Fundació Privada Quiropràctica

Política de protección de datos personales

Versión 0.1

17-5-2018

Contenido

Política de protección de datos personales

El presente documento, redactado en cumplimiento de lo dispuesto en el reglamento recoge las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD/RGPD.

1 Ámbito de aplicación del documento

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de Fundació Privada Quiropràctica, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

2 Gestión de soportes y documentos

Todo soporte o documento que contenga datos personales debe indicar claramente el tipo de información que contiene y estar controlado mediante un inventario. Solamente podrán acceder a dichos documentos aquellas personas que acrediten la autorización siguiente:

Perfil	Autorización **mediante**
Director/a de la fundación	Autorizados/as natos
Administrativos	Contrato laboral
Profesores	Autorización *ad hoc*
Gerente	Autorizados/as natos
Administradores/as de sistemas informáticos	Autorización *ad hoc*

Otras personas que requieran acceder deberán hacerlo mediante autorización *ad hoc*.

No es necesario cumplir las obligaciones anteriores en el caso de los siguientes soportes debido a sus características físicas:

No se han descrito hasta la fecha.

2.1 Etiquetado, inventariado, almacenamiento y archivo de soportes y documentos

Los expedientes de los estudiantes serán etiquetadas de la siguiente forma:

Las tres primeras letras del apellido seguidas del número de historia clínica que ofrece de modo secuencial el programa gestor.

En lo referente al almacenamiento de soportes electrónicos, se seguirán estas directrices:

Etiquetado: BCC – Equipo del que realiza copias - fecha de entrada en servicio (mes y año) – Capacidad – Número de disco (debe corresponderse con el número asignado por el sistema de copias del sistema operativo) – Encriptado (S/N)

Ejemplo: BCC-ServerBCC-Mayo2018-1TB-3-S

Los expedientes de estudiantes se conservan en papel, bajo llave en archivadores.

Del servidor BCC se hace una copia diaria en un disco externo que se almacena, bajo llave. El disco se sustituye semanalmente. El responsable de la gestión de los discos es el DPD.

Las salidas de copias de seguridad se registrar en un registro en soporte papel.

Aquellos documentos o soportes con datos personales que no se hayan archivado aún por encontrarse en proceso de tramitación deberán tener una persona designada a cargo de su custodia que impida el acceso de personas no autorizadas.

2.2 Entrada, salida y distribución de soportes y documentos

Toda entrada o salida de un local bajo el control del responsable del tratamiento de cualquier tipo de soporte o documento que contenga datos de carácter personal quedará registrada utilizando el siguiente procedimiento:

Este registro se almacenará en soporte papel y constará de los siguientes campos:

Campos de entrada:

Al menos tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la recepción.

Campos de salidas:

Al menos el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la entrega.

Además, toda entrada o salida de un soporte o documento que contenga datos de carácter personal debe estar autorizada por el responsable de dicho soporte/documento o aquella persona sobre la que se hubiese delegado dicha autoridad. El procedimiento de autorización seguirá los siguientes pasos:

Se autorizará por escrito la salida de los datos. Junto a la autorización se entregará un recordatorio de las responsabilidades y obligaciones de la persona que realiza la salida de datos. La persona que realiza la salida de datos firmará un acuse de recibo de la autorización y del recordatorio de responsabilidades y obligaciones.

En el caso de soportes con información de carácter personal especialmente importante, será necesario efectuar los siguientes procedimientos antes de su distribución o salida:

Los descritos en el punto anterior.

2.3 Destrucción o borrado de soportes o documentos

En caso de que algún soporte vaya a ser destruido o borrados sus datos, debe seguirse el siguiente procedimiento para evitar el acceso o recuperación posterior de la información que contuviera:

La información en soporte papel se destruirá con destructoras de papel categoría 5.
El borrado de información en soporte electrónico se realizará mediante la herramienta Active KillDisk.

3 Identificación y acceso

Todo trabajador con acceso a datos personales deberá seguir el siguiente proceso de identificación y autenticación:

Para los soportes en papel: firmar la hoja de registro de accesos.

Para los registros electrónicos se les genera una contraseña inicial que se les entrega en persona y que deben cambiar en su primer acceso al sistema. Las contraseñas requieren de 8 caracteres mínimos, mayúscula, minúscula y número. Caducan cada 15 días.

En lo referente al acceso a información personal, éste se limitará a aquella necesaria por cada trabajador para el ejercicio de sus funciones.

Solamente administradores del sistema podrán conceder alterar o anular el acceso a ficheros o recursos que contengan datos de carácter personal en base a los siguientes criterios: su pertenencia a uno de los roles con permisos de acceso o por requerimientos de mantenimiento técnico.

De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

3.1 Registro de acceso

Para el acceso a ficheros con datos personales especialmente sensibles o importantes se registrará al menos por cada acceso la identificación del usuario con la fecha y hora, el fichero accedido, el tipo de acceso y si ha sido autorizada o denegada.

Los datos del registro de accesos se conservarán durante un tiempo no inferior a dos años.

Además, el responsable de seguridad debe revisar una vez al mes como mínimo la información de los registros y elaborar un informe al respecto.

3.2 Acceso a través de una red

Todo dato personal especialmente sensible transmitido por una red de comunicación pública o inalámbrica será cifrado previamente.

4 Trabajo fuera de los locales de la ubicación del soporte o fichero

Se permite realizar los siguientes tratamientos con datos de carácter personal contenidos en los ficheros listados a continuación fuera de los locales del responsable del fichero o mediante dispositivos portátiles:

Acceso, modificación y borrado.

Esta autorización tendrá validez durante el periodo de relación contractual con la empresa para los siguientes usuarios: Administradores del sistema.

4.1 Traslado de información

Siempre que se proceda al traslado de información que contenga datos personales se tomarán las siguientes medidas con el fin de evitar el acceso a dicha información o su manipulación:

Las historias clínicas se mantienen en todo momento en un maletín con llave bajo el control del supervisor de clínica.

4.2 Ficheros temporales y copias de trabajo y reproducción de ficheros

En el caso de que sea necesario trabajar con ficheros temporales o copias auxiliares se deberá cumplir con el nivel de seguridad correspondiente a lo especificado en la ley. Además, serán borrados una vez dejen de ser necesarios para el motivo o la necesidad de trabajo para la que fueron creados.

Toda copia o reproducción de ficheros con datos personales se realizará bajo el control del siguiente personal autorizado:

- DPD.

Además, se destruirán las copias desechadas para evitar el acceso a su información mediante cualquiera de los siguientes medios:

- Destructoras de papel categoría 5 para documentos en papel.
- Borrado con Active KillDisk al final de la vida de los soportes electrónicos o al cambiar su destino.

5 Trabajo con información personal para fines de investigación

A la hora de llevar a cabo un proyecto de investigación o un trabajo con fines estadísticos es especialmente importante proteger los datos personales de los interesados. Para todo trabajo con fines de investigación se hará especial énfasis en la minimización de los datos personales. Esto podrá implicar, entre otros procedimientos, trabajar con datos agregados y datos que hayan pasado previamente por un proceso de seudonimización

(cuando esto sea compatible con la finalidad del trabajo). De manera general, se utilizarán los siguientes métodos para minimizar datos personales:

- Recabar únicamente los datos imprescindibles para el estudio
- Sustituir los nombres por códigos

Es importante tener en cuenta que, a pesar de que los datos con los que se trabaje estén seudonimizados, se siguen considerando como datos personales por lo que se les aplica la política del presente documento y la normativa RGPD.

Se recomienda consultar la "Política de buenas prácticas para trabajar con datos personales para fines de investigación y estadísticos" a la hora de tener en cuenta otros aspectos como el ejercicio de los derechos de los interesados, y la información sobre el tratamiento que se vaya a realizar.

6 Responsable de seguridad

Se designa un responsable de seguridad, que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero de acuerdo con el RLOPD/RGPD.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de un año. Una vez transcurrido este plazo se podrá nombrar al mismo responsable de seguridad o a otro diferente.

7 Información y obligaciones del personal

7.1 Información al personal

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:

Se llevará a cabo una primera sesión informativa seguida de información periódica relativa a modificaciones, recordatorios. La información a remitir será acordada entre el responsable de seguridad y el responsable del fichero.

7.2 Funciones y obligaciones del personal

Todo el personal que acceda a los datos de carácter personal está obligado a conocer

y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al responsable de seguridad las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este documento, y en concreto en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias."

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

7.3 Consecuencias del incumplimiento

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a:

Nivel profesional	Sanción
Administrativos	Laboral grave
Profesores	Laboral grave
Estudiantes	Expediente disciplinario y expulsión
Proveedores	Denuncia en los juzgados, rescisión de los contratos
Responsable de seguridad	Expediente disciplinario y si procede denuncia en los juzgados
Responsable del fichero	Expediente disciplinario y si procede denuncia en los juzgados

8 Procedimientos de notificación, gestión y respuesta ante las incidencias

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este documento, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del Barcelona Chiropractic Center SL.

El procedimiento a seguir para la notificación de incidencias será:
La persona que detecta una incidencia debe notificarla a la mayor brevedad posible (en cualquier caso no superando las 72 horas) escribiendo a la dirección electrónica dpd@bcchiropractic.es. Deberá indicar nombre apellido y número de teléfono, la naturaleza de la incidencia y las personas implicadas. La incidencia será gestionada por el responsable de seguridad o, en su defecto, por el responsable del fichero.

El registro de incidencias se gestionará en soporte papel, indicando los siguientes campos:

- Tipo de incidencia
- Fecha y hora en la que sucedió
- Fecha y hora en la que fue detectada
- Persona que la notificó
- Persona notificada
- Efectos que se derivaron
- Medidas correctoras aplicadas

9 Procedimientos de revisión

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.