Reader) que contiene un aviso (en rojo en Fig. 5) que nos indica que rellenemos el formulario, es decir, lo que se abre podemos rellenarlo en las casillas correspondientes pinchando sobre ellas con el ratón.



6. Como lo que queremos es dar de alta el fichero pinchamos en la casilla que pone "Alta", apareciendo en ese momento debajo del último párrafo (Fig 6) otro que pondrá "Modelo de declaración" (nota: cada vez que pinchemos en una casilla esta aparecerá señalada, no es posible volver atrás, si nos equivocamos deberemos cerrar esa ventana y volver al punto 4).



□ 7. En "Modelo de declaración" podemos elegir dos opciones, la "Normal" nos permitirá rellenar el formulario a nuestro gusto, mientras que la opción "Tipo" presenta un formulario adaptado a nuestra necesidad (en este caso: fichero de pacientes), por tanto vamos a elegir la opción "Tipo". Al marcar esta opción aparecerán varios nombres de modelos, nosotros debemos señalar el de "pacientes" (Fig. 7)

Por favor, rellene el siguiente formulario. Puede guardar los datos escritos en este formulario.

Indique qué operación va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de inscripción que se asignó al fichero en el momento de su alta en el RGPD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitan los apartados que se desea modificar y el Nombre o Razón Social del responsable.

Alta Modificación Supresión

Modelo de declaración

Si la notificación se refiere a un tratamiento de datos sobre miembros de comunidades de propietarios, clientes propios, libro de recetaario, (clientes de farmacias), nóminas-recursos humanos (empleados) o pacientes, y la finalidad es la gestión propia de estos colectivos, puede marcar el cuadro TIPO y seleccionar el modelo que corresponda (se rellenan determinados apartados con valores apropiados) o bien seleccionar NORMAL, para partir de un formulario totalmente vacío.

Normal Tipo

Tipos

Comunidad de Propietarios Nóminas-Recursos Humanos

Clientes y/o proveedores Pacientes

Libro Recetaario Gestión Escalar

□ 8. El siguiente casillero a rellenar es la forma en la que vamos a presentar el documento, tenemos tres opciones: con formulario de papel, a través de internet o a través de internet con certificado de firma digital. La mejor forma es hacerlo a través de internet y con certificado de firma digital. Este certificado se obtiene si tenemos el nuevo DNI electrónico o por medio de la Tarjeta Rido del Consejo de Dentistas.

Si no lo tenemos y no tenemos pensado obtenerlo, las otras dos opciones nos obligan a enviar por correo postal o fax a la Agencia de Protección de Datos el formulario una vez rellenado (la dirección de la Agencia es: Agencia Española de Protección de Datos C. Jorge Juan, 6 28001- Madrid, y el fax: 91 445 25 29 ó 91 448 36 80). Es recomendable seguir la opción de rellenar el documento a través de internet (si no tenemos firma digital), para posteriormente imprimir el documento y enviarlo como queramos.

Al señalar cualquiera de las 3 opciones la página saltará a un documento ("Hoja de Solicitud") nuevo que deberemos rellenar. Es importante tener en cuenta que cada vez que rellenemos correctamente un apartado de ese documento debemos pulsar sobre la pestaña "validar" que aparece a la derecha de cada apartado, si nos hemos equivocado podremos pulsar en borrar y nos vaciará los casilleros que hemos rellenado nosotros.

- 9. El primer campo a rellenar es el de responsable del fichero (fig. 8).

Formulario "Responsable del fichero" con los siguientes campos:

- Denominación social del responsable del fichero
- Actividad (con flecha desplegable)
- CIF/NIF
- Domicilio Social
- Localidad
- Código Postal
- Provincia
- País
- Teléfono
- Fax
- Correo electrónico

Este campo lo rellenaremos con nuestro nombre (si somos los responsables del fichero, por ejemplo si soy el dueño de la clínica) o con el nombre del responsable del fichero si se trata de una sociedad. Señalamos "sanidad" en la flecha desplegable en el cuadro "Actividad" y rellenamos el resto de los campos (no es obligatorio rellenar teléfono, fax y correo electrónico).

- 10. El segundo campo es "Derechos de oposición, acceso, rectificación y cancelación" (fig. 9) Este campo solo debe rellenarse si la dirección es distinta al domicilio social del primer campo. Si son varias clínicas, indicar la principal.

Formulario "Derechos de oposición, acceso, rectificación y cancelación" con los siguientes campos:

- Nombre de la oficina o dependencia
- Dirección postal / Apdo. de Correos
- Localidad
- Código Postal
- Provincia
- País
- Teléfono
- Fax
- Correo electrónico

- 11. El tercer campo (encargado del tratamiento, fig 10) debe rellenarse si el responsable del fichero no es el que realiza el tratamiento. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento tratará los datos conforme a las instrucciones del responsable del fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas, este contrato debe incluirse en el **Documento de seguridad** que debe tener el responsable del fichero en su clínica.

Si los encargados del tratamiento son varios solo será necesario inscribir a uno, se recomienda que se haga constar al que realice el tratamiento de datos que pueda implicar una mayor duración en el tiempo, o riesgos mayores según el tipo y la cantidad de datos tratados.

Formulario "Encargado del tratamiento" con los siguientes campos:

- Denominación social del encargado del tratamiento
- Dirección postal
- Localidad
- Código Postal
- Provincia
- País
- Teléfono
- Fax
- Correo electrónico

□ 12. El apartado 5 es "Identificación y finalidad del fichero" y ya nos aparece previamente rellenado, así que, si estamos de acuerdo con lo que pone lo dejamos tal cual. Este apartado tiene un campo que nos deja añadir otras finalidades al tipo de fichero, si queremos incluir alguna de las dos o quitar alguna de las que hay incluidas solo tendremos que pinchar en las flechas de dirección (fig. 11).

Tipificación correspondiente a la finalidad y usos previstos

Finalidades

Usos que podemos añadir si queremos

INVESTIGACION EPIDEMIOLOGICA Y ACTIVIDADES ANALOGAS
OTRO TIPO DE FINALIDAD

Usos previstos

GESTION Y CONTROL SANITARIO
HISTORIAL CLINICO

□ 13. El siguiente campo (fig. 12) también aparece relleno y, como en el anterior, podemos añadir a "padres y tutores" si prevemos que vamos a obtener datos de estos últimos.

6 Origen y procedencia de los datos Validar Borrar

Origen

El propio interesado o su representante legal Otras personas físicas Fuentes accesibles al público

Registros públicos Entidad privada Administraciones Públicas

Colectivos o categorías de interesados

PADRES O TUTORES

PACIENTES

14. El apartado 7 sigue la dinámica de los anteriores y aparece totalmente relleno, podemos añadir además otros datos de carácter identificativo como fotos de los pacientes en la casilla en blanco (fig. 13).



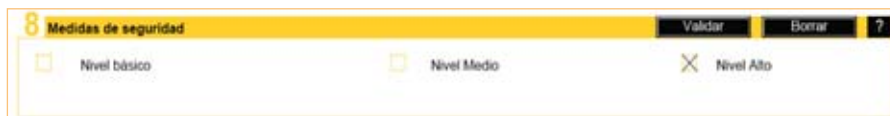
Disponemos de un cuadro como los de los apartados 5 y 6 en el que nos deja añadir o quitar algunos datos que nosotros consideremos de interés para hacer constar dentro de la historia clínica.

Muy importante es el cuadro de la fig. 14 (en el mismo apartado 7) en el que debemos señalar que tipo de fichero es el nuestro: "automatizado" (es decir, informatizado), "manual" (con fichas escritas a mano) o mixto (ambos).

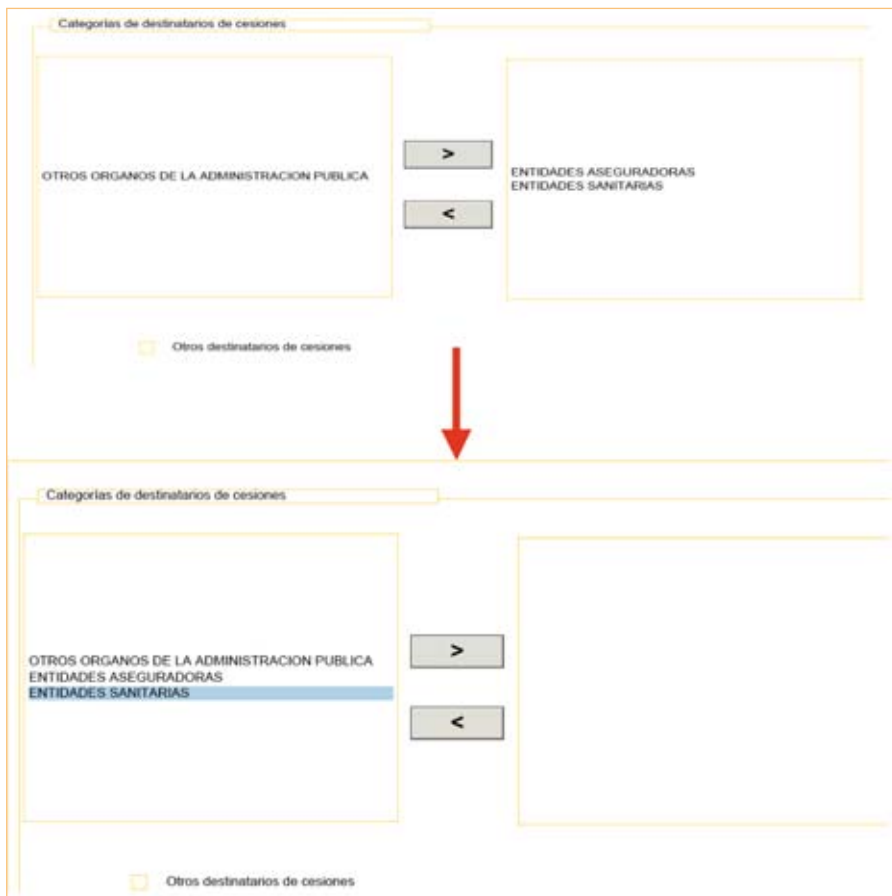
En el ejemplo que exponemos a continuación supondremos que solo tenemos uno manual (que además requiere medidas de seguridad más fáciles de cumplir) y lo señalaremos [los otros dos tienen igual sistemática].



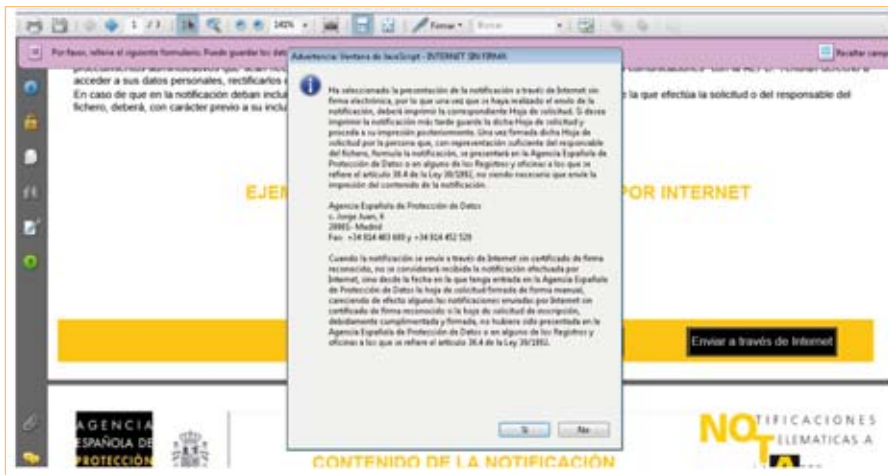
15. El apartado 8 (que ya viene señalado –fig 15) indica el nivel de seguridad que debe tener nuestro fichero, al tratarse de datos de carácter sanitario, el nivel de seguridad será siempre alto.



16. El último apartado solo se debe rellenar si se prevé que se van a ceder datos alguna entidad (ya sea un seguro, una entidad sanitaria o un órgano de la administración pública), sería por ejemplo el caso que trabajemos con una entidad aseguradora y esta nos pida datos de tratamientos de pacientes para su contabilidad (por ejemplo si el paciente utiliza tarjeta sanitaria). Si no lo vamos a hacer quitaremos las dos opciones que están puestas (fig 16).



□ 17. Una vez cumplimentados todos los campos, nos vamos al final y pulsamos en "Validar" (si no lo hemos hecho con todos y cada uno de los apartados). Si queremos podemos imprimir o guardar el documento. El paso siguiente es pulsar sobre "Cumplimentar Hoja de Solicitud", nos saltará a otro documento que nos encontraremos relleno con los datos que hemos escrito antes, junto con dos apartados: "Declarante" (si es el mismo que el responsable del fichero rellenar con los mismos datos) y "Dirección a efectos de notificación" (dirección completa que la administración tendrá para notificarnos cualquier incidencia). Una vez cumplimentado todo y aceptadas las condiciones, pulsaremos en "Enviar a través de Internet", momento en el cual nos aparecerá un mensaje como en la figura 17.



Este aviso nos dice que si queremos enviar el documento por internet sin firma digital debemos imprimir la hoja de solicitud y enviarla por correo o por fax a la Agencia de Protección de Datos. El fichero solo se considera recibido si la Agencia ha recibido la hoja de notificación.

18. Al pulsar en "Si", nos aparece otra notificación que nos dice que nos están enviando la hoja de solicitud para que procedamos a imprimirla y mandarla a la Agencia. Confirmamos y se actualizará la página con la hoja (ya no es un borrador como antes) de solicitud. Esta hoja es la que debemos imprimir (y si queremos guardar) y mandar a la agencia firmada. Para imprimir directamente pulsamos en el icono de la impresora que hay en la parte superior izquierda (fig. 18)



En el caso de tener firma digital este paso no lo tenemos que realizar, ya que firmaremos con nuestro certificado digital en la casilla correspondiente.

□ 19. Si ya hemos cumplimentado el envío, podemos consultar el estado de la tramitación desde la misma página de la agencia de protección de datos (en la misma sección que se señala en el apartado 2) en la pestaña "Consulta del estado de la solicitud" (fig. 19) y debemos rellenar el campo de NIF y el número de envío(que aparece en la hoja de Solicitud de inscripción debajo de "Tipo de Solicitud", puede verse en la fig 18 abajo a la derecha). En caso de haber inscrito el fichero con certificado de firma digital solo será necesario rellenar el campo de NIF.

The image shows a screenshot of a web browser displaying the 'Consulta del estado de la solicitud' page on the website of the Agencia de Protección de Datos. The browser's address bar shows the URL 'http://www.agpd.es/index.php/laSeccion=386'. The page header includes the agency's logo and navigation links such as 'Inicio de la Agencia', 'Ficheros inscritos', 'Canal del ciudadano', 'Canal del responsable de ficheros', 'Canal de documentación', 'Resolución de incidencias', 'Internacional', and 'Servicios de la Agencia'. The main content area is titled 'Canal del responsable de ficheros' and 'Consulta del estado de la solicitud'. A sidebar on the left contains a menu with options like 'SOLICITACIONES', 'INSCRIPCIÓN DE FICHEROS', 'ESTADO EN EL CONVENIO DE LA INSCRIPCIÓN', 'CONSULTA DEL ESTADO DE LA SOLICITUD', 'Consultas', 'SOLICITUD DE ACCESO A LA INFORMACIÓN PERSONAL', 'SOLICITUD DE RECTIFICACIÓN DE DATOS', 'SOLICITUD DE SUPRESIÓN DE DATOS', and 'SOLICITUD DE ANONIMIZACIÓN'. The main form area is titled 'Solicitud de ficheros de titularidad Pública: Solicitud general' and contains the following fields: 'DATOS DEL DECLARANTE' with a 'NIF' field; 'FIRMADO' with 'Código de envío' and 'Código de inscripción' fields; and a 'Botón' at the bottom right.



MEDIDAS DE SEGURIDAD

Las medidas de seguridad a aplicar a los ficheros de pacientes son las de nivel alto, por tanto a su vez son de aplicación las de nivel básico y medio.

Es necesario aclarar previamente los siguientes conceptos:

Responsable de seguridad: es el encargado de coordinar y controlar las medidas del documento. Debe designar a uno o varios responsables de seguridad (sin delegar en los mismos).

Personal: cada uno de ellos tendrá sus funciones definidas y documentadas. Se debe difundir entre el personal las normas que les afecten y las consecuencias de su incumplimiento.

Incidencias: deben registrarse todas las incidencias (incluyendo: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras) y proceder a su notificación y gestión. En ficheros automatizados: Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente; y las autorizaciones del responsable del fichero para la recuperación de datos.

A continuación se detallan las medidas de seguridad a adoptar para cada apartado.

Control de Acceso:

- Tener una relación actualizada de usuarios y accesos autorizados
- Control de accesos permitidos a cada usuario según las funciones asignadas.
- Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.
- Concesión de permisos de acceso sólo por personal autorizado.
- Mismas condiciones para personal ajeno con acceso a los recursos de datos.
- **Solo ficheros automatizados:** Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información (es decir: llave del local). Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado (esta función la suele hacer el programa de gestión de clínica). Revisión mensual del registro por el responsable de seguridad. Conservación 2 años. No será necesario este registro si el responsable del fichero es una persona física y es el único usuario.

- **Solo ficheros no automatizados:** Control de accesos autorizados (llave en los ficheros y llave en el lugar donde se encuentren). Identificación de accesos para documentos accesibles por múltiples usuarios.

Identificación y autenticación: solo en ficheros automatizados:

- Identificación y autenticación personalizada, procedimiento de asignación y distribución de contraseñas (cada usuario una contraseña diferente).
- Almacenamiento ininteligible de las contraseñas (no almacenarlas en un papel).
- Periodicidad del cambio de contraseñas (>1 año).
- Limite de intentos reiterados de acceso no autorizado (que no se pueda probar a introducir una contraseña un número indefinido de veces).

Gestión de Soportes: es obligatorio tener un inventario de soportes

- Identificación del tipo de información que contienen, o sistema de etiquetado
- Acceso restringido al lugar de almacenamiento (llave)
- Autorización de las salidas de soportes (incluidas a través de e-mail)
- Medidas para el transporte y el desecho de soportes.

En ficheros automatizados además habrá que tener

- Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.
- Sistema de etiquetado confidencial
- Cifrado de datos en la distribución de soportes.
- Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).

[Para los dos últimos puntos, existen discos duros y programas informáticos de cifrado de datos que protegen la información].¹

Copias de Respaldo: [Solo para ficheros automatizados]

- Copia de respaldo semanal (es decir, copia de seguridad semanal)
- Procedimientos de generación de copias de respaldo y recuperación de datos (protocolos de cómo hacer copias de seguridad y de cómo recuperar los datos).
- Verificación semestral de los procedimientos.
- Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita.

¹ Para mas información consultar el artículo de Odontología e Informática de Mayo de 2008 en la revista Profesión Dental.

- Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.
- Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos (tener una copia en un lugar que no sea la clínica).

Criterios de Archivo: [solo ficheros no automatizados] El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (en adelante: ARCO).

Almacenamiento: [solo ficheros no automatizados]

- Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura (cerraduras, candados..).
- Armarios, archivadores,... de documentos en áreas con acceso protegido con puertas con llave.

Custodia de los Soportes: [solo ficheros no automatizados] Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.

Copia o Reproducción: [solo ficheros no automatizados]

- Sólo puede realizarse por los usuarios autorizados
- Destrucción de copias desechadas (la destrucción debe garantizar la ilegibilidad del documento)

Auditoria:

- Al menos cada dos años, interna o externa.
- Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad.
- Verificación y control de la adecuación de las medidas.
- Informe de detección de deficiencias y propuestas correctoras.
- Análisis del responsable de seguridad y conclusiones al responsable del fichero.

Telecomunicaciones: [solo ficheros automatizados]

- Transmisión de datos a través de redes electrónicas cifradas.
- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.

Traslado de documentación: [solo ficheros no automatizados] Medidas que impidan el acceso o manipulación.

Otras consideraciones de seguridad:

- La ejecución de trabajos fuera de los locales del responsable o del encargado del tratamiento debe ser previamente autorizada por el responsable del fichero, constanding en el documento de seguridad, y garantizando el nivel de seguridad.
- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.
- El Acceso facilitado a un encargado del tratamiento deberá constar en el documento de seguridad y deberá comprometerse al cumplimiento de las medidas de seguridad previstas.

Radiografías, fotografías o modelos dentales en congresos o publicidad: la AGP ha informado que en el caso que se quiera utilizar cualquiera de los citados soportes para su uso en congresos o como publicidad de la clínica deberá contar con el consentimiento expreso (y siempre mejor por escrito) del afectado o de sus padres o tutores en caso de menores de edad, informándole de lo que supone el consentimiento dado y las consecuencias y derechos que ese consentimiento supone.

Tratamiento de los datos en caso de venta de clínica: el nuevo responsable del fichero deberá recabar nuevamente el consentimiento de los pacientes para manejar sus datos de salud.

Videovigilancia: en caso de tener instaladas en la clínica cámaras de videovigilancia es obligatorio colocar una nota informativa a vista del público y un cartel informativo.

La nota informativa puede ser como el ejemplo siguiente:

"De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado "...." y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.
2. Que el destinatario de sus datos personales es:
 - a. La empresa de seguridad.....
 - b. El dueño del establecimiento.....
3. Que puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante el responsable del fichero.
4. Que el responsable del fichero tratamiento es " (....nombre o razón social.....)" o su representante D./D^a:"....." ubicado en C/..."

Esta nota debe colocarse en el cartel.

El cartel puede ser descargado de la web de la AGPD (en "documentación"- "informes jurídicos", una vez en "informes jurídicos" buscar en la columna de la izquierda "Videovigilancia", hacer clic en informe 2007-0084 "Cartel informativo").